The Generalised Continuum Hypothesis Implies the Axiom of Choice in Coq

Dominik Kirst and Felix Rech

Certified Programs and Proofs
January 17-19, 2021

SAARLAND UNIVERSITY
COMPUTER SCIENCE
SIC Saarland Informatics Campus

Sierpiński's Theorem*

Generalised Continuum Hypothesis (GCH):
There are no cardinalities between an infinite set and its power set.

*Sierpiński (1947), Specker (1990)

Sierpiński's Theorem*

Generalised Continuum Hypothesis (GCH):
There are no cardinalities between an infinite set and its power set.

$$\forall XY.\, |\mathbb{N}| \leq |X| \to |X| \leq |Y| \leq |\mathcal{P}(X)| \to |Y| \leq |X| \vee |\mathcal{P}(X)| \leq |Y|$$

*Sierpiński (1947), Specker (1990)

Sierpiński's Theorem*

Generalised Continuum Hypothesis (GCH):
There are no cardinalities between an infinite set and its power set.

$$\forall XY.\, |\mathbb{N}| \leq |X| \rightarrow |X| \leq |Y| \leq |\mathcal{P}(X)| \rightarrow |Y| \leq |X| \vee |\mathcal{P}(X)| \leq |Y|$$

*Sierpiński (1947), Specker (1990)

Sierpiński's Theorem*

Generalised Continuum Hypothesis (GCH):
There are no cardinalities between an infinite set and its power set.

$$\forall XY.\, |\mathbb{N}| \leq |X| \rightarrow |X| \leq |Y| \leq |\mathcal{P}(X)| \rightarrow |Y| \leq |X| \vee |\mathcal{P}(X)| \leq |Y|$$

*Sierpiński (1947), Specker (1990)

Sierpiński's Theorem*

Generalised Continuum Hypothesis (GCH):
There are no cardinalities between an infinite set and its power set.

$$\forall XY.\, |\mathbb{N}| \le |X| \to |X| \le |Y| \le |\mathcal{P}(X)| \to |Y| \le |X| \lor |\mathcal{P}(X)| \le |Y|$$

*Sierpiński (1947), Specker (1990)

Sierpiński's Theorem*

Generalised Continuum Hypothesis (GCH):
There are no cardinalities between an infinite set and its power set.

$$\forall XY.\, |\mathbb{N}| \leq |X| \to |X| \leq |Y| \leq |\mathcal{P}(X)| \to |Y| \leq |X| \vee |\mathcal{P}(X)| \leq |Y|$$

$$\Downarrow$$

Axiom of Choice (AC):
Every total relation contains the graph of a function.

*Sierpiński (1947), Specker (1990)

Sierpiński's Theorem*

Generalised Continuum Hypothesis (GCH):
There are no cardinalities between an infinite set and its power set.

$$\forall XY.\, |\mathbb{N}| \leq |X| \to |X| \leq |Y| \leq |\mathcal{P}(X)| \to |Y| \leq |X| \vee |\mathcal{P}(X)| \leq |Y|$$

$$\Downarrow$$

Axiom of Choice (AC):
Every total relation contains the graph of a function.

$$\forall R.\, (\forall x.\, \exists y.\, Rxy) \to \exists f.\, \forall x.\, Rx(fx)$$

*Sierpiński (1947), Specker (1990)

Sierpiński's Theorem - Outline*

1. Instead of AC, show the equivalent well-ordering theorem (WO)

*Gillman (2002), Smullyan and Fitting (2010)

Sierpiński's Theorem - Outline*

1. Instead of AC, show the equivalent well-ordering theorem (WO)

2. To well-order X it suffices to find well-ordered Y with $|X| \leq |Y|$

*Gillman (2002), Smullyan and Fitting (2010)

Sierpiński's Theorem - Outline*

1. Instead of AC, show the equivalent well-ordering theorem (WO)
2. To well-order X it suffices to find well-ordered Y with $|X| \leq |Y|$
3. Enough to only well-order infinite X since always $|X| \leq |\mathbb{N} \cup X|$

*Gillman (2002), Smullyan and Fitting (2010)

Sierpiński's Theorem - Outline*

1. Instead of AC, show the equivalent well-ordering theorem (WO)
2. To well-order X it suffices to find well-ordered Y with $|X| \leq |Y|$
3. Enough to only well-order infinite X since always $|X| \leq |\mathbb{N} \cup X|$
4. Central construction: Hartogs number $\aleph(X)$

*Gillman (2002), Smullyan and Fitting (2010)

Sierpiński's Theorem - Outline*

1. Instead of AC, show the equivalent well-ordering theorem (WO)
2. To well-order X it suffices to find well-ordered Y with $|X| \leq |Y|$
3. Enough to only well-order infinite X since always $|X| \leq |\mathbb{N} \cup X|$
4. Central construction: Hartogs number $\aleph(X)$
   - Large well-order: $|\aleph(X)| \not\leq |X|$

*Gillman (2002), Smullyan and Fitting (2010)

Sierpiński's Theorem - Outline*

1. Instead of AC, show the equivalent well-ordering theorem (WO)

2. To well-order X it suffices to find well-ordered Y with $|X| \leq |Y|$

3. Enough to only well-order infinite X since always $|X| \leq |\mathbb{N} \cup X|$

4. Central construction: Hartogs number $\aleph(X)$
   - Large well-order: $|\aleph(X)| \not\leq |X|$
   - Controlled height: $|\aleph(X)| \leq |\mathcal{P}^k(X)|$ for some k

*Gillman (2002), Smullyan and Fitting (2010)

Sierpiński's Theorem - Outline*

1. Instead of AC, show the equivalent well-ordering theorem (WO)
2. To well-order X it suffices to find well-ordered Y with $|X| \leq |Y|$
3. Enough to only well-order infinite X since always $|X| \leq |\mathbb{N} \cup X|$
4. Central construction: Hartogs number $\aleph(X)$
   - Large well-order: $|\aleph(X)| \not\leq |X|$
   - Controlled height: $|\aleph(X)| \leq |\mathcal{P}^k(X)|$ for some k
5. Use GCH to iteratively squeeze in $\aleph(X)$ and obtain $|X| \leq |\aleph(X)|$

*Gillman (2002), Smullyan and Fitting (2010)

Goal: Mechanisation in Coq

Goal: Mechanisation in Coq

Proof outline surprisingly abstract, only need to find formal notions of:

- Power sets
- Numbers
- Relations
- Functions
- Cardinality
- Orderings

Goal: Mechanisation in Coq

Proof outline surprisingly abstract, only need to find formal notions of:

- Power sets
- Numbers
- Relations
- Functions
- Cardinality
- Orderings

An expressive type theory like Coq's type theory allows two strategies:

Goal: Mechanisation in Coq

Proof outline surprisingly abstract, only need to find formal notions of:

- Power sets
- Numbers
- Relations
- Functions
- Cardinality
- Orderings

An expressive type theory like Coq's type theory allows two strategies:

1. Axiomatise some variant of set theory

Goal: Mechanisation in Coq

Proof outline surprisingly abstract, only need to find formal notions of:

- Power sets
- Numbers
- Relations
- Functions
- Cardinality
- Orderings

An expressive type theory like Coq's type theory allows two strategies:

1. Axiomatise some variant of set theory
2. Use Coq itself to represent the necessary notions

Goal: Mechanisation in Coq

Proof outline surprisingly abstract, only need to find formal notions of:

- Power sets
- Numbers
- Relations
- Functions
- Cardinality
- Orderings

An expressive type theory like Coq's type theory allows two strategies:

1. Axiomatise some variant of set theory
2. Use Coq itself to represent the necessary notions

Why are both variants interesting?

Goal: Mechanisation in Coq

Proof outline surprisingly abstract, only need to find formal notions of:

- Power sets
- Numbers
- Relations
- Functions
- Cardinality
- Orderings

An expressive type theory like Coq's type theory allows two strategies:

1. Axiomatise some variant of set theory
2. Use Coq itself to represent the necessary notions

Why are both variants interesting?

1. Many renderings of axiomatic set theory in type theory

Goal: Mechanisation in Coq

Proof outline surprisingly abstract, only need to find formal notions of:

- Power sets
- Numbers
- Relations
- Functions
- Cardinality
- Orderings

An expressive type theory like Coq's type theory allows two strategies:

1. Axiomatise some variant of set theory
2. Use Coq itself to represent the necessary notions

Why are both variants interesting?

1. Many renderings of axiomatic set theory in type theory
2. Insights about type theory itself

Variant 1: First-Order vs. Higher-Order ZF

Common setting: work in model $\mathcal{S} : \mathbb{T}$ providing set-theoretic structure

$$\in\ : \mathcal{S} \to \mathcal{S} \to \mathbb{P} \qquad \bigcup : \mathcal{S} \to \mathcal{S} \qquad \emptyset : \mathcal{S}$$
$$\{\_,\_\} : \mathcal{S} \to \mathcal{S} \to \mathcal{S} \qquad \mathcal{P} : \mathcal{S} \to \mathcal{S} \qquad \omega : \mathcal{S}$$

Variant 1: First-Order vs. Higher-Order ZF

Common setting: work in model $\mathcal{S} : \mathbb{T}$ providing set-theoretic structure

$$\in : \mathcal{S} \to \mathcal{S} \to \mathbb{P} \qquad \bigcup : \mathcal{S} \to \mathcal{S} \qquad \emptyset : \mathcal{S}$$

$$\{\_,\_\} : \mathcal{S} \to \mathcal{S} \to \mathcal{S} \qquad \mathcal{P} : \mathcal{S} \to \mathcal{S} \qquad \omega : \mathcal{S}$$

First-order ZF adds replacement for first-order relations:

$$\{x \mid \exists z \in y.\, \varphi(z, x)\} \qquad (\varphi \text{ a functional first-order formula})$$

Variant 1: First-Order vs. Higher-Order ZF

Common setting: work in model $\mathcal{S} : \mathbb{T}$ providing set-theoretic structure

$$\in : \mathcal{S} \to \mathcal{S} \to \mathbb{P} \qquad \bigcup : \mathcal{S} \to \mathcal{S} \qquad \emptyset : \mathcal{S}$$
$$\{\_,\_\} : \mathcal{S} \to \mathcal{S} \to \mathcal{S} \qquad \mathcal{P} : \mathcal{S} \to \mathcal{S} \qquad \omega : \mathcal{S}$$

First-order ZF adds replacement for first-order relations:

$$\{x \mid \exists z \in y.\, \varphi(z, x)\} \quad (\varphi \text{ a functional first-order formula})$$

Higher-order ZF admits replacement for all relations:

$$\{x \mid \exists z \in y.\, R\, z\, x\} \quad (R \text{ a functional relation } \mathcal{S} \to \mathcal{S} \to \mathbb{P})$$

Variant 1: First-Order vs. Higher-Order ZF

Common setting: work in model $\mathcal{S} : \mathbb{T}$ providing set-theoretic structure

$$\in : \mathcal{S} \to \mathcal{S} \to \mathbb{P} \qquad \bigcup : \mathcal{S} \to \mathcal{S} \qquad \emptyset : \mathcal{S}$$
$$\{\_,\_\} : \mathcal{S} \to \mathcal{S} \to \mathcal{S} \qquad \mathcal{P} : \mathcal{S} \to \mathcal{S} \qquad \omega : \mathcal{S}$$

First-order ZF adds replacement for first-order relations:

$$\{x \mid \exists z \in y.\, \varphi(z, x)\} \quad (\varphi \text{ a functional first-order formula})$$

Higher-order ZF admits replacement for all relations:

$$\{x \mid \exists z \in y.\, R\, z\, x\} \quad (R \text{ a functional relation } \mathcal{S} \to \mathcal{S} \to \mathbb{P})$$

- Convenient to work with by reusing meta-level structure

Variant 1: First-Order vs. Higher-Order ZF

Common setting: work in model $\mathcal{S} : \mathbb{T}$ providing set-theoretic structure

$$\begin{array}{lll} \in : \mathcal{S} \to \mathcal{S} \to \mathbb{P} & \bigcup : \mathcal{S} \to \mathcal{S} & \emptyset : \mathcal{S} \\ \{\_, \_\} : \mathcal{S} \to \mathcal{S} \to \mathcal{S} & \mathcal{P} : \mathcal{S} \to \mathcal{S} & \omega : \mathcal{S} \end{array}$$

