Axiom of Choice

Equivalents, Consequences, and Independence

Travor Liu, Yi Liu, Daya Singh, Tairan Wang

Department of Mathematics
University College London

June 6, 2023

Table of Contents

Partial Order

Definition

A relation R is a partial order on a set S iff

- Reflexivity: aRa for any $a \in S$.
- Anti-symmetry: If aRb and bRa, then $a = b$.
- Transitivity: If aRb and bRc, then aRc.

Examples

1. $(\mathbb{R}, \leq)$, where $\leq$ is the usual order.
2. $(\mathbb{N}, \leq)$, where $a \leq b$ iff $a|b$, called ordering by divisibility.

Totally Ordered Set and Well-Ordered Set

Definition

1. Let $(S, \leq)$ be partially ordered. S is totally ordered iff $\forall a, b \in S$ either $a \leq b$ or $b \leq a$.
2. Let $(S, \leq)$ be totally ordered. S is well-ordered iff every non-empty subset of S has a least element.

Examples

Let $\leq$ be the usual order. Then

1. $(\mathbb{R}, \leq)$ is totally ordered but not well-ordered.
2. $(\mathbb{N}, \leq)$ is well-ordered.

Maximum and Maximal Element

Definition

Let $(S, \leq)$ be a partially ordered set.

1. $m \in S$ is a maximal element of S iff m is greater than or equal to all elements comparable with m.
2. $M \in S$ is the maximum of S iff $\forall x \in S, x \leq M$.

Examples Let $(\mathbb{N}, \leq)$ be defined such that $a \leq b$ iff $b|a$. Then

1. 1 is the maximum of $(\mathbb{N}, \leq)$.
2. Prime numbers are the maximal elements of $(\mathbb{N} \setminus \{1\}, \leq)$.

Chain and Upper Bound

Definition

Let $(S, \leq)$ be a partially ordered set and $S' \subseteq S$.

1. $u \in S$ is an upper bound for S' iff $\forall x \in S', x \leq u$.
2. S' is a chain iff $(S', \leq)$ is a totally ordered.

Examples

Let $S = \mathbb{N}$, and $a \leq b$ iff. $a|b$.

1. $S_1 = \{1, 2, 3, 5, 12, 15\}$: 60 is an upper bound.
2. $S_2 = \{2^n | n \in \mathbb{N}\}$ is a chain.

Equivalence

The following statements are equivalent:

1. **Well-Ordering Theorem:** For any set S, there exists a relation R on S such that (S, R) is well-ordered.
2. **Axiom of Choice:** Let $\{A_i\}_{i \in I}$ be a family of non-empty sets indexed by I. Then there exists some f such that $f(A_i) \in A_i$ for all $i \in I$.
3. **Zorn's Lemma:** Let S be a non-empty partially ordered set. If every chain in S has an upper bound in S, then S contains a maximal element.

Applications to Linear Algebra

Theorem 2.1

Every nonzero vector space V contains a basis.

Proof.

Let S be the set of linearly independent subsets in V.

- S is non-empty.
- $(S, \subseteq)$ is partially ordered.
- Every chain of S has an upper bound in S.
- Zorn's Lemma $\implies$ S has a maximal element $\mathcal{B}$.
- $\mathcal{B}$ is a basis for V.

□

Applications to Linear Algebra

Corollary 2.2

Every spanning set of a nonzero vector space V contains a basis of V.

Proof.

Let S be a spanning set of V. Consider the set S' of linearly independent subsets of S.

- S' is nonempty. $(S', \subseteq)$ is partially ordered. Every chain of S' has an upper bound in S'.
- Zorn's lemma $\implies$ S' has a maximal element $\mathcal{B}$.
- Show that $\mathcal{B}$ is a basis of V by showing $\mathcal{B}$ spans S which spans V.

□

Applications to Linear Algebra

Corollary 2.3

Every linearly independent subset of a nonzero vector space V can be extended to a basis of V. In particular, every subspace W of V is a direct summand: $V = W \oplus U$ for some subspace U of V.

Corollary 2.4

There exists some $f : \mathbb{R} \to \mathbb{R}$ satisfying $f(x+y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$ and not of the form $f(x) = cx$ for some $c \in R$.

Corollary 2.5

As abelian groups, the vector space $\mathbb{R}^n$ with $+$ is isomorphic to the group $(\mathbb{R}, +)$ for every $n \geq 1$.

The Banach Tarski Paradox

The Banach Tarski Principle is a demonstration of how the axiom of choice can use volume preserving transformations (such as rotations) to duplicate the volume of an object.

Terrence Tao's Proof

Terrence Tao proved a smaller version of the paradox; which works off a line instead of a sphere.

Terrence Tao's Proof

Theorem 3.1

There exists an (uncountably large) subset of $[0, 2]$, breaking it up into a countable number of disjoint subsets, and translating each subset to form $\mathbb{R}$

Step 1

- Define $\sim$ over $[0, 1]$ to be an equivalence relation where $x \sim y$ iff $x - y \in \mathbb{Q}$, creating uncountable equivalence classes countably large.

