Dr. Zorn's Lemma, or:

How I Learned to Stop Worrying and Love the Axiom of Choice

Iian Smythe
umsmythi@cc.umanitoba.ca

Department of Mathematics
University of Manitoba

Canadian Undergraduate Mathematics Conference 2010

Outline

Zermelo-Fraenkel Set Theory with Choice

- At the foundation of most of modern mathematics sit the 9 axioms of *Zermelo-Fraenkel Set Theory with Choice* (ZFC)
- Of these axioms, the *Axiom of Choice* has generated the most controversy
- Due to this, the Axiom of Choice is still mentioned explicitly when used outside of set theory, while use of the other axioms often goes unmentioned

The Axiom of Choice

The Axiom of Choice (AC)

Given a nonempty collection of nonempty sets, $\mathcal{A}$, there exists a function $f : \mathcal{A} \to \cup\mathcal{A}$ such that for every $A \in \mathcal{A}$, $f(A) \in A$.

- That is, AC asserts the existence of a function which *chooses* elements from the members of $\mathcal{A}$
- Such a function is often called a *choice function*

Prima Facie Doubts

- AC is explicitly *nonconstructive*
- It asserts the existence of a choice function over a family of nonempty sets without describing how to *construct* such a function
- For example, if we consider the set of all nonempty subsets of $\mathbb{N}$, then we can describe a choice function; simply choose the least element of each subset
- But what about all nonempty subsets of $\mathbb{R}$? AC tells us a choice function exists, but we have no way of describing it

The Banach-Tarski Paradox

Theorem (The Banach-Tarski Paradox)

A closed ball, B, in $\mathbb{R}^3$ can be decomposed into finitely many pieces, which when rearranged using only rigid motions can form two closed balls of the same dimensions as B.

- This is possibly the most infamous consequence of AC

Well-Ordered Sets

Definition

A set X, together with a relation $<$, is well-ordered if it is *linearly ordered* by $<$ and every nonempty subset of X has a least element. That is, for every $x, y, z \in X$:

- It is *never* the case that $x < x$ ($<$ is *irreflexive*)
- $x < y$ and $y < z$ implies that $x < z$ ($<$ is *transitive*)
- $x < y$, $x = y$ or $y < x$ ($<$ satisfies *trichotomy*)
- And for any $S \subseteq X$, $S \neq \emptyset$, there exists $s_0 \in S$ such that $s_0 \leq s$ for every $s \in S$.

- Example: $\mathbb{N}$ with the usual ordering is well-ordered, while $\mathbb{R}$ is not

The Well-Ordering Theorem

Theorem (The Well-Ordering Theorem)

Every set can be well-ordered.

- Much like AC itself, this consequence is controversial due to its nonconstructive nature
- For instance, how would one construct a well-ordering of $\mathbb{R}$? All we know is that one exists

Independence of AC

Theorem (Gödel, 1938)

Given the other axioms of ZFC, AC is not disprovable.

- So assuming everything else is consistent, AC cannot be false
- This is promising, but:

Theorem (Cohen, 1964)

Given the other axioms of ZFC, AC is not provable either.

- Oh well.

Should I be Worried?

- It appears that at the foundation of mathematics lies this controversial, nonconstructive axiom which implies bizarre paradoxes
- By the work of Gödel and Cohen, we know that we have to choose (no pun intended) whether or not AC is an acceptable axiom
- Despite the aforementioned controversy, we will see that some very important results in mathematics which we *already* accept actually depend on AC

Equivalent Forms of AC

- AC has numerous equivalent forms, both within set theory and outside of it; we list some of the most well-known below:

The following are equivalent

- (*AC*) Given a nonempty collection of nonempty sets, $\mathcal{A}$, there exists a function $f : \mathcal{A} \to \cup\mathcal{A}$ such that for every $A \in \mathcal{A}$, $f(A) \in A$.
- Given a nonempty collection of nonempty, *pairwise disjoint* sets, $\mathcal{A}$, there exists a set C such that for every $A \in \mathcal{A}$, $C \cap A$ is a singleton.
- The (Cartesian) product of nonempty sets is nonempty.
- (*The Well-Ordering Theorem*) Every set can be well-ordered.

Zorn's Lemma

- Another extremely useful equivalent form of AC is *Zorn's Lemma*

Definition

A collection of sets, $\mathcal{C}$, is called a chain if for every pair of sets $A, B \in \mathcal{C}$ either $A \subseteq B$ or $B \subseteq A$.

Zorn's Lemma (ZL)

Let $\mathcal{A}$ be set such that for every chain $\mathcal{C} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{C} \in \mathcal{A}$. Then $\mathcal{A}$ contains an element M such that M is not a subset of any other set in $\mathcal{A}$ (that is, M is *maximal* in $\mathcal{A}$).

- ZL is often rephrased using the language of *partially ordered sets*

Topological Spaces

Definition

A pair (X, τ), where X is a set and τ is a collection of subsets of X, is called a topological space if:

- $\emptyset, X \in \tau$,
- if $U_i \in \tau$ for $i \in I$, then $\bigcup_{i \in I} U_i \in \tau$,
- if $U_i \in \tau$ for $i = 1, ..., n$, then $\bigcap_{i=1}^{n} U_i \in \tau$.

τ is the topology over X, elements of τ are called the open sets, while complements of open sets are closed sets.

- Example: $\mathbb{R}$ with open sets as unions of open intervals is a topological space

The Product Topology

Definition

Let X_i be a topological space for $i \in I$, and $X = \prod_{i \in I} X_i$. The product topology over X is formed by unions of sets $\prod_{i \in I} U_i$, where:

- each U_i is open in X_i
- for all but *finitely many* $i \in I$, $U_i = X_i$.

- It turns out that this is the “nicest” way to choose a topology over the product of spaces

Compactness

Definition

A topological space X is compact if for every collection of open sets $\mathcal{U}$ with $\bigcup \mathcal{U} = X$ (an *open cover* of X), there is a finite subset $\mathcal{U}' \subseteq \mathcal{U}$ such that $\bigcup \mathcal{U}' = X$.

- Compactness generalizes the properties of closed and bounded subsets of $\mathbb{R}$

Theorem (An equivalent characterization of compactness)

A topological space X is compact iff for every nonempty family of closed sets, $\mathcal{F}$, such that each finite subset of $\mathcal{F}$ has nonempty intersection ($\mathcal{F}$ satisfies the finite intersection property), $\bigcap \mathcal{F} \neq \emptyset$.

Tychonoff's Theorem

Theorem (Tychonoff's Theorem)

If X_i is a compact topological space for every $i \in I$, then $X = \prod_{i \in I} X_i$, with the product topology, is also compact.

- This is one of the central results of general topology
- Its proof can be given through alternative characterizations of compactness, either in terms of *ultranet convergence*, or *subbases* in which each open cover allows a finite subcover
- Either approach relies on AC, in particular Zorn's Lemma, so we have that AC implies Tychonoff's Theorem
- It turns out the converse of this implication is also true

From Tychonoff's Theorem Back to AC

Theorem

Tychonoff's Theorem implies AC.

- In particular, we can show that assuming Tychonoff's Theorem, the product of nonempty sets is nonempty

Proof (Kelley, 1950).

Let $X_i \neq \emptyset$, for every $i \in I$.
Adjoin an outside element a to each X_i, forming $Y_i = X_i \cup \{a\}$, for $i \in I$.
We may define a topology over each Y_i by letting $\emptyset$, Y_i, and $\{a\}$ be the open sets.

Clearly each Y_i is compact, since any open cover will include Y_i itself.

From Tychonoff's Theorem Back to AC (cont'd)

(Cont'd).

So, we have that $Y_i = X_i \cup \{a\}$, for $i \in I$, and each is a compact space. Let $Y = \prod_{i \in I} Y_i$ with the product topology. By Tychonoff's Theorem, Y is compact.

For $i \in I$, let $Z_i = \{x \in Y : \text{the } i^{\text{th}} \text{ coordinate of } x \text{ is in } X_i\}$.
It can be easily shown that each Z_i is closed in Y.

Let J be a finite subset of I, then $\bigcap_{j \in J} Z_j \neq \emptyset$ since we may take z such that the j^{th} coordinate of z is in X_j, for $j \in J$, while the i^{th} coordinate is a, for $i \notin J$. Since J is finite, this requires only finitely many choices. Hence, the family of all such Z_i satisfies the finite intersection property, so by compactness $\bigcap_{i \in I} Z_i \neq \emptyset$.