First-order ZF adds replacement for first-order relations:

$$\{x \mid \exists z \in y.\, \varphi(z, x)\} \quad (\varphi \text{ a functional first-order formula})$$

Higher-order ZF admits replacement for all relations:

$$\{x \mid \exists z \in y.\, R\, z\, x\} \quad (R \text{ a functional relation } \mathcal{S} \to \mathcal{S} \to \mathbb{P})$$

- Convenient to work with by reusing meta-level structure
- Streamlined infinity and foundation axioms (Kirst and Smolka (2018))

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x. P\,x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Represent GCH and AC in Coq by the following propositions:

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Represent GCH and AC in Coq by the following propositions:

$$\forall XY.\, |\mathbb{N}| \leq |X| \leq |Y| \leq |\mathcal{P}(X)| \to |Y| \leq |X| \vee |\mathcal{P}(X)| \leq |Y|$$

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Represent GCH and AC in Coq by the following propositions:

$$\forall XY.\, |\mathbb{N}| \leq |X| \leq |Y| \leq |\mathcal{P}(X)| \to |Y| \leq |X| \vee |\mathcal{P}(X)| \leq |Y|$$

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Represent GCH and AC in Coq by the following propositions:

$$\forall XY : \mathbb{T}.\, |\mathbb{N}| \leq |X| \leq |Y| \leq |X \to \mathbb{P}| \to |Y| \leq |X| \vee |X \to \mathbb{P}| \leq |Y|$$

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Represent GCH and AC in Coq by the following propositions:

$$\forall XY : \mathbb{T}.\, |\mathbb{N}| \leq |X| \leq |Y| \leq |X \to \mathbb{P}| \to |Y| \leq |X| \vee |X \to \mathbb{P}| \leq |Y|$$

$$\forall R.\, (\forall x.\, \exists y.\, Rxy) \to \exists f.\, \forall x.\, Rx(fx)$$

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Represent GCH and AC in Coq by the following propositions:

$$\forall XY : \mathbb{T}.\, |\mathbb{N}| \leq |X| \leq |Y| \leq |X \to \mathbb{P}| \to |Y| \leq |X| \lor |X \to \mathbb{P}| \leq |Y|$$

$$\forall R.\, (\forall x.\, \exists y.\, Rxy) \to \exists f.\, \forall x.\, Rx(fx)$$

Variant 2: Synthetic Set Theory

Some abstract set-theoretic results apply to dependent type theories, e.g. the equivalence of WO and AC (cf. Ilik (2006); Smolka et al. (2015))

Coq's type theory with impredicative universe $\mathbb{P}$ of propositions:

- Type of predicates $X \to \mathbb{P}$ represents the power set of X
- Anonymous propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ available
- Propositional cardinality comparisons: existence of injective functions
- Consistent with unique choice (UC) hard-wired in set theory

Represent GCH and AC in Coq by the following propositions:

$$\forall XY : \mathbb{T}.\, |\mathbb{N}| \leq |X| \leq |Y| \leq |X \to \mathbb{P}| \to |Y| \leq |X| \vee |X \to \mathbb{P}| \leq |Y|$$

$$\forall XY : \mathbb{T}.\, \forall (R : X \to Y \to \mathbb{P}).\, (\forall x.\, \exists y.\, Rxy) \to \exists (f : X \to Y).\, \forall x.\, Rx(fx)$$

Three Levels of Set Theory in Coq

	First-Order ZF	Higher-Order ZF	Type Theory
Power sets	$\mathcal{P}(A)$		$X \to \mathbb{P}$
Numbers	ω	-	$\mathbb{N}$
Relations	$\mathcal{P}(A \times B)$	both coincide	$X \to Y \to \mathbb{P}$
Functions	$\{f \subseteq A \times B \mid \dots\}$	-	$X \to Y$
Cardinality	$\exists f \subseteq A \times B \dots$		$\exists f : X \to Y \dots$
Orderings	$\exists R \subseteq A \times A \dots$		$\exists R : X \to X \to \mathbb{P} \dots$

Three Levels of Set Theory in Coq

	First-Order ZF	Higher-Order ZF	Type Theory
Power sets	$\mathcal{P}(A)$		$X \to \mathbb{P}$
Numbers	ω	-	$\mathbb{N}$
Relations	$\mathcal{P}(A \times B)$	both coincide	$X \to Y \to \mathbb{P}$
Functions	$\{f \subseteq A \times B \mid \dots\}$	-	$X \to Y$
Cardinality	$\exists f \subseteq A \times B \dots$		$\exists f : X \to Y \dots$
Orderings	$\exists R \subseteq A \times A \dots$		$\exists R : X \to X \to \mathbb{P} \dots$

Rephrasing Quine: *"Higher-order ZF is type theory in sheep's clothing."*

Summary of our Paper

Sierpiński's theorem already mechanised in Metamath by Carneiro (2015) based on a library of first-order ZF, we synthesise 3 alternatives in Coq:

- Coq* mechanisation based on higher-order ZF (2700loc)
- Adaptation to Coq* itself assuming unique choice (1400loc)
- Variant without unique choice (300loc on top)

*extended with functional and propositional extensionality as well as excluded middle

Summary of our Paper

Sierpiński's theorem already mechanised in Metamath by Carneiro (2015) based on a library of first-order ZF, we synthesise 3 alternatives in Coq:

- Coq* mechanisation based on higher-order ZF (2700loc)
- Adaptation to Coq* itself assuming unique choice (1400loc)
- Variant without unique choice (300loc on top)

Coq as a proof-assistant well-suited:

- Axiomatic freedom (classical logic, extensionality)
- Helpful features (type classes, setoid rewriting, auto rewriting)

*extended with functional and propositional extensionality as well as excluded middle

Summary of our Paper

Sierpiński's theorem already mechanised in Metamath by Carneiro (2015) based on a library of first-order ZF, we synthesise 3 alternatives in Coq:

- Coq* mechanisation based on higher-order ZF (2700loc)
- Adaptation to Coq* itself assuming unique choice (1400loc)
- Variant without unique choice (300loc on top)

Coq as a proof-assistant well-suited:

- Axiomatic freedom (classical logic, extensionality)
- Helpful features (type classes, setoid rewriting, auto rewriting)

`https://www.ps.uni-saarland.de/extras/sierpinski`

*extended with functional and propositional extensionality as well as excluded middle

First Half in Higher-Order ZF

Higher-Order ZF Set Theory

Work in a model $(\mathcal{S}, \in, \{\_, \_\}, \bigcup, \mathcal{P}, \emptyset, \omega)$.

Higher-Order ZF Set Theory

Work in a model $(\mathcal{S}, \in, \{\_, \_\}, \bigcup, \mathcal{P}, \emptyset, \omega)$.

Replace three of the usual first-order axioms by stronger versions:

Higher-Order ZF Set Theory

Work in a model $(\mathcal{S}, \in, \{\_,\_\}, \bigcup, \mathcal{P}, \emptyset, \omega)$.

Replace three of the usual first-order axioms by stronger versions:

$$\forall A.\, \mathsf{WF}_{\in}\, A \qquad \text{(Foundation)}$$

$$\forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x = \sigma^n(\emptyset) \qquad \text{(Infinity)}$$

$$\lambda y.\, \exists x \in A.\, R\, x\, y \;\text{ is a set for all functional } R \qquad \text{(Replacement)}$$

Higher-Order ZF Set Theory

Work in a model $(\mathcal{S}, \in, \{\_, \_\}, \bigcup, \mathcal{P}, \emptyset, \omega)$.

Replace three of the usual first-order axioms by stronger versions:

$$\forall A.\, \mathsf{WF}_{\in}\, A \qquad \text{(Foundation)}$$

$$\forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x = \sigma^n(\emptyset) \qquad \text{(Infinity)}$$

$$\lambda y.\, \exists x \in A.\, R\, x\, y \ \text{ is a set for all functional } R \qquad \text{(Replacement)}$$

Higher-order replacement yields a unique choice operator:

Higher-Order ZF Set Theory

Work in a model $(\mathcal{S}, \in, \{\_,\_\}, \bigcup, \mathcal{P}, \emptyset, \omega)$.

Replace three of the usual first-order axioms by stronger versions:

$$\forall A.\, \mathsf{WF}_\in\, A \qquad \text{(Foundation)}$$

$$\forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x = \sigma^n(\emptyset) \qquad \text{(Infinity)}$$

$$\lambda y.\, \exists x \in A.\, R\,x\,y \;\text{ is a set for all functional } R \qquad \text{(Replacement)}$$

Higher-order replacement yields a unique choice operator:

$$\delta : \;\forall p : \mathcal{S} \to \mathbb{P}.\, (\exists! A.\, pA) \to \Sigma A.\, pA$$

$$\delta p := \bigcup \{ y \mid \exists x \in \mathcal{P}(\emptyset).\, py \}$$

Higher-Order ZF Set Theory

Work in a model $(\mathcal{S}, \in, \{\_,\_\}, \bigcup, \mathcal{P}, \emptyset, \omega)$.

Replace three of the usual first-order axioms by stronger versions:

$$\forall A.\, \mathsf{WF}_{\in}\, A \qquad \text{(Foundation)}$$

$$\forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x = \sigma^n(\emptyset) \qquad \text{(Infinity)}$$

$$\lambda y.\, \exists x \in A.\, R\,x\,y \;\text{ is a set for all functional } R \qquad \text{(Replacement)}$$

Higher-order replacement yields a unique choice operator:

$$\delta : \;\forall p : \mathcal{S} \to \mathbb{P}.\, (\exists! A.\, pA) \to \Sigma A.\, pA$$

$$\delta p := \bigcup \{ y \mid \exists x \in \mathcal{P}(\emptyset).\, py \}$$

Collapses total functional relations and functions on $\mathcal{S}$ as expected!

Inductive Ordinals*

Definition

A set x is transitive if every element is a subset ($z \in y \in x \to z \in x$).

*Gert Smolka (2016); Smullyan and Fitting (2010)

Inductive Ordinals*

Definition

A set x is transitive if every element is a subset ($z \in y \in x \to z \in x$).

The class $\mathcal{O} : \mathcal{S} \to \mathbb{P}$ of ordinals can be defined inductively by a single rule:

$$\frac{\alpha \subseteq \mathcal{O} \quad \text{transitive}\,\alpha}{\alpha \in \mathcal{O}}$$

*Gert Smolka (2016); Smullyan and Fitting (2010)

Inductive Ordinals*

Definition

A set x is transitive if every element is a subset ($z \in y \in x \to z \in x$).

The class $\mathcal{O} : \mathcal{S} \to \mathbb{P}$ of ordinals can be defined inductively by a single rule:

$$\frac{\alpha \subseteq \mathcal{O} \quad \text{transitive}\, \alpha}{\alpha \in \mathcal{O}}$$

Equivalently, one can characterise $\mathcal{O}$ with 3 rules unveiling constructors:

$$\frac{}{\emptyset \in \mathcal{O}} \qquad \frac{\alpha \in \mathcal{O}}{\sigma(\alpha) \in \mathcal{O}} \qquad \frac{\lambda \subseteq \mathcal{O} \quad (\bigcup \lambda \subseteq \lambda)}{\bigcup \lambda \in \mathcal{O}}$$

*Gert Smolka (2016); Smullyan and Fitting (2010)

Inductive Ordinals*

Definition

A set x is transitive if every element is a subset ($z \in y \in x \to z \in x$).

The class $\mathcal{O} : \mathcal{S} \to \mathbb{P}$ of ordinals can be defined inductively by a single rule:

$$\frac{\alpha \subseteq \mathcal{O} \quad \text{transitive}\,\alpha}{\alpha \in \mathcal{O}}$$

Equivalently, one can characterise $\mathcal{O}$ with 3 rules unveiling constructors:

$$\frac{}{\emptyset \in \mathcal{O}} \qquad \frac{\alpha \in \mathcal{O}}{\sigma(\alpha) \in \mathcal{O}} \qquad \frac{\lambda \subseteq \mathcal{O} \quad (\bigcup \lambda \subseteq \lambda)}{\bigcup \lambda \in \mathcal{O}}$$

By simple induction on $\mathcal{O}$, one obtains the desired ordering properties:

Fact

Every ordinal is well-ordered by $\in$ and order-isomorphic ordinals are equal.

*Gert Smolka (2016); Smullyan and Fitting (2010)

Constructing Large Ordinals: $|\aleph(A)| \not\leq |A|$

Definition

The Hartogs number of a set A is the class $\aleph(A) := \lambda\alpha \in \mathcal{O}.\, |\alpha| \leq |A|$.

Constructing Large Ordinals: $|\aleph(A)| \not\leq |A|$

Definition

The Hartogs number of a set A is the class $\aleph(A) := \lambda\alpha \in \mathcal{O}.\, |\alpha| \leq |A|$.

Theorem

The Hartogs number $\aleph(A)$ of A satisfies the following properties:

1. $|\aleph(A)| \leq |\mathcal{P}^6(A)|$
2. $\aleph(A) \in \mathcal{O}$
3. $|\aleph(A)| \not\leq |A|$

Constructing Large Ordinals: $|\aleph(A)| \not\leq |A|$

Definition

The Hartogs number of a set A is the class $\aleph(A) := \lambda\alpha \in \mathcal{O}.\, |\alpha| \leq |A|$.

Theorem

The Hartogs number $\aleph(A)$ of A satisfies the following properties:

1. $|\aleph(A)| \leq |\mathcal{P}^6(A)|$
2. $\aleph(A) \in \mathcal{O}$
3. $|\aleph(A)| \not\leq |A|$

Proof.

Constructing Large Ordinals: $|\aleph(A)| \not\leq |A|$

Definition

The Hartogs number of a set A is the class $\aleph(A) := \lambda\alpha \in \mathcal{O}.\, |\alpha| \leq |A|$.

Theorem

The Hartogs number $\aleph(A)$ of A satisfies the following properties:

1. $|\aleph(A)| \leq |\mathcal{P}^6(A)|$
2. $\aleph(A) \in \mathcal{O}$
3. $|\aleph(A)| \not\leq |A|$

Proof.

1. By representing ordinals $|\alpha| \leq |A|$ as well-ordered subsets of A.

Constructing Large Ordinals: $|\aleph(A)| \not\leq |A|$

Definition

The Hartogs number of a set A is the class $\aleph(A) := \lambda\alpha \in \mathcal{O}.\, |\alpha| \leq |A|$.

Theorem

The Hartogs number $\aleph(A)$ of A satisfies the following properties:

1. $|\aleph(A)| \leq |\mathcal{P}^6(A)|$
2. $\aleph(A) \in \mathcal{O}$
3. $|\aleph(A)| \not\leq |A|$

Proof.

1. By representing ordinals $|\alpha| \leq |A|$ as well-ordered subsets of A.
2. Straightforward by definition of ordinals.

Constructing Large Ordinals: $|\aleph(A)| \not\leq |A|$

Definition

The Hartogs number of a set A is the class $\aleph(A) := \lambda\alpha \in \mathcal{O}.\, |\alpha| \leq |A|$.

Theorem

The Hartogs number $\aleph(A)$ of A satisfies the following properties:

1. $|\aleph(A)| \leq |\mathcal{P}^6(A)|$
2. $\aleph(A) \in \mathcal{O}$
3. $|\aleph(A)| \not\leq |A|$

Proof.

1. By representing ordinals $|\alpha| \leq |A|$ as well-ordered subsets of A.
2. Straightforward by definition of ordinals.
3. Straightforward by definition of $\aleph(A)$. □

Second Half in Coq's Type Theory

Small Ordinals in Type Theory

How to construct Hartogs numbers in Coq's type theory?
No canonical representation of well-orders as ordinals*

*without quotient axioms or univalence

Small Ordinals in Type Theory

How to construct Hartogs numbers in Coq's type theory?
No canonical representation of well-orders as ordinals*

Consider small ordinals representable in a given type X:

*without quotient axioms or univalence

Small Ordinals in Type Theory

How to construct Hartogs numbers in Coq's type theory?
No canonical representation of well-orders as ordinals*

Consider small ordinals representable in a given type X:

- Elements p of $\mathcal{P}(X) = X \to \mathbb{P}$ are subsets of X

*without quotient axioms or univalence

Small Ordinals in Type Theory

How to construct Hartogs numbers in Coq's type theory?
No canonical representation of well-orders as ordinals*

Consider small ordinals representable in a given type X:

- Elements p of $\mathcal{P}(X) = X \to \mathbb{P}$ are subsets of X
- Elements P of $\mathcal{P}^2(X)$ are sets of subsets, some of them are well-ordered by inclusion $p \subseteq q := \forall x.\, p\,x \to q\,x$

*without quotient axioms or univalence

Small Ordinals in Type Theory

How to construct Hartogs numbers in Coq's type theory?
No canonical representation of well-orders as ordinals*

Consider small ordinals representable in a given type X:

- Elements p of $\mathcal{P}(X) = X \to \mathbb{P}$ are subsets of X
- Elements P of $\mathcal{P}^2(X)$ are sets of subsets, some of them are well-ordered by inclusion $p \subseteq q := \forall x.\, p\,x \to q\,x$
- Elements α of $\mathcal{P}^3(X)$ are classes of sets of subsets, we call the ones that are equivalence classes of well-ordered P small ordinals

*without quotient axioms or univalence

Small Ordinals in Type Theory

How to construct Hartogs numbers in Coq's type theory?
No canonical representation of well-orders as ordinals*

Consider small ordinals representable in a given type X:

- Elements p of $\mathcal{P}(X) = X \to \mathbb{P}$ are subsets of X
- Elements P of $\mathcal{P}^2(X)$ are sets of subsets, some of them are well-ordered by inclusion $p \subseteq q := \forall x.\, p\, x \to q\, x$
- Elements α of $\mathcal{P}^3(X)$ are classes of sets of subsets, we call the ones that are equivalence classes of well-ordered P small ordinals
- $H(X)$ is defined as the subtype of small ordinals α

*without quotient axioms or univalence

Small Ordinals in Type Theory

How to construct Hartogs numbers in Coq's type theory?
No canonical representation of well-orders as ordinals*

Consider small ordinals representable in a given type X:

- Elements p of $\mathcal{P}(X) = X \to \mathbb{P}$ are subsets of X
- Elements P of $\mathcal{P}^2(X)$ are sets of subsets, some of them are well-ordered by inclusion $p \subseteq q := \forall x.\, p\,x \to q\,x$
- Elements α of $\mathcal{P}^3(X)$ are classes of sets of subsets, we call the ones that are equivalence classes of well-ordered P small ordinals
- $H(X)$ is defined as the subtype of small ordinals α

Theorem

$H(X)$ is well-ordered and satisfies $|H(X)| \not\leq |X|$ and $|H(X)| \leq |\mathcal{P}^3(X)|$.

---

*without quotient axioms or univalence

Sierpiński's Theorem - Proof

Theorem

GCH implies AC.

Sierpiński's Theorem - Proof

Theorem

GCH implies AC.

Proof.

Sierpiński's Theorem - Proof

Theorem

GCH implies AC.

Proof.

Assume GCH, it suffices to show that every infinite type is well-orderable.

Sierpiński's Theorem - Proof

Theorem

GCH implies AC.

Proof.

Assume GCH, it suffices to show that every infinite type is well-orderable. So for some infinite X, apply GCH to the situation obtained by Lemma 1:

$$|\mathcal{P}^2(X)| \leq |\mathcal{P}^2(X) + H(X)| \leq |\mathcal{P}^3(X)|$$

Lemma 1

If X is infinite, then $|X| = |\mathbb{1} + X|$ and $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$.

Sierpiński's Theorem - Proof

Theorem

GCH implies AC.

Proof.

Assume GCH, it suffices to show that every infinite type is well-orderable. So for some infinite X, apply GCH to the situation obtained by Lemma 1:

$$|\mathcal{P}^2(X)| \leq |\mathcal{P}^2(X) + H(X)| \leq |\mathcal{P}^3(X)|$$

- $|\mathcal{P}^2(X) + H(X)| \leq |\mathcal{P}^2(X)|$ yields $|H(X)| \leq |\mathcal{P}^2(X)|$, start again

Lemma 1

If X is infinite, then $|X| = |\mathbb{1} + X|$ and $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$.

Sierpiński's Theorem - Proof

Theorem

GCH implies AC.

Proof.

Assume GCH, it suffices to show that every infinite type is well-orderable. So for some infinite X, apply GCH to the situation obtained by Lemma 1:

$$|\mathcal{P}^2(X)| \leq |\mathcal{P}^2(X) + H(X)| \leq |\mathcal{P}^3(X)|$$

- $|\mathcal{P}^2(X) + H(X)| \leq |\mathcal{P}^2(X)|$ yields $|H(X)| \leq |\mathcal{P}^2(X)|$, start again
- $|\mathcal{P}^3(X)| \leq |\mathcal{P}^2(X) + H(X)|$ yields $|\mathcal{P}^3(X)| \leq |H(X)|$ by Lemma 2 $\square$

Lemma 2

If $|\mathcal{P}(X)| \leq |X + Y|$ *and* $|X + X| \leq |X|$, *then already* $|\mathcal{P}(X)| \leq |Y|$.

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\mathsf{UC} := \forall X. \forall p : X \to \mathbb{P}. (\exists! x. px) \to \Sigma x. px$$

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\mathsf{UC} \;:=\; \forall X.\, \forall p : X \to \mathbb{P}.\, (\exists! x.\, px) \to \Sigma x.\, px$$

Given types X, Y, a predicate $p : X \to \mathbb{P}$, and an injection $f : X \to Y$:

$$|\mathbb{N}| = |\mathbb{1} + \mathbb{N}| \qquad |\mathbb{B}| \overset{\mathsf{UC}}{=} |\mathbb{P}|$$

$$|X + X| = |\mathbb{B} \times X| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma x. px + \Sigma x.\, \neg px|$$

$$|\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma y.\, \exists x.\, y = fx|$$

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\mathsf{UC} \;:=\; \forall X.\, \forall p : X \to \mathbb{P}.\, (\exists! x.\, px) \to \Sigma x.\, px$$

Given types X, Y, a predicate $p : X \to \mathbb{P}$, and an injection $f : X \to Y$:

$$|\mathbb{N}| = |\mathbb{1} + \mathbb{N}| \qquad |\mathbb{B}| \overset{\mathsf{UC}}{=} |\mathbb{P}|$$

$$|X + X| = |\mathbb{B} \times X| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma x. px + \Sigma x.\, \neg px|$$

$$|\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma y.\, \exists x.\, y = fx|$$

Lemma 1

If X is infinite, then $|X| \overset{\mathsf{UC}}{=} |\mathbb{1} + X|$ and $|\mathcal{P}(X)| \overset{\mathsf{UC}}{=} |\mathcal{P}(X) + \mathcal{P}(X)|$.

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\text{UC} \;:=\; \forall X.\, \forall p : X \to \mathbb{P}.\, (\exists! x.\, px) \to \Sigma x.\, px$$

Given types X, Y, a predicate $p : X \to \mathbb{P}$, and an injection $f : X \to Y$:

$$|\mathbb{N}| = |\mathbb{1} + \mathbb{N}| \qquad |\mathbb{B}| \overset{\text{UC}}{=} |\mathbb{P}|$$

$$|X + X| = |\mathbb{B} \times X| \qquad |X| \overset{\text{UC}}{=} |\Sigma x.px + \Sigma x.\, \neg px|$$

$$|\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)| \qquad |X| \overset{\text{UC}}{=} |\Sigma y.\, \exists x.\, y = fx|$$

Lemma 1

If X is infinite, then $|X| \overset{\text{UC}}{=} |\mathbb{1} + X|$ and $|\mathcal{P}(X)| \overset{\text{UC}}{=} |\mathcal{P}(X) + \mathcal{P}(X)|$.

Proof.

By equational reasoning, e.g. the former implies the latter as follows:

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\text{UC} := \forall X. \forall p : X \to \mathbb{P}. (\exists! x. px) \to \Sigma x. px$$

Given types X, Y, a predicate $p : X \to \mathbb{P}$, and an injection $f : X \to Y$:

$$|\mathbb{N}| = |\mathbb{1} + \mathbb{N}| \qquad |\mathbb{B}| \overset{\text{UC}}{=} |\mathbb{P}|$$

$$|X + X| = |\mathbb{B} \times X| \qquad |X| \overset{\text{UC}}{=} |\Sigma x.px + \Sigma x. \neg px|$$

$$|\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)| \qquad |X| \overset{\text{UC}}{=} |\Sigma y. \exists x. y = fx|$$

Lemma 1

If X is infinite, then $|X| \overset{\text{UC}}{=} |\mathbb{1} + X|$ and $|\mathcal{P}(X)| \overset{\text{UC}}{=} |\mathcal{P}(X) + \mathcal{P}(X)|$.

Proof.

By equational reasoning, e.g. the former implies the latter as follows:
$|\mathcal{P}(X)| \overset{\text{UC}}{=} |\mathcal{P}(\mathbb{1}+X)|$

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\text{UC} := \forall X.\, \forall p : X \to \mathbb{P}.\, (\exists! x.\, px) \to \Sigma x.\, px$$

Given types X, Y, a predicate $p : X \to \mathbb{P}$, and an injection $f : X \to Y$:

$$|\mathbb{N}| = |\mathbb{1} + \mathbb{N}| \qquad |\mathbb{B}| \overset{\text{UC}}{=} |\mathbb{P}|$$

$$|X + X| = |\mathbb{B} \times X| \qquad |X| \overset{\text{UC}}{=} |\Sigma x.px + \Sigma x.\, \neg px|$$

$$|\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)| \qquad |X| \overset{\text{UC}}{=} |\Sigma y.\, \exists x.\, y = fx|$$

Lemma 1

If X is infinite, then $|X| \overset{\text{UC}}{=} |\mathbb{1} + X|$ and $|\mathcal{P}(X)| \overset{\text{UC}}{=} |\mathcal{P}(X) + \mathcal{P}(X)|$.

Proof.

By equational reasoning, e.g. the former implies the latter as follows:
$|\mathcal{P}(X)| \overset{\text{UC}}{=} |\mathcal{P}(\mathbb{1}+X)| = |\mathcal{P}(\mathbb{1})\times\mathcal{P}(X)|$

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\mathsf{UC} := \forall X. \forall p : X \to \mathbb{P}. (\exists! x.\, px) \to \Sigma x.\, px$$

Given types X, Y, a predicate $p : X \to \mathbb{P}$, and an injection $f : X \to Y$:

$$|\mathbb{N}| = |\mathbb{1} + \mathbb{N}| \qquad |\mathbb{B}| \overset{\mathsf{UC}}{=} |\mathbb{P}|$$

$$|X + X| = |\mathbb{B} \times X| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma x. px + \Sigma x. \neg px|$$

$$|\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma y. \exists x. y = fx|$$

Lemma 1

If X is infinite, then $|X| \overset{\mathsf{UC}}{=} |\mathbb{1} + X|$ and $|\mathcal{P}(X)| \overset{\mathsf{UC}}{=} |\mathcal{P}(X) + \mathcal{P}(X)|$.

Proof.

By equational reasoning, e.g. the former implies the latter as follows:
$|\mathcal{P}(X)| \overset{\mathsf{UC}}{=} |\mathcal{P}(\mathbb{1}+X)| = |\mathcal{P}(\mathbb{1})\times\mathcal{P}(X)| \overset{\mathsf{UC}}{=} |\mathbb{B}\times\mathcal{P}(X)|$

Infinite Types: $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$

$$\mathsf{UC} \;:=\; \forall X.\, \forall p : X \to \mathbb{P}.\, (\exists! x.\, px) \to \Sigma x.\, px$$

Given types X, Y, a predicate $p : X \to \mathbb{P}$, and an injection $f : X \to Y$:

$$|\mathbb{N}| = |\mathbb{1} + \mathbb{N}| \qquad |\mathbb{B}| \overset{\mathsf{UC}}{=} |\mathbb{P}|$$

$$|X + X| = |\mathbb{B} \times X| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma x. px + \Sigma x. \neg px|$$

$$|\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)| \qquad |X| \overset{\mathsf{UC}}{=} |\Sigma y.\, \exists x.\, y = fx|$$

Lemma 1

If X is infinite, then $|X| \overset{\mathsf{UC}}{=} |\mathbb{1} + X|$ and $|\mathcal{P}(X)| \overset{\mathsf{UC}}{=} |\mathcal{P}(X) + \mathcal{P}(X)|$.

Proof.

By equational reasoning, e.g. the former implies the latter as follows:
$|\mathcal{P}(X)| \overset{\mathsf{UC}}{=} |\mathcal{P}(\mathbb{1}+X)| = |\mathcal{P}(\mathbb{1}) \times \mathcal{P}(X)| \overset{\mathsf{UC}}{=} |\mathbb{B} \times \mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$ □

Eliminating Unique Choice

1. Introduce weaker notions $|X| \leq_r |Y|$ and $|X| =_r |Y|$ based on injective and invertible total functional relations instead of functions

Eliminating Unique Choice

1. Introduce weaker notions $|X| \leq_r |Y|$ and $|X| =_r |Y|$ based on injective and invertible total functional relations instead of functions
2. Obtain the critical relational bijection without UC:

$$|\mathcal{P}(X)| =_r |\mathcal{P}(X) + \mathcal{P}(X)|$$

Eliminating Unique Choice

1. Introduce weaker notions $|X| \leq_r |Y|$ and $|X| =_r |Y|$ based on injective and invertible total functional relations instead of functions
2. Obtain the critical relational bijection without UC:

$$|\mathcal{P}(X)| =_r |\mathcal{P}(X) + \mathcal{P}(X)|$$

3. Consider respective reformulations GCH' and AC':

Eliminating Unique Choice

1. Introduce weaker notions $|X| \leq_r |Y|$ and $|X| =_r |Y|$ based on injective and invertible total functional relations instead of functions
2. Obtain the critical relational bijection without UC:

$$|\mathcal{P}(X)| =_r |\mathcal{P}(X) + \mathcal{P}(X)|$$

3. Consider respective reformulations GCH' and AC':

$$\forall XY.\, |\mathbb{N}| \leq |X| \leq_r |Y| \leq_r |\mathcal{P}(X)| \rightarrow |Y| \leq_r |X| \vee |\mathcal{P}(X)| \leq_r |Y|$$

Eliminating Unique Choice

1. Introduce weaker notions $|X| \leq_r |Y|$ and $|X| =_r |Y|$ based on injective and invertible total functional relations instead of functions
2. Obtain the critical relational bijection without UC:

$$|\mathcal{P}(X)| =_r |\mathcal{P}(X) + \mathcal{P}(X)|$$

3. Consider respective reformulations GCH' and AC':

$$\forall XY.\, |\mathbb{N}| \leq |X| \leq_r |Y| \leq_r |\mathcal{P}(X)| \to |Y| \leq_r |X| \lor |\mathcal{P}(X)| \leq_r |Y|$$

$$\forall XY.\, \forall R : X \to Y \to \mathbb{P}.\, (\forall x.\, \exists y.\, Rxy) \to \exists R' \subseteq R.\, \forall x.\, \exists! y.\, R'xy$$

Eliminating Unique Choice

1. Introduce weaker notions $|X| \leq_r |Y|$ and $|X| =_r |Y|$ based on injective and invertible total functional relations instead of functions

2. Obtain the critical relational bijection without UC:

$$|\mathcal{P}(X)| =_r |\mathcal{P}(X) + \mathcal{P}(X)|$$

3. Consider respective reformulations GCH' and AC':

$$\forall XY.\, |\mathbb{N}| \leq |X| \leq_r |Y| \leq_r |\mathcal{P}(X)| \rightarrow |Y| \leq_r |X| \vee |\mathcal{P}(X)| \leq_r |Y|$$

$$\forall XY.\, \forall R : X \rightarrow Y \rightarrow \mathbb{P}.\, (\forall x.\, \exists y.\, Rxy) \rightarrow \exists R' \subseteq R.\, \forall x.\, \exists! y.\, R'xy$$

Theorem

GCH' implies AC'.

Wrap-Up

Take-Homes

Three ways to mechanise set-theoretic results in type-theoretic systems:

- First-order axiomatisation unavoidable for meta-theoretic results
- Higher-order axiomatisation available for internal results
- Type-level structure sometimes sufficient for abstract results

Take-Homes

Three ways to mechanise set-theoretic results in type-theoretic systems:

- First-order axiomatisation unavoidable for meta-theoretic results
- Higher-order axiomatisation available for internal results
- Type-level structure sometimes sufficient for abstract results

In this setting, higher-order ZF is a bridge between both worlds:

- Explicit set-theoretic primitives and notions
- Inheritance of type-theoretic structure
- Convenient to work with, especially without library support

Open Questions

- How constructive is the main GCH to AC implication?
  - Mostly needed for ordering properties (linearity, WF)
  - Maybe factoring through the classical WO not necessary
  - Would show that GCH implies excluded middle

Open Questions

- How constructive is the main GCH to AC implication?
  - Mostly needed for ordering properties (linearity, WF)
  - Maybe factoring through the classical WO not necessary
  - Would show that GCH implies excluded middle
- What is the situation in other type theories?
  - MLTT: lacks a direct notion of propositional existence and power sets
  - Type theory with AC: renders Sierpiński's theorem vacuous
  - HoTT: probably a good target since FE, PE, and UC are provable

Open Questions

- How constructive is the main GCH to AC implication?
  - Mostly needed for ordering properties (linearity, WF)
  - Maybe factoring through the classical WO not necessary
  - Would show that GCH implies excluded middle
- What is the situation in other type theories?
  - MLTT: lacks a direct notion of propositional existence and power sets
  - Type theory with AC: renders Sierpiński's theorem vacuous
  - HoTT: probably a good target since FE, PE, and UC are provable
- How connected are GCH on type-level and in the set-level model?
  - Certainly the former implies the latter
  - Converse implication probably independent

Bibliography

Carneiro, M. (2015). GCH implies AC, a Metamath Formalization. In *8th Conference on Intelligent Computer Mathematics*, Workshop on Formal Mathematics for Mathematicians.

Gert Smolka (2016). Lecture Notes in Computational Logic II. `https://courses.ps.uni-saarland.de/cl2_16/`.

Gillman, L. (2002). Two classical surprises concerning the axiom of choice and the continuum hypothesis. *The American Mathematical Monthly*, 109(6):544–553.

Ilik, D. (2006). Zermelo's well-ordering theorem in type theory. In *International Workshop on Types for Proofs and Programs*, pages 175–187. Springer.

Kirst, D. and Smolka, G. (2018). Categoricity results and large model constructions for second-order zf in dependent type theory. *Journal of Automated Reasoning*. First Online: 11 October 2018.

Sierpiński, W. (1947). L'hypothèse généralisée du continu et l'axiome du choix. *Fundamenta Mathematicae*, 1(34):1–5.

Smolka, G., Schäfer, S., and Doczkal, C. (2015). Transfinite constructions in classical type theory. In *International Conference on Interactive Theorem Proving*, pages 391–404. Springer.

Smullyan, R. M. and Fitting, M. (2010). *Set theory and the continuum problem*. Dover Publications.

Specker, E. (1990). Verallgemeinerte Kontinuumshypothese und Auswahlaxiom. In Jäger, G., Läuchli, H., Scarpellini, B., and Strassen, V., editors, *Ernst Specker Selecta*, pages 86–91. Birkhäuser, Basel.