Step 2

- Define $\sim$ over $[0, 1]$ to be an equivalence relation where $x \sim y$ iff $x - y \in \mathbb{Q}$, creating uncountable equivalence classes countably large.
- Use the AC to create a new set X by selecting an arbitrary element from each equivalence class

Step 3

- Define $\sim$ over $[0, 1]$ to be an equivalence relation where $x \sim y$ iff $x - y \in \mathbb{Q}$, creating uncountable equivalence classes countably large.
- Use the AC to create a new set X by selecting an arbitrary element from each equivalence class
- Note that $X + q$ is disjoint for any $q \in \mathbb{Q} \cap [0, 1]$. Let Y be the union of these sets; this is an uncountably large subset of $[0, 2]$ made up of a countable number of disjoint subsets.

Step 4

- Define $\sim$ over $[0,1]$ to be an equivalence relation where $x \sim y$ iff $x - y \in \mathbb{Q}$, creating uncountable equivalence classes countably large.
- Use the AC to create a new set X by selecting an arbitrary element from each equivalence class
- Note that $X + q$ is disjoint for any $q \in \mathbb{Q} \cap [0,1]$. Let Y be the union of these sets; this is an uncountably large subset of $[0,2]$ made up of a countable number of disjoint subsets.
- Let f be a mapping from all rationals in $[0,1]$ (which exists as both sets are countably infinity) to the entirety of $\mathbb{Q}$. *Translate* all of $X + q$ to $X + f(q)$. This is $\mathbb{R}$.

Formal Theory

A **theory** T is a collection of logical statements.

Example

Let T_G be consisted of the following:

1. Closure: $\forall a, b \in G \quad a * b \in G$,
2. Associativity: $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$,
3. Identity: $\exists e \in G \forall a \in G \quad a * e = e * a = a$,
4. Inverse: $\forall a \in G \exists b \in G \quad a * b = b * a$.

Then T_G is a theory for groups.

Zermelo-Fraenkel Set Theory

ZF denotes the Zermelo-Fraenkel axioms excluding AC:

1. Extensionality: $\forall A, B[\forall x(x \in A \iff x \in B)] \iff A = B$.
2. Regularity: $\forall A[A \neq \varnothing \implies \exists x \in A(x \cap A = \varnothing)]$.
3. Separation: $\{x \in A : \phi(x)\}$ defines a set.
4. Pairing: $\{x, y\}$ is a set.
5. Union: Let $\mathcal{F}$ be a set of sets. Then $\{x : \exists A \in \mathcal{F}(x \in A)\}$ is a set.
6. Replacement: If $\forall x \in A \exists! y[\phi(x, y)]$, then $\{y : \exists x \in A[\phi(x, y)]\}$ is a set.
7. Infinity: $\mathbb{N}$ is a set.
8. Power set: $\{X : X \subseteq A\}$ is a set.

Consistency of Formal Theories

T is **consistent** iff no contradiction can be proved from T.

For any proposition p and any consistent T,

- T proves p iff $T \cup \{\neg p\}$ is inconsistent.
- $T \cup \{p\}$ and $T \cup \{\neg p\}$ cannot be both inconsistent.
- p is **independent** from T when p can neither be proved nor disproved from T.

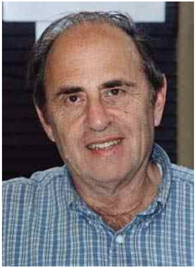
Independence of AC from ZF

Theorem 4.1

If ZF is consistent, then

- Kurt Gödel (1938): $ZF \cup \{AC\}$ is consistent.
- Paul Cohen (1963): $ZF \cup \{\neg AC\}$ is consistent.

Kurt Gödel



Paul Cohen

Ideas of Independence Proofs

A group $(G, *)$ is said to be abelian iff it satisfies T_G and

- Commutativity: $\forall a, b \in G \quad a * b = b * a$.

Theorem 4.2

Commutativity is independent from T_G.

Proof.

Note that $(\mathbb{Z}, +)$ and $(S_3, \circ)$ are both groups:

- If commutativity can be disproved from T_G, then $(\mathbb{Z}, +)$ is not abelian.
- If commutativity can be proved from T_G, then $(S_3, \circ)$ must be abelian.
- Contradiction in both cases!

□

Models for Set Theory

Mathematics is a game played according to certain simple rules with meaningless marks on paper. —— David Hilbert

- $(\mathbb{Z}, +)$ and $(S_3, \circ)$ are **models** for $(T_G, G, *)$.
- When T is a collection of axioms for set theory, a model for $(T, V, \in)$ specifies the collection of sets V and defines $\in$ so that all statements in T are true.
- Soundness: T is consistent if it has a model.
- Gödel found a model for $(ZF \cup \{AC\}, V, \in)$.
- Cohen found a model for $(ZF \cup \{\neg AC\}, V, \in)$.

Bibliography

Paul Cohen (1966).
Set Theory and the Continuum Hypothesis

Keith Conrad.
Zorn's Lemma and Some Applications
https://kconrad.math.uconn.edu/blurbs/zorn1.pdf

Kenneth Kunen (1980).
Set Theory: An Introduction To Independence Proofs

Terence Tao.
The axiom of choice and Banach-Tarski paradoxes
https://www.math.ucla.edu/~tao/resource/general/121.1.00s/tarski.html