Unexpected Consequences of the Axiom of Choice

hexy

October 30, 2019

Zermelo-Fraenkel Set Theory

Zermelo-Fraenkel Set Theory, or **ZF**, is a formulation of set theory with 8 main axioms. They are the current foundation for all of mathematics, where everything we know can be built up from these 8 statements.

The axioms roughly state what types of objects can be sets, and that the natural numbers $\mathbb{N}$ are a set.

Zermelo-Fraenkel Set Theory

This new axiom system was formulates partially as a response to **Russell's Paradox**, which is a contradiction in naive set theory that led to problems.

Zermelo-Fraenkel Set Theory

This new axiom system was formulates partially as a response to **Russell's Paradox**, which is a contradiction in naive set theory that led to problems. The paradox is the fact that without any restrictions on what can be a set, one can do the following:

Let S be the set of all sets that don't contain themselves.
Does S contain S?

There isn't really a consistent way to answer this question.

Axiom of Choice

The **Axiom of Choice**, or **AC** is a 9th axiom of set theory that can be added to ZF, and is usually assumed by default. When we do add it, we say we are working within **ZFC**.

Axiom of Choice

The **Axiom of Choice**, or **AC** is a 9th axiom of set theory that can be added to ZF, and is usually assumed by default. When we do add it, we say we are working within **ZFC**.

Theorem (Axiom of Choice)

Suppose S is a collection of nonempty sets. Then there is a **choice function** *f that for every set $A \in S$, picks out an element $f(A) \in A$.*

By itself, it seems very simple, but this statement has some very bizarre consequences.

Axiom of Choice

To give an example, suppose

$$S = \{\{1, 2, 3\}, \{a, b\}, \{4, 5\}\}.$$

Then a choice function would look like the following:

$$\begin{aligned} f(\{1, 2, 3\}) &= 2 \\ f(\{a, b\}) &= b \\ f(\{4, 5\}) &= 4 \end{aligned}$$

Axiom of Choice

To give an example, suppose

$$S = \{\{1, 2, 3\}, \{a, b\}, \{4, 5\}\}.$$

Then a choice function would look like the following:

$$\begin{aligned} f(\{1, 2, 3\}) &= 2 \\ f(\{a, b\}) &= b \\ f(\{4, 5\}) &= 4 \end{aligned}$$

The axiom of choice simply states that this choice function always exists no matter what set S is given.

Axiom of Choice

The axiom of choice actually has an interesting relation to ZF set theory:

Axiom of Choice

The axiom of choice actually has an interesting relation to ZF set theory:

- In 1938, Kurt Gödel (of Gödel's incompleteness theorems) proved that the negation of AC cannot be proven in ZF.

Axiom of Choice

The axiom of choice actually has an interesting relation to ZF set theory:

- In 1938, Kurt Gödel (of Gödel's incompleteness theorems) proved that the negation of AC cannot be proven in ZF.
- In 1963, Paul Cohen proved that AC cannot be proven in ZF using a novel technique called *forcing*. This won him the Fields medal.

Axiom of Choice

The axiom of choice actually has an interesting relation to ZF set theory:

- In 1938, Kurt Gödel (of Gödel's incompleteness theorems) proved that the negation of AC cannot be proven in ZF.
- In 1963, Paul Cohen proved that AC cannot be proven in ZF using a novel technique called *forcing*. This won him the Fields medal.

This implied that AC was independent of ZF, and could neither be proven or disproven within the system. Therefore, one must assume ZF $+$ AC or ZF $+$ $\neg$AC to work with it.

Equivalent Statements

Now, we will go over statements that are equivalent to AC: this means that saying that AC is true is the exact same thing as saying these other statements are true. These statements range from being almost obviously true to being clearly nonsensical, but each of them is saying the exact same thing as AC.

Unnamed Equivalences

Theorem (Restatement of AC)

The Cartesian product of a family of non-empty sets is non-empty.

This is saying almost the exact same thing as AC, and is just a simple restatement of the fact.

Unnamed Equivalences

Theorem

If A is an infinite set, then there is a bijection between A and $A \times A$: that is, $|A| = |A \times A|$.

This is intuitively true with there being a bijection between $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$, as well as between $\mathbb{R}$ and $\mathbb{R} \times \mathbb{R}$.

Unnamed Equivalences

Theorem

Every vector space has a basis.

Recall that a basis for a vector space is a linearly independent set of vectors that spans the entire space.

Well-Ordering Theorem

Theorem (Well-Ordering Theorem)

Every set can be well-ordered.

Wait...what's a well-ordering? We first have to explain what an ordering is.

Well-Ordering Theorem

Definition (Partial Order)

Given a set S, a partial order on S, $\leq$, satisfies the 3 following constraints:

1. Reflexivity: For every $a \in S$, we have $a \leq a$.
2. Antisymmetry: If $a \leq b$ and $b \leq a$, then $a = b$.
3. Transitivity: If $a \leq b$ and $b \leq c$, then $a \leq c$.

Well-Ordering Theorem

Definition (Total Order)

Let S be a set with a partial order $\leq$. Then $\leq$ is a total order if for every two elements $a, b \in S$ we have that $a \leq b$ or $b \leq a$.

