The Axiom of Choice

Gregory Cherlin

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

IMR Aug. 28, 2010

Choice Functions

Proposition

There is a function $f : \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} \to \mathbb{N}$ *such that*

$$f(A) \in A \text{ for } A \subseteq \mathbb{N},\ A \neq \emptyset$$

Choice Functions

Proposition

There is a function $f : \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} \to \mathbb{N}$ *such that*

$$f(A) \in A \text{ for } A \subseteq \mathbb{N},\ A \neq \emptyset$$

Proof.

$\min(A)$ □

Choice Functions

Proposition

There is a function $f : \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} \to \mathbb{N}$ *such that*

$$f(A) \in A \text{ for } A \subseteq \mathbb{N},\ A \neq \emptyset$$

Corollary

There is a function $f : \mathcal{P}(\mathbb{Q}) \setminus \{\emptyset\} \to \mathbb{Q}$ *such that*

$$f(A) \in A \text{ for } A \subseteq \mathbb{Q},\ A \neq \emptyset$$

Choice Functions

Proposition

There is a function $f : \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} \to \mathbb{N}$ *such that*

$$f(A) \in A \text{ for } A \subseteq \mathbb{N},\ A \neq \emptyset$$

Corollary

There is a function $f : \mathcal{P}(\mathbb{Q}) \setminus \{\emptyset\} \to \mathbb{Q}$ *such that*

$$f(A) \in A \text{ for } A \subseteq \mathbb{Q},\ A \neq \emptyset$$

Problem

Is there a function $f : \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\} \to \mathbb{R}$ *such that*

$$f(A) \in A \text{ for } A \subseteq \mathbb{R},\ A \neq \emptyset?$$

The Axiom

Axiom of Choice

$$\forall S \quad \exists f: \quad \mathcal{P}(S) \setminus \{\emptyset\} \to S$$
$$f(A) \in A \quad \text{all} \quad A \subseteq S, A \neq \emptyset$$

The Axiom

Axiom of Choice

$$\forall S \quad \exists f : \quad \mathcal{P}(S) \setminus \{\emptyset\} \to S$$
$$f(A) \in A \quad \text{all} \quad A \subseteq S, A \neq \emptyset$$

EQUIVALENTLY

- $\forall (A_i)_{i \in I} \quad \exists (a_i)_{i \in I} \quad a_i \in A_i \qquad [\prod_i A_i \neq \emptyset];$

The Axiom

Axiom of Choice

$$\forall S \quad \exists f : \quad \mathcal{P}(S) \setminus \{\emptyset\} \to S$$
$$f(A) \in A \quad \text{all} \quad A \subseteq S, A \neq \emptyset$$

EQUIVALENTLY

- $\forall (A_i)_{i \in I} \quad \exists (a_i)_{i \in I} \quad a_i \in A_i \qquad [\prod_i A_i \neq \emptyset];$
- For all partitions $(A_i)_{i \in I}$ of A, there is a *cross-section* $X \subseteq A$: $\quad |X \cap A_i| = 1$ all i.

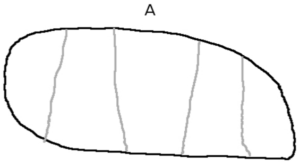
The Axiom

Axiom of Choice

$$\forall S \quad \exists f : \quad \mathcal{P}(S) \setminus \{\emptyset\} \to S$$
$$f(A) \in A \quad \text{all} \quad A \subseteq S, A \neq \emptyset$$

EQUIVALENTLY

- $\forall (A_i)_{i \in I} \quad \exists (a_i)_{i \in I} \quad a_i \in A_i \qquad [\prod_i A_i \neq \emptyset]$;
- For all partitions $(A_i)_{i \in I}$ of A, there is a *cross-section* $X \subseteq A$: $\quad |X \cap A_i| = 1$ all i.



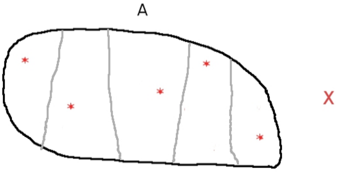
The Axiom

Axiom of Choice

$$\forall S \quad \exists f: \quad \mathcal{P}(S) \setminus \{\emptyset\} \to S$$
$$f(A) \in A \quad \text{all} \quad A \subseteq S, A \neq \emptyset$$

EQUIVALENTLY

- $\forall (A_i)_{i \in I} \quad \exists (a_i)_{i \in I} \quad a_i \in A_i \qquad [\prod_i A_i \neq \emptyset]$;
- For all partitions $(A_i)_{i \in I}$ of A, there is a *cross-section* $X \subseteq A$: $\quad |X \cap A_i| = 1$ all i.



SO WHAT?

1. Useful and essential for infinite processes.
   Example: Bases in infinite dimensional vector spaces.

SO WHAT?

1. Useful and essential for infinite processes.
   Example: Bases in infinite dimensional vector spaces.
2. Nonconstructive.
   Asserts existence only.
   Sometimes, it is enough to know that something *exists.*
   Other times, we need to *find* it explicitly.

SO WHAT?

1. Useful and essential for infinite processes.
   Example: Bases in infinite dimensional vector spaces.
2. Nonconstructive.
   Asserts existence only.
   Sometimes, it is enough to know that something *exists.*
   Other times, we need to *find* it explicitly.
3. Surprising ("paradoxical") consequences.

SO WHAