The Generalised Continuum Hypothesis Implies the Axiom of Choice in HoTT

Dominik Kirst and Felix Rech

Workshop on Homotopy Type Theory / Univalent Foundations
July 18, 2021

SAARLAND UNIVERSITY
COMPUTER SCIENCE
SIC Saarland Informatics Campus

The Generalised Continuum Hypothesis Implies the Axiom of Choice in ZF

The Generalised Continuum Hypothesis Implies the Axiom of Choice in ZF

There are no cardinalities between an infinite set and its power set (GCH)

$\Downarrow$

Every set has a choice function / can be well-ordered (AC/WO)

The Generalised Continuum Hypothesis Implies the Axiom of Choice in ZF

There are no cardinalities between an infinite set and its power set (GCH)

$\Downarrow$

Every set has a choice function / can be well-ordered (AC/WO)

- Result in ZF set theory announced by Lindenbaum and Tarski (1926)
- First published proof by Sierpiński (1947)
- Refinement using GCH more locally by Specker (1990)

The Generalised Continuum Hypothesis Implies the Axiom of Choice in ZF

There are no cardinalities between an infinite set and its power set (GCH)

$\Downarrow$

Every set has a choice function / can be well-ordered (AC/WO)

- Result in ZF set theory announced by Lindenbaum and Tarski (1926)
- First published proof by Sierpiński (1947)
- Refinement using GCH more locally by Specker (1990)
- Mechanisation in Metamath by Carneiro (2015)
- Paper "GCH implies AC in Coq" by Kirst and Rech (2021)[1]
  - Two mechanised variants: higher-order ZF and Coq's type theory

[1] Mostly following Gillman (2002) and Smullyan and Fitting (2010).

Set Theory in Coq's Type Theory

Using impredicative universe $\mathbb{P}$ and propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ we have:

	ZF set theory	Coq's Type Theory
Membership	$x \in y$	$x : X \quad (\text{for } X : \mathbb{T})$
Power sets	$\mathcal{P}(A)$	$X \to \mathbb{P}$
Numbers	ω	$\mathbb{N}$
Cardinality	$\exists f \subseteq A \times B \ldots$	$\exists f : X \to Y \ldots$
Orderings	$\exists R \subseteq A \times A \ldots$	$\exists R : X \to X \to \mathbb{P} \ldots$

Set Theory in Coq's Type Theory

Using impredicative universe $\mathbb{P}$ and propositional existence $(\exists x.\, P\, x) : \mathbb{P}$ we have:

	ZF set theory	Coq's Type Theory
Membership	$x \in y$	$x : X \quad (\text{for } X : \mathbb{T})$
Power sets	$\mathcal{P}(A)$	$X \to \mathbb{P}$
Numbers	ω	$\mathbb{N}$
Cardinality	$\exists f \subseteq A \times B \ldots$	$\exists f : X \to Y \ldots$
Orderings	$\exists R \subseteq A \times A \ldots$	$\exists R : X \to X \to \mathbb{P} \ldots$

Axioms necessary to make Coq's type theory behave like set theory:

- Functional extensionality, to tame function space
- Propositonal extensionality, to tame predicate space
- Unique choice, to identify functions with total functional relations

Set Theory in Homotopy Type Theory

Using propositional resizing to represent propositions in $\Omega : \mathcal{U}_0$ we have:

	ZF set theory	Homotopy Type Theory
Membership	$x \in y$	$x : X \quad (\text{for } X : \text{hSet})$
Power sets	$\mathcal{P}(A)$	$X \to \Omega$
Numbers	ω	$\mathbb{N}$
Cardinality	$\exists f \subseteq A \times B \dots$	$\|\|\Sigma f : X \to Y \dots\|\|$
Orderings	$\exists R \subseteq A \times A \dots$	$\|\|\Sigma R : X \to X \to \Omega \dots\|\|$

Set Theory in Homotopy Type Theory

Using propositional resizing to represent propositions in $\Omega : \mathcal{U}_0$ we have:

	ZF set theory	Homotopy Type Theory
Membership	$x \in y$	$x : X \quad (\text{for } X : \text{hSet})$
Power sets	$\mathcal{P}(A)$	$X \to \Omega$
Numbers	ω	$\mathbb{N}$
Cardinality	$\exists f \subseteq A \times B \ldots$	$\|\|\Sigma f : X \to Y \ldots\|\|$
Orderings	$\exists R \subseteq A \times A \ldots$	$\|\|\Sigma R : X \to X \to \Omega \ldots\|\|$

Naturally suited to represent set theory:

- Functional extensionality: implied by univalence
- Propositonal extensionality: implied by univalence
- Unique choice: by the elimination principle of propositional truncation

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

> There are no cardinalities between an infinite set and its power set.

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

There are no cardinalities between an infinite set and its power set.

$$\forall XY : \text{hSet}.\ \mathbb{N} \leq X \leq Y \leq \mathcal{P}(X) \ \to\ Y \leq X \ +\ \mathcal{P}(X) \leq Y$$

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $\|\Sigma f : X \to Y.\, \text{injective}\, f\|$:

There are no cardinalities between an infinite set and its power set.

$$\forall XY : \text{hSet}.\ \mathbb{N} \leq X \leq Y \leq \mathcal{P}(X) \ \to \ Y \leq X \ + \ \mathcal{P}(X) \leq Y$$

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

There are no cardinalities between an infinite set and its power set.

$$\forall XY : \text{hSet}.\ \mathbb{N} \leq X \leq Y \leq \mathcal{P}(X) \to \ Y \leq X \ + \ \mathcal{P}(X) \leq Y$$

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\,\text{injective}\, f||$:

> There are no cardinalities between an infinite set and its power set.
>
> $$\forall XY : \text{hSet}.\ \mathbb{N} \leq X \leq Y \leq \mathcal{P}(X) \ \to\ Y \leq X \ +\ \mathcal{P}(X) \leq Y$$

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

There are no cardinalities between an infinite set and its power set.

$$\forall XY : \text{hSet}.\ \mathbb{N} \leq X \leq Y \leq \mathcal{P}(X) \ \to\ Y \leq X \ +\ \mathcal{P}(X) \leq Y$$

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

There are no cardinalities between an infinite set and its power set.

$$\forall XY : \text{hSet}.\ \mathbb{N} \leq X \leq Y \leq \mathcal{P}(X) \ \to \ Y \leq X \ + \ \mathcal{P}(X) \leq Y$$

- Proposition since concluding disjunction is exclusive (Cantor's theorem)

Formulating GCH in HoTT

With $X \leq Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

There are no cardinalities between an infinite set and its power set.

$$\forall XY : \text{hSet}.\ \mathbb{N} \leq X \leq Y \leq \mathcal{P}(X) \ \to \ Y \leq X \ + \ \mathcal{P}(X) \leq Y$$

- Proposition since concluding disjunction is exclusive (Cantor's theorem)
- Formulated positively since cardinalities aren't comparable without AC

Formulating GCH in HoTT

With $X \le Y$ as propositional cardinality comparison $||\Sigma f : X \to Y.\, \text{injective}\, f||$:

There are no cardinalities between an infinite set and its power set.

$$\forall XY : \text{hSet}.\ \mathbb{N} \le X \le Y \le \mathcal{P}(X) \ \to\ Y \le X \ +\ \mathcal{P}(X) \le Y$$

- Proposition since concluding disjunction is exclusive (Cantor's theorem)
- Formulated positively since cardinalities aren't comparable without AC
- Conclusion just the missing comparison, not yet the equivalence

GCH implies LEM

Already a weaker formulation of CH = GCH($\mathbb{N}$) implies the excluded middle (LEM):

Fact (cf. Bridges (2016))

$$(\forall X : \mathsf{hSet}.\, \mathbb{N} \leq X \leq \mathcal{P}(\mathbb{N}) \to X \leq \mathbb{N} + \mathcal{P}(\mathbb{N}) \leq X) \;\to\; \forall P : \mathsf{hProp}.\, P + \neg P$$

GCH implies LEM

Already a weaker formulation of CH = GCH($\mathbb{N}$) implies the excluded middle (LEM):

Fact (cf. Bridges (2016))

$$(\forall X : \mathsf{hSet}.\, \mathbb{N} \leq X \leq \mathcal{P}(\mathbb{N}) \to X \leq \mathbb{N} + \mathcal{P}(\mathbb{N}) \leq X) \;\to\; \forall P : \mathsf{hProp}.\, P + \neg P$$

Proof.

GCH implies LEM

Already a weaker formulation of CH = GCH($\mathbb{N}$) implies the excluded middle (LEM):

Fact (cf. Bridges (2016))

$$(\forall X : \mathsf{hSet}.\, \mathbb{N} \le X \le \mathcal{P}(\mathbb{N}) \to X \le \mathbb{N} + \mathcal{P}(\mathbb{N}) \le X) \;\to\; \forall P : \mathsf{hProp}.\, P + \neg P$$

Proof.

1. Given P : hProp, the set $X := \Sigma\, p : \mathcal{P}(\mathbb{N}).\, ||\text{singleton}\; p + (P + \neg P)||$ satisfies the premises.

GCH implies LEM

Already a weaker formulation of CH = GCH($\mathbb{N}$) implies the excluded middle (LEM):

Fact (cf. Bridges (2016))

$$(\forall X : \mathsf{hSet}.\, \mathbb{N} \leq X \leq \mathcal{P}(\mathbb{N}) \to X \leq \mathbb{N} + \mathcal{P}(\mathbb{N}) \leq X) \;\to\; \forall P : \mathsf{hProp}.\, P + \neg P$$

Proof.

1. Given P : hProp, the set $X := \Sigma\, p : \mathcal{P}(\mathbb{N}).\, ||\mathsf{singleton}\, p + (P + \neg P)||$ satisfies the premises.
2. We can even show $X \not\leq \mathbb{N}$, hence we obtain an injection $i : \mathcal{P}(\mathbb{N}) \to X$.

GCH implies LEM

Already a weaker formulation of CH = GCH($\mathbb{N}$) implies the excluded middle (LEM):

Fact (cf. Bridges (2016))

$(\forall X : \mathrm{hSet}.\, \mathbb{N} \leq X \leq \mathcal{P}(\mathbb{N}) \to X \leq \mathbb{N} + \mathcal{P}(\mathbb{N}) \leq X) \;\to\; \forall P : \mathrm{hProp}.\, P + \neg P$

Proof.

1. Given P : hProp, the set $X := \Sigma\, p : \mathcal{P}(\mathbb{N}).\, \|\mathrm{singleton}\, p + (P + \neg P)\|$ satisfies the premises.
2. We can even show $X \not\leq \mathbb{N}$, hence we obtain an injection $i : \mathcal{P}(\mathbb{N}) \to X$.
3. By a variant of Cantor's theorem there is $p : \mathcal{P}(\mathbb{N})$ such that $\pi_1(i\, p)$ is not a singleton.

GCH implies LEM

Already a weaker formulation of CH = GCH($\mathbb{N}$) implies the excluded middle (LEM):

Fact (cf. Bridges (2016))

$$(\forall X : \mathsf{hSet}.\, \mathbb{N} \le X \le \mathcal{P}(\mathbb{N}) \to X \le \mathbb{N} + \mathcal{P}(\mathbb{N}) \le X) \;\to\; \forall P : \mathsf{hProp}.\, P + \neg P$$

Proof.

1. Given P : hProp, the set $X := \Sigma\, p : \mathcal{P}(\mathbb{N}).\, ||\mathsf{singleton}\; p + (P + \neg P)||$ satisfies the premises.
2. We can even show $X \not\le \mathbb{N}$, hence we obtain an injection $i : \mathcal{P}(\mathbb{N}) \to X$.
3. By a variant of Cantor's theorem there is $p : \mathcal{P}(\mathbb{N})$ such that $\pi_1(i\, p)$ is not a singleton.
4. Thus $P + \neg P$ must be the case. □

GCH implies LEM

Already a weaker formulation of CH = GCH($\mathbb{N}$) implies the excluded middle (LEM):

Fact (cf. Bridges (2016))

$(\forall X : \mathsf{hSet}.\, \mathbb{N} \le X \le \mathcal{P}(\mathbb{N}) \to X \le \mathbb{N} + \mathcal{P}(\mathbb{N}) \le X) \;\to\; \forall P : \mathsf{hProp}.\, P + \neg P$

Proof.

1. Given P : hProp, the set $X := \Sigma\, p : \mathcal{P}(\mathbb{N}).\, ||\mathrm{singleton}\, p + (P + \neg P)||$ satisfies the premises.
2. We can even show $X \not\le \mathbb{N}$, hence we obtain an injection $i : \mathcal{P}(\mathbb{N}) \to X$.
3. By a variant of Cantor's theorem there is $p : \mathcal{P}(\mathbb{N})$ such that $\pi_1(i\, p)$ is not a singleton.
4. Thus $P + \neg P$ must be the case. □

So by classical reasoning, i.e. the Cantor-Bernstein theorem:

Corollary

GCH is equivalent to $\forall XY : \mathsf{hSet}.\, \mathbb{N} \le X \le Y \le \mathcal{P}(X) \;\to\; Y = X \;+\; Y = \mathcal{P}(X)$.

Proof Overview

Outline

1. Instead of AC, show the equivalent WO

Outline

1. Instead of AC, show the equivalent WO
2. To well-order X it suffices to find ordinal α with $X \leq \alpha$

Outline

1. Instead of AC, show the equivalent WO
2. To well-order X it suffices to find ordinal α with $X \leq \alpha$
3. Central construction: Hartogs number $\aleph(X)$

Outline

1. Instead of AC, show the equivalent WO
2. To well-order X it suffices to find ordinal α with $X \leq \alpha$
3. Central construction: Hartogs number $\aleph(X)$
   - Large ordinal: $\aleph(X) \not\leq X$

Outline

1. Instead of AC, show the equivalent WO
2. To well-order X it suffices to find ordinal α with $X \leq \alpha$
3. Central construction: Hartogs number $\aleph(X)$
   - Large ordinal: $\aleph(X) \not\leq X$
   - Controlled height: $\aleph(X) \leq \mathcal{P}^3(X)$

Outline

1. Instead of AC, show the equivalent WO
2. To well-order X it suffices to find ordinal α with $X \leq \alpha$
3. Central construction: Hartogs number $\aleph(X)$
   - Large ordinal: $\aleph(X) \not\leq X$
   - Controlled height: $\aleph(X) \leq \mathcal{P}^3(X)$
4. Develop cardinal arithmetic in the absence of AC

Outline

1. Instead of AC, show the equivalent WO
2. To well-order X it suffices to find ordinal α with $X \leq \alpha$
3. Central construction: Hartogs number $\aleph(X)$
   - Large ordinal: $\aleph(X) \nleq X$
   - Controlled height: $\aleph(X) \leq \mathcal{P}^3(X)$
4. Develop cardinal arithmetic in the absence of AC
5. Use GCH to iteratively squeeze in $\aleph(X)$ and obtain $X \leq \aleph(X)$

Constructive Ordinal Numbers (Chapter 10.3 of the HoTT book)

Definition

An ordinal is a set equipped with a well-founded, extensional, transitive, mere relation.

Constructive Ordinal Numbers (Chapter 10.3 of the HoTT book)

Definition

An ordinal is a set equipped with a well-founded, extensional, transitive, mere relation.

Properties needed for main result:

- Isomorphic ordinals are equal (instance of SIP)
- Type Ord of ordinals with natural ordering is an ordinal
- Every ordinal is isomorphic to its set of initial segments
- Ordinals satisfy trichotomy and have least elements (requiring LEM)

Constructive Ordinal Numbers (Chapter 10.3 of the HoTT book)

Definition

An ordinal is a set equipped with a well-founded, extensional, transitive, mere relation.

Properties needed for main result:

- Isomorphic ordinals are equal (instance of SIP)
- Type Ord of ordinals with natural ordering is an ordinal
- Every ordinal is isomorphic to its set of initial segments
- Ordinals satisfy trichotomy and have least elements (requiring LEM)

Also successor and limit ordinals mechanised but irrelevant for main result.

The Hartogs Number $\aleph(X)$ of a Set X, without AC

The Hartogs Number $\aleph(X)$ of a Set X, without AC

Definition

We define $\aleph'(X)$: Ord as the type of ordinals α with $\alpha \leq X$, ordered by the natural ordering.

The Hartogs Number $\aleph(X)$ of a Set X, without AC

Definition

We define $\aleph'(X)$: Ord as the type of ordinals α with $\alpha \leq X$, ordered by the natural ordering.

The ordinal $\aleph'(X)$ lives in a higher universe level than X, therefore need to resize:

The Hartogs Number $\aleph(X)$ of a Set X, without AC

Definition

We define $\aleph'(X)$: Ord as the type of ordinals α with $\alpha \leq X$, ordered by the natural ordering.

The ordinal $\aleph'(X)$ lives in a higher universe level than X, therefore need to resize:

Theorem

Using LEM, we obtain $\aleph(X)$ by resizing $\aleph'(X)$ along the canonical injection $\aleph'(X) \leq \mathcal{P}^3(X)$. Then $\aleph(X)$ is in the same universe as X and satisfies $\aleph(X) \leq \mathcal{P}^3(X)$ as well as $\aleph(X) \not\leq X$.

The Hartogs Number $\aleph(X)$ of a Set X, without AC

Definition

We define $\aleph'(X)$: Ord as the type of ordinals α with $\alpha \leq X$, ordered by the natural ordering.

The ordinal $\aleph'(X)$ lives in a higher universe level than X, therefore need to resize:

Theorem

Using LEM, we obtain $\aleph(X)$ by resizing $\aleph'(X)$ along the canonical injection $\aleph'(X) \leq \mathcal{P}^3(X)$. Then $\aleph(X)$ is in the same universe as X and satisfies $\aleph(X) \leq \mathcal{P}^3(X)$ as well as $\aleph(X) \not\leq X$.

Proof.

The Hartogs Number $\aleph(X)$ of a Set X, without AC

Definition

We define $\aleph'(X)$: Ord as the type of ordinals α with $\alpha \leq X$, ordered by the natural ordering.

The ordinal $\aleph'(X)$ lives in a higher universe level than X, therefore need to resize:

Theorem

Using LEM, we obtain $\aleph(X)$ by resizing $\aleph'(X)$ along the canonical injection $\aleph'(X) \leq \mathcal{P}^3(X)$. Then $\aleph(X)$ is in the same universe as X and satisfies $\aleph(X) \leq \mathcal{P}^3(X)$ as well as $\aleph(X) \not\leq X$.

Proof.

1. Injection $i : \aleph'(X) \to \mathcal{P}^3(X)$ maps $\alpha \leq X$ to its induced order on X (using trichotomy).

The Hartogs Number $\aleph(X)$ of a Set X, without AC

Definition

We define $\aleph'(X)$: Ord as the type of ordinals α with $\alpha \leq X$, ordered by the natural ordering.

The ordinal $\aleph'(X)$ lives in a higher universe level than X, therefore need to resize:

Theorem

Using LEM, we obtain $\aleph(X)$ by resizing $\aleph'(X)$ along the canonical injection $\aleph'(X) \leq \mathcal{P}^3(X)$. Then $\aleph(X)$ is in the same universe as X and satisfies $\aleph(X) \leq \mathcal{P}^3(X)$ as well as $\aleph(X) \not\leq X$.

Proof.

1. Injection $i : \aleph'(X) \to \mathcal{P}^3(X)$ maps $\alpha \leq X$ to its induced order on X (using trichotomy).
2. Obtain $\aleph(X)$ as range of i with ordering of $\aleph'(X)$, then $\aleph(X) \leq \mathcal{P}^3(X)$ by construction.

The Hartogs Number $\aleph(X)$ of a Set X, without AC

Definition

We define $\aleph'(X)$: Ord as the type of ordinals α with $\alpha \leq X$, ordered by the natural ordering.

The ordinal $\aleph'(X)$ lives in a higher universe level than X, therefore need to resize:

Theorem

Using LEM, we obtain $\aleph(X)$ by resizing $\aleph'(X)$ along the canonical injection $\aleph'(X) \leq \mathcal{P}^3(X)$. Then $\aleph(X)$ is in the same universe as X and satisfies $\aleph(X) \leq \mathcal{P}^3(X)$ as well as $\aleph(X) \nleq X$.

Proof.

1. Injection $i : \aleph'(X) \to \mathcal{P}^3(X)$ maps $\alpha \leq X$ to its induced order on X (using trichotomy).
2. Obtain $\aleph(X)$ as range of i with ordering of $\aleph'(X)$, then $\aleph(X) \leq \mathcal{P}^3(X)$ by construction.
3. $\aleph(A) \nleq A$ since otherwise $\aleph(A)$ would be an initial segment of the isomorphic $\aleph'(A)$. □

Cardinal Arithmetic, without AC

With AC, infinite sets X satisfy $X \simeq X + X$.

Cardinal Arithmetic, without AC

With AC, infinite sets X satisfy $X \simeq X + X$. Without AC we get:

Lemma

Using LEM, every set X with $\mathbb{N} \leq X$ satisfies $X \simeq \mathbb{1} + X$ and $\mathcal{P}(X) \simeq \mathcal{P}(X) + \mathcal{P}(X)$.

Cardinal Arithmetic, without AC

With AC, infinite sets X satisfy $X \simeq X + X$. Without AC we get:

Lemma

Using LEM, every set X with $\mathbb{N} \leq X$ satisfies $X \simeq \mathbb{1} + X$ and $\mathcal{P}(X) \simeq \mathcal{P}(X) + \mathcal{P}(X)$.

Sketch.

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

$$\mathcal{P}(X) \overset{\text{LEM}}{\simeq} \mathcal{P}(\mathbb{1} + X) \simeq \mathcal{P}(\mathbb{1}) \times \mathcal{P}(X) \overset{\text{LEM}}{\simeq} \mathbb{B} \times \mathcal{P}(X) \simeq \mathcal{P}(X) + \mathcal{P}(X)$$

□

Cardinal Arithmetic, without AC

With AC, infinite sets X satisfy $X \simeq X + X$. Without AC we get:

Lemma

Using LEM, every set X with $\mathbb{N} \leq X$ satisfies $X \simeq \mathbb{1} + X$ and $\mathcal{P}(X) \simeq \mathcal{P}(X) + \mathcal{P}(X)$.

Sketch.