As examples, the natural numbers $\mathbb{N}$ are totally ordered with the usual $\leq$ relation.

Well-Ordering Theorem

Definition (Total Order)

Let S be a set with a partial order $\leq$. Then $\leq$ is a total order if for every two elements $a, b \in S$ we have that $a \leq b$ or $b \leq a$.

As examples, the natural numbers $\mathbb{N}$ are totally ordered with the usual $\leq$ relation.

We can define a partial order $\leq_{alt}$ on $\mathbb{N}$ where $a \leq_{alt} b$ when $\frac{a}{b}$ is an integer, and this is not a total order.

Well-Ordering Theorem

Definition (Well Ordering)

We say a set S with a total order $\leq$ is well-ordered if every subset $A \subseteq S$ has a least element a_0 such that for every $a \in A$ we have $a_0 \leq a$.

The natural numbers $\mathbb{N}$ are well-ordered under the usual $\leq$ relation, where the real numbers $\mathbb{R}$ aren't under the usual $\leq$ relation.

Well-Ordering Theorem

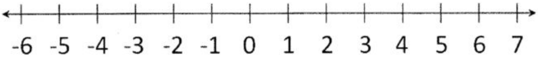
Coming back to the statement of the well-ordering theorem, it simply states that there is a way to define a total order $\leq$ on any set S such that S is well-ordered under $\leq$.

Well-Ordering Theorem

Coming back to the statement of the well-ordering theorem, it simply states that there is a way to define a total order $\leq$ on any set S such that S is well-ordered under $\leq$.

Corollary

$\mathbb{R}$ can be well-ordered.



Source: https://mathcreativity.com/the-future-of-numbers/

Well-Ordering Theorem

The previous fact seems patently absurd: how can you possibly well-order the real numbers?!

Well-Ordering Theorem

The previous fact seems patently absurd: how can you possibly well-order the real numbers?!

What is particularly worrying about this is that there is *no way to show the existence of this well-ordering without the axiom of choice*, meaning that there is no way to write down an explicit definition of the well-ordering of the reals.

Zorn's Lemma

Theorem

Let S be a non-empty set and $\leq$ a partial order on that set. Then if every chain of S has an upper bound, then S has a maximal element.

We have to define what a chain is, what it means for it to have an upper bound, and what a maximal element means here.

Zorn's Lemma

Definition

A **chain** in a set S with a partial order $\leq$ is a subset $A \subseteq S$ under which $\leq$ is a total order on A.

What it means for a chain to have an upper bound is that there is another element in the set $b \in S$ such that for every element of the chain $a \in A$ that $a \leq b$.

Zorn's Lemma

Definition

A **chain** in a set S with a partial order $\leq$ is a subset $A \subseteq S$ under which $\leq$ is a total order on A.

What it means for a chain to have an upper bound is that there is another element in the set $b \in S$ such that for every element of the chain $a \in A$ that $a \leq b$.

Then what Zorn's Lemma is stating is that if every chain has an upper bound, then there is a maximal element, i.e. there is some element $m \in S$ such that for every $s \in S$ that $s \leq m$.

A Remark

"The Axiom of Choice is obviously true, the Well-Ordering theorem is obviously false; and who can tell about Zorn's Lemma?"

— Jerry Bona

Trichotomy

Theorem (Trichotomy)

Let A, B be sets. Then either $|A| < |B|$, $|A| = |B|$, or $|A| > |B|$.

What it means for $|A| < |B|$ is that there is an injection from $A \to B$ but no bijection, and $|A| > |B|$ means that there is a surjection $A \to B$ but no bijection.

Implications

Next, we will go over statements that require AC to prove, but are not equivalent to AC. That is to say, they are strictly weaker statements than AC. Nevertheless, they are interesting in their own right.

Unnamed Implications

Theorem

The union of a countable number of countable sets is countable.

Here, a countable set is a set that has the same cardinality as $\mathbb{N}$.

Unnamed Implications

Theorem

The union of a countable number of countable sets is countable.

Here, a countable set is a set that has the same cardinality as $\mathbb{N}$. Surprisingly, the proof of this theorem implicitly requires the Axiom of Choice, but not its full strength.

Unnamed Implications

Theorem

$(\mathbb{R}, +)$ *and* $(\mathbb{C}, +)$ *are isomorphic as vector spaces.*

Unnamed Implications

Theorem

$(\mathbb{R}, +)$ *and* $(\mathbb{C}, +)$ *are isomorphic as vector spaces.*

This is a consequence of the fact that every vector space has a basis, as one can prove that both these spaces are vector spaces over $\mathbb{Q}$ and $\mathbb{Q} \times \mathbb{Q}$ respectively.

Vitali Theorem

Theorem (Vitali Theorem)

There are non-measurable subsets of $\mathbb{R}$.

To explain what this means, we first have to go over what a measure is.

Vitali Theorem

Theorem (Vitali Theorem)

There are non-measurable subsets of $\mathbb{R}$.

To explain what this means, we first have to go over what a measure is.