But $\bigcap_{i \in I} Z_i = \prod_{i \in I} X_i$, so $\prod_{i \in I} X_i \neq \emptyset$. □

Rings

Definition

A set R, together with two binary operations, '$+$' and '$\cdot$', is a ring if for every $a, b, c \in R$:

- $a + b = b + a$
- $(a + b) + c = a + (b + c)$
- there exists $0 \in R$, such that $a + 0 = a$
- there exists $(-a) \in R$, such that $a + (-a) = 0$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$

Rings (cont'd)

Definition

A ring R is a commutative ring if for every $a, b \in R$:

- $a \cdot b = b \cdot a$

R is a ring with unity if for every $a \in R$:

- there exists $1 \in R$, such that $a \cdot 1 = 1 \cdot a = a$

- We will primarily be examining *commutative rings with unity*
- Example: $\mathbb{Z}$ with the usual addition and multiplication

Ideals

Definition

Let R be a commutative ring with unity and $I \subseteq R$, $I \neq \emptyset$. Then I is an ideal of R if for every $a, b \in I, r \in R$:

- $a \pm b \in I$
- $r \cdot a \in I$

An ideal $I \subsetneq R$ is a maximal ideal of R if it is not contained in any other proper ideal of R.

- Observe that $\{0\}$ is an ideal, and contained in every ideal
- An ideal I of R contains 1 iff $I = R$

Krull's Theorem

Theorem (Krull's Theorem)

Every commutative ring with unity such that $1 \neq 0$ *contains a maximal ideal.*

- The proof of this result is a standard application of ZL

Krull's Theorem (cont'd)

Proof.

Let R be a commutative ring with unity such that $1 \neq 0$, and $\mathcal{A}$ be the set of all proper ideals of R. $\mathcal{A} \neq \emptyset$ since $\{0\} \in \mathcal{A}$.

Let $\mathcal{C}$ be a *chain* in $\mathcal{A}$, that is for every pair of sets $A, B \in \mathcal{C}$ either $A \subseteq B$ or $B \subseteq A$.

Let $a, b \in \bigcup \mathcal{C}, r \in R$. There exists $I_1, I_2 \in \mathcal{C}$ such that $a \in I_1, b \in I_2$.
Since $\mathcal{C}$ is a chain, without loss of generality $I_1 \subseteq I_2$.
I_2 is an ideal, so $a \pm b \in I_2 \subseteq \bigcup \mathcal{C}$, and $r \cdot a \in I_2 \subseteq \bigcup \mathcal{C}$.
Hence $\bigcup \mathcal{C}$ is an ideal, and it is proper since it does not contain 1.
Thus, $\bigcup \mathcal{C} \in \mathcal{A}$.

By ZL, $\mathcal{A}$ contains a maximal element, and thus we have that R contains a maximal ideal. □

Krull's Theorem (cont'd)

- Hence, we have that AC implies Krull's Theorem
- Once again, it turns out that the converse of this implication is true
- This requires some additional terminology from ring theory

Polynomial Rings

Definition

Let R be a ring, X a nonempty set. Then $R[X]$ is the set of all polynomials over R with indeterminates in X.

- That is, elements of $R[X]$ are polynomials whose "variables" are elements of X
- Example: $3x^2y - 5xy^3z + 7zy - z \in \mathbb{Z}[\{x, y, z\}]$
- $R[X]$, with the usual polynomial operations, is a ring, and if R is a commutative ring with unity such that $1 \neq 0$, then so is $R[X]$

Integral Domains and Quotient Fields

Definition

A commutative ring with unity is an integral domain if $1 \neq 0$ and for every $a, b \in R$, $a \cdot b = 0$ implies that either $a = 0$ or $b = 0$.

- If R is an integral domain, then $R[X]$ is also an integral domain

Definition

Let R be an integral domain. The field of quotients of R is the set of all quotients $\frac{a}{b}$, where $a, b \in R, b \neq 0$, with equality, addition and multiplication as usually defined for fractions. We denote this $Q(R)$.

- $Q(R)$ is a field with R as a subring
- Example: $Q(\mathbb{Z}) = \mathbb{Q}$

Ideals Generated by a Set

Definition

Let R be a commutative ring with unity and $X \subseteq R$. The ideal generated by X is the set $RX = \{r_1 \cdot x_1 + \ldots + r_n \cdot x_n : r_i \in R, x_i \in X\}$.

That is, RX is the set of all R-linear combinations of elements in X.

- RX is the smallest ideal of R containing X

From Krull's Theorem Back to AC

Theorem

Krull's Theorem implies AC.

- This result is due to Hodges, 1979, but we will outline the proof given by Banaschewski, 1994.
- In particular, we can show that given a nonempty collection of nonempty, *pairwise disjoint* sets, $\mathcal{E}$, there exists a set C such that for every $A \in \mathcal{E}$, $C \cap A$ is a singleton

From Krull's Theorem Back to AC (cont'd)

Proof (Outline, from Banaschewski, 1994).

Let $\mathcal{E}$ be a nonempty collection of nonempty, pairwise disjoint sets, and set $E = \bigcup \mathcal{E}$.

We will call a subset $S \subseteq E$ a *spread* if for every $A \in \mathcal{E}$, $S \cap A$ has *at most* one element.
Our desired form of AC asserts the existence of maximal spreads, which is what we set out to prove.

Let $R = \mathbb{Q}[E]$, the ring of polynomials over the rationals with indeterminates in E.

Let $\mathcal{O}$ be the set of all spreads, and set $T = \bigcup\{RX : X \in \mathcal{O}\}$, and $U = T^c = \bigcap\{(RX)^c : X \in \mathcal{O}\}$, where RX is the ideal generated by X.

From Krull's Theorem Back to AC (cont'd)

(Cont'd).

It can be shown that for every $X \in \mathcal{O}$, $(RX)^c$ is closed under multiplication, and hence $U = \bigcap\{(RX)^c : X \in \mathcal{O}\}$ is likewise closed under multiplication.

Consider $R[U^{-1}] = \{\frac{r}{u} : r \in R, u \in U\}$, a subring of Q(R). This is well defined since $0 \notin U$ (recall that 0 is contained in every ideal), and U is closed under multiplication.
In fact, $R[U^{-1}]$ is commutative ring with unity such that $1 \neq 0$, hence by Krull's Theorem, it has a maximal ideal M.

Let $H = M \cap R$. It can be shown that H is an ideal of R which is contained in $T = \bigcup\{RX : X \in \mathcal{O}\}$, and is maximal amongst all ideals of R contained in T.

From Krull's Theorem Back to AC (cont'd)

(Cont'd).

So, we have $H = M \cap R$, where M is a maximal ideal of $R[U^{-1}]$.

Let $K = H \cap E$, it can then be shown that $H = RK$.

Suppose that K is *not* a spread.
That is, we suppose that there exists $A \in \mathcal{E}$ such that $K \cap A$ contains *at least* two distinct elements, say x and y.
$x + y \in RK = H \subseteq T$, so there exists a spread S such that $x + y \in RS$.
It can be shown since $x, y \in E$, $x, y \in S$. But then $x, y \in S \cap A$, contradicting S being a spread.

Thus, K is a spread. Since $RK = H$ is a maximal amongst all ideals of R contained in T, K must be a maximal spread.
It follows that for every $A \in \mathcal{E}$, $K \cap A$ is a singleton. □

Other Results

- So, AC is equivalent to theorems in topology and ring theory
- Hence, if we give up AC, we lose both of the aforementioned theorems, not to mention their numerous consequences
- Not convinced? There are many more results that depend on AC, including the following:

Theorem

Every vector space has a basis.

Theorem (The Baire Category Theorem)

Every subset of a complete metric space which is a countable union of nowhere dense sets has empty interior.

Summary

- The Axiom of Choice, one of the foundational axioms of mathematics, states that given a collection of nonempty sets, there is a function which chooses elements from each set
- AC is nonconstructive in nature, and implies some paradoxical results which has caused it to be controversial
- Despite this controversy, AC has many useful equivalent forms including Tychonoff's Theorem in topology and Krull's Theorem in ring theory
- While there may be philosophical worries about AC, there can be little doubt of its importance throughout mathematics

- These slides will be available on my University of Manitoba webpage: home.cc.umanitoba.ca/˜umsmythi/documents.html

References

- Banaschewski, Bernhard. A New Proof that “Krull Implies Zorn”. *Mathematical Logic Quarterly* **40** (1994), 478-480.
- Blass, Andreas. Existence of Bases Implies the Axiom of Choice. *Contemporary Mathematics* **31** (1984), 31-34.
- Hodges, Wilfrid. Krull Implies Zorn. *Journal of the London Mathematical Society* **19** (1979), 285-287.
- Kelley, J. L. The Tychonoff Product Theorem Implies the Axiom of Choice. *Fundamenta Mathematicae* **37** (1950), 75-76.
- Jech, Thomas J. *The Axiom of Choice*. New York: Dover, 2008.