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

$$\mathcal{P}(X) \overset{\text{LEM}}{\simeq} \mathcal{P}(\mathbb{1} + X) \simeq \mathcal{P}(\mathbb{1}) \times \mathcal{P}(X) \overset{\text{LEM}}{\simeq} \mathbb{B} \times \mathcal{P}(X) \simeq \mathcal{P}(X) + \mathcal{P}(X)$$ □

Call X large enough if $X \simeq X + X$, then using Cantor's theorem once again:

Lemma

For sets X large enough and Y with $\mathcal{P}(X) \leq X + Y$ we obtain $\mathcal{P}(X) \leq Y$.

Cardinal Arithmetic, without AC

With AC, infinite sets X satisfy $X \simeq X + X$. Without AC we get:

Lemma

Using LEM, every set X with $\mathbb{N} \leq X$ satisfies $X \simeq \mathbb{1} + X$ and $\mathcal{P}(X) \simeq \mathcal{P}(X) + \mathcal{P}(X)$.

Sketch.

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

$$\mathcal{P}(X) \overset{\text{LEM}}{\simeq} \mathcal{P}(\mathbb{1} + X) \simeq \mathcal{P}(\mathbb{1}) \times \mathcal{P}(X) \overset{\text{LEM}}{\simeq} \mathbb{B} \times \mathcal{P}(X) \simeq \mathcal{P}(X) + \mathcal{P}(X)$$

□

Call X large enough if $X \simeq X + X$, then using Cantor's theorem once again:

Lemma

For sets X large enough and Y with $\mathcal{P}(X) \leq X + Y$ we obtain $\mathcal{P}(X) \leq Y$.

Sketch.

Obtain $i : \mathcal{P}(X) \times \mathcal{P}(X) \hookrightarrow X + Y$, use $\lambda p.\, i(p, c) : \mathcal{P}(X) \hookrightarrow Y$, c the diagonal set of i^{-1}. □

Iterate GCH to conclude $X \leq \aleph(X)$

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \mathrm{hSet}_i \to \mathrm{hSet}_i$ *such that there is* $k : \mathbb{N}$ *with* $F(X) \leq \mathcal{P}^k(X)$ *and* $F(X) \not\leq X$ *for all* X*. Then for every large enough set* X *we obtain* $X \leq F(X)$*.*

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \mathsf{hSet}_i \to \mathsf{hSet}_i$ *such that there is* $k : \mathbb{N}$ *with* $F(X) \leq \mathcal{P}^k(X)$ *and* $F(X) \nleq X$ *for all* X*. Then for every large enough set* X *we obtain* $X \leq F(X)$.

Proof.

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \mathsf{hSet}_i \to \mathsf{hSet}_i$ *such that there is* $k : \mathbb{N}$ *with* $F(X) \leq \mathcal{P}^k(X)$ *and* $F(X) \not\leq X$ *for all* X*. Then for every large enough set* X *we obtain* $X \leq F(X)$*.*

Proof.

Given a large enough set X, we show $X \leq F(X)$ by induction on k:

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \mathrm{hSet}_i \to \mathrm{hSet}_i$ *such that there is* $k : \mathbb{N}$ *with* $F(X) \leq \mathcal{P}^k(X)$ *and* $F(X) \nleq X$ *for all* X*. Then for every large enough set* X *we obtain* $X \leq F(X)$*.*

Proof.

Given a large enough set X, we show $X \leq F(X)$ by induction on k:

- If $k = 0$ the assumptions $F(X) \leq \mathcal{P}^k(X)$ and $F(X) \nleq X$ are contradictory.

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \mathrm{hSet}_i \to \mathrm{hSet}_i$ *such that there is* $k : \mathbb{N}$ *with* $F(X) \leq \mathcal{P}^k(X)$ *and* $F(X) \not\leq X$ *for all* X*. Then for every large enough set* X *we obtain* $X \leq F(X)$*.*

Proof.

Given a large enough set X, we show $X \leq F(X)$ by induction on k:

- If $k = 0$ the assumptions $F(X) \leq \mathcal{P}^k(X)$ and $F(X) \not\leq X$ are contradictory.
- For $k + 1$ apply GCH to the situation $\mathcal{P}^k(X) \ \leq \ \mathcal{P}^k(X) + F(X) \ \leq \ \mathcal{P}^{k+1}(X)$:

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \text{hSet}_i \to \text{hSet}_i$ such that there is $k : \mathbb{N}$ with $F(X) \leq \mathcal{P}^k(X)$ and $F(X) \not\leq X$ for all X. Then for every large enough set X we obtain $X \leq F(X)$.

Proof.

Given a large enough set X, we show $X \leq F(X)$ by induction on k:

- If $k = 0$ the assumptions $F(X) \leq \mathcal{P}^k(X)$ and $F(X) \not\leq X$ are contradictory.
- For $k + 1$ apply GCH to the situation $\mathcal{P}^k(X) \;\leq\; \mathcal{P}^k(X) + F(X) \;\leq\; \mathcal{P}^{k+1}(X)$:
  - If $\mathcal{P}^k(X) + F(X) \leq \mathcal{P}^k(X)$ then already $F(X) \leq \mathcal{P}^k(X)$, conclude with IH.

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \mathrm{hSet}_i \to \mathrm{hSet}_i$ *such that there is* $k : \mathbb{N}$ *with* $F(X) \leq \mathcal{P}^k(X)$ *and* $F(X) \not\leq X$ *for all* X*. Then for every large enough set* X *we obtain* $X \leq F(X)$*.*

Proof.

Given a large enough set X, we show $X \leq F(X)$ by induction on k:

- If $k = 0$ the assumptions $F(X) \leq \mathcal{P}^k(X)$ and $F(X) \not\leq X$ are contradictory.
- For $k + 1$ apply GCH to the situation $\mathcal{P}^k(X) \leq \mathcal{P}^k(X) + F(X) \leq \mathcal{P}^{k+1}(X)$:
  - If $\mathcal{P}^k(X) + F(X) \leq \mathcal{P}^k(X)$ then already $F(X) \leq \mathcal{P}^k(X)$, conclude with IH.
  - If $\mathcal{P}^{k+1}(X) \leq \mathcal{P}^k(X) + F(X)$ then already $\mathcal{P}^{k+1}(X) \leq F(X)$, conclude $X \leq F(X)$. □

Iterate GCH to conclude $X \leq \aleph(X)$

Theorem

Assume GCH and a function $F : \mathrm{hSet}_i \to \mathrm{hSet}_i$ such that there is $k : \mathbb{N}$ with $F(X) \leq \mathcal{P}^k(X)$ and $F(X) \not\leq X$ for all X. Then for every large enough set X we obtain $X \leq F(X)$.

Proof.

Given a large enough set X, we show $X \leq F(X)$ by induction on k:

- If $k = 0$ the assumptions $F(X) \leq \mathcal{P}^k(X)$ and $F(X) \not\leq X$ are contradictory.
- For $k + 1$ apply GCH to the situation $\mathcal{P}^k(X) \;\leq\; \mathcal{P}^k(X) + F(X) \;\leq\; \mathcal{P}^{k+1}(X)$:
  - If $\mathcal{P}^k(X) + F(X) \leq \mathcal{P}^k(X)$ then already $F(X) \leq \mathcal{P}^k(X)$, conclude with IH.
  - If $\mathcal{P}^{k+1}(X) \leq \mathcal{P}^k(X) + F(X)$ then already $\mathcal{P}^{k+1}(X) \leq F(X)$, conclude $X \leq F(X)$. □

Corollary

GCH implies AC.

Observations

Mechanisation Details

Mechanisation Details

Based on (and contributed to) the Coq HoTT library (Bauer et al. (2017))

- Cardinals, ordinals, Hartogs numbers, GCH $\to$ LEM, GCH $\to$ AC, 5 versions of Cantor
- 1400 lines in total (1300 relevant for result, 700 on ordinals, 250 on Hartogs number)
- Some code from previous development could be reused
- Easy to work with for pure Coq users (tactics, notations, typeclass for hProp)

Mechanisation Details

Based on (and contributed to) the Coq HoTT library (Bauer et al. (2017))

- Cardinals, ordinals, Hartogs numbers, GCH $\to$ LEM, GCH $\to$ AC, 5 versions of Cantor
- 1400 lines in total (1300 relevant for result, 700 on ordinals, 250 on Hartogs number)
- Some code from previous development could be reused
- Easy to work with for pure Coq users (tactics, notations, typeclass for hProp)

Only difficulties connected to power sets and universes:

- Resizing by hand tedious and sometimes very slow
- Power sets actually defined as $X \to$ hProp, only resized where needed
- Construction of $\aleph(X)$ in two parts for performance reasons
- Showing that power sets are sets caused universe conflicts with section usage

Comparison to Previous Coq Mechanisation

Comparison to Previous Coq Mechanisation

- Similar proofs concerning cardinal arithmetic and main theorem
  - Some necessary equivalences already in HoTT library

Comparison to Previous Coq Mechanisation

- Similar proofs concerning cardinal arithmetic and main theorem
  - Some necessary equivalences already in HoTT library
- Ordinals admit a better organized set-theoretic construction of $\aleph(X)$
  - Previous development based on "small" ordinals embeddable into X

Comparison to Previous Coq Mechanisation

- Similar proofs concerning cardinal arithmetic and main theorem
  - Some necessary equivalences already in HoTT library
- Ordinals admit a better organized set-theoretic construction of $\aleph(X)$
  - Previous development based on "small" ordinals embeddable into X
- Setoid rewriting could be avoided by univalence
  - No need for morphism lemmas like $|X| = |Y| \to |\mathcal{P}(X)| = |\mathcal{P}(Y)|$

Comparison to Previous Coq Mechanisation

- Similar proofs concerning cardinal arithmetic and main theorem
  - Some necessary equivalences already in HoTT library
- Ordinals admit a better organized set-theoretic construction of $\aleph(X)$
  - Previous development based on "small" ordinals embeddable into X
- Setoid rewriting could be avoided by univalence
  - No need for morphism lemmas like $|X| = |Y| \to |\mathcal{P}(X)| = |\mathcal{P}(Y)|$
- Overall code reduction from 1700loc to 1300loc relevant for main theorem
  - Code for $\aleph(X)$ more principled than previous ad-hoc construction

Comparison to Previous Coq Mechanisation

- Similar proofs concerning cardinal arithmetic and main theorem
  - Some necessary equivalences already in HoTT library
- Ordinals admit a better organized set-theoretic construction of $\aleph(X)$
  - Previous development based on "small" ordinals embeddable into X
- Setoid rewriting could be avoided by univalence
  - No need for morphism lemmas like $|X| = |Y| \to |\mathcal{P}(X)| = |\mathcal{P}(Y)|$
- Overall code reduction from 1700loc to 1300loc relevant for main theorem
  - Code for $\aleph(X)$ more principled than previous ad-hoc construction
- More satisfying theoretical foundation for set-theoretic results
  - Could dispose of the ad-hoc assumptions from previous development

Comparison to Previous Coq Mechanisation

- Similar proofs concerning cardinal arithmetic and main theorem
  - Some necessary equivalences already in HoTT library
- Ordinals admit a better organized set-theoretic construction of $\aleph(X)$
  - Previous development based on "small" ordinals embeddable into X
- Setoid rewriting could be avoided by univalence
  - No need for morphism lemmas like $|X| = |Y| \to |\mathcal{P}(X)| = |\mathcal{P}(Y)|$
- Overall code reduction from 1700loc to 1300loc relevant for main theorem
  - Code for $\aleph(X)$ more principled than previous ad-hoc construction
- More satisfying theoretical foundation for set-theoretic results
  - Could dispose of the ad-hoc assumptions from previous development
- Caveat: Coq users are used to static impredicativity
  - Hard to trace and debug implicitly added universe constraints

Open Questions

Could a static HProp universe be used instead of resizing by hand?

Open Questions

Could a static HProp universe be used instead of resizing by hand?

Is “light HoTT” combining weak univalence with UIP in static $\mathbb{P}$ useful?

Open Questions

Could a static HProp universe be used instead of resizing by hand?

Is "light HoTT" combining weak univalence with UIP in static $\mathbb{P}$ useful?

Are there meaningful/consistent formulations of GCH for higher n-types?

Open Questions

Could a static HProp universe be used instead of resizing by hand?

Is "light HoTT" combining weak univalence with UIP in static $\mathbb{P}$ useful?

Are there meaningful/consistent formulations of GCH for higher n-types?

Do constructive versions of GCH imply constructive versions of WO?

Bibliography

Bauer, A., Gross, J., Lumsdaine, P. L., Shulman, M., Sozeau, M., and Spitters, B. (2017). The HoTT Library: a formalization of homotopy type theory in Coq. In *Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 164–172.

Bridges, D. S. (2016). The continuum hypothesis implies excluded middle. *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, 6:111.

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

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

Kirst, D. and Rech, F. (2021). The generalised continuum hypothesis implies the axiom of choice in Coq. In *Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs*, pages 313–326.

Lindenbaum, A. and Tarski, A. (1926). *Communication sur les recherches de le théorie des ensembles*.

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

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.

Variants of Cantor's theorem

Fact (Injective Cantor)

Given a type X, there is no injection $\mathcal{P}(X) \leq X$.

Fact (Singleton Cantor)

Given a set X and an injection $i : \mathcal{P}(X) \to \mathcal{P}(X)$, there is p s.t. $i\,p$ is not a singleton.

Fact (Surjective Cantor)

Given a type X and a function $f : X \to \mathcal{P}(X)$, there is p s.t. $f\,x \neq p$ for all x.

Fact (Predicative Cantor)

Given a type X and a function $f : X \to (X \to \mathcal{U})$, there is p s.t. $f\,x \neq p$ for all x.

Fact (Relational Cantor)

Given a type X and a functional relation $R : X \to \mathcal{P}(X) \to \Omega$, there is p s.t. $\neg R\,x\,p$ for all x.