A measure is a generalized way to define the "length" of a set. For example, the length of the interval $[0, 1] \subseteq \mathbb{R}$ should be 1, and the measure of that set is correspondingly 1.

Vitali Theorem

Definition

Let X be a set. A **measure** $\mu : \mathcal{P}(X) \to \mathbb{R}$ has the following properties:

1. Non-negativity: $\mu(S) \geq 0$ for any subset $S \subseteq X$.
2. $\mu(\varnothing) = 0$.
3. σ-additivity: If $\{S_i\}_{i\in\mathbb{N}}$ is a countable collection of disjoint subsets, then

$$\mu\left(\bigcup_{i\in\mathbb{N}} S_i\right) = \sum_{i\in\mathbb{N}} \mu(S_i).$$

Vitali Theorem

The non-measurable set V is then constructed by using AC to pick representatives out of the set $\mathbb{R}/\mathbb{Q}$ that are in the interval $[0, 1]$, which we can define as $\mathbb{R}$ mod the equivalence relation $a \sim b$ iff $a - b \in \mathbb{Q}$.

Vitali Theorem

The non-measurable set V is then constructed by using AC to pick representatives out of the set $\mathbb{R}/\mathbb{Q}$ that are in the interval $[0,1]$, which we can define as $\mathbb{R}$ mod the equivalence relation $a \sim b$ iff $a - b \in \mathbb{Q}$.

This set then has the property that the difference between any two of its members is irrational, and is so ill-formed that we are able to prove that

$$1 \leq \sum_{i \in \mathbb{N}} \mu(V) \leq 3$$

which is impossible since the infinite sum of something positive is either 0 or ∞.

Banach-Tarski Paradox

Theorem (Banach-Tarski Paradox)

There is a way to split the solid ball in 3-dimensional space into a finite number of pieces, and only by translating and rotating the pieces, construct 2 copies of the original ball.

The full proof of the Banach-Tarski paradox is too complicated to go over, but VSauce did a famous video on the subject that explains it simply, although glossing over much of the harder details.

Banach-Tarski Paradox

Theorem (Banach-Tarski Paradox)

There is a way to split the solid ball in 3-dimensional space into a finite number of pieces, and only by translating and rotating the pieces, construct 2 copies of the original ball.

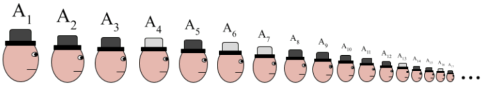
The full proof of the Banach-Tarski paradox is too complicated to go over, but VSauce did a famous video on the subject that explains it simply, although glossing over much of the harder details.

This statement can be considered as a consequence of the existence of non-measurable sets, and doesn't hold if all sets are measurable.

The Hat Problem

Problem

There are a countably infinite number of prisoners standing in a line, all wearing either a white hat or a black hat. They can see the hat color of everyone in front of them, but not their own hat color. Each person is told to guess their hat color. They *cannot* hear the guesses of the people before them. How many guesses can they get right?



Source: https://risingentropy.com/axiom-of-choice-and-hats/

The Hat Problem

Answer: All but finitely many can guess their hat color correctly!

The Hat Problem

Answer: All but finitely many can guess their hat color correctly!

Mathologer's video on "Death by infinity puzzles and the Axiom of Choice" covers this topic, but the idea is to define an equivalence relation on sequences of 0's or 1's by saying $a_n \sim b_n$ when there is some $N \in \mathbb{N}$ such that $a_n = b_n$ for all $n \geq N$: that is to say, they are eventually equal after some finite number of terms.

One can then use the Axiom of Choice to pick a representative from each of these equivalence classes, and every prisoner can instantly know which sequence they are in since only a finite part of the sequence is missing, guaranteeing only finitely many people fail.

What if We Don't Assume AC?

One might assume that since AC has so many unintuitive consequences, we should just not assume it at all. However, this has its own set of unintuitive consequences.

What if We Don't Assume AC?

One might assume that since AC has so many unintuitive consequences, we should just not assume it at all. However, this has its own set of unintuitive consequences.

- $|\mathbb{R}/\mathbb{Q}| > |\mathbb{R}|$, which makes absolutely no sense. There is a beautiful talk about the subject called "How to have more things by forgetting where you put them".

What if We Don't Assume AC?

One might assume that since AC has so many unintuitive consequences, we should just not assume it at all. However, this has its own set of unintuitive consequences.

- $|\mathbb{R}/\mathbb{Q}| > |\mathbb{R}|$, which makes absolutely no sense. There is a beautiful talk about the subject called "How to have more things by forgetting where you put them".
- There is an infinite Dedekind-finite subset of $\mathbb{R}$: this means that there is a set that is infinite but has no bijection with a proper subset of itself. This is also equivalent to having no countable subset.

What if We Don't Assume AC?

- $\mathbb{R}$ could be a countable union of countable sets, completely breaking any notion of measure theory.

What if We Don't Assume AC?

- $\mathbb{R}$ could be a countable union of countable sets, completely breaking any notion of measure theory.
- There is a vector space with two different bases of different cardinalities!

Conclusion

Thanks for listening!

Any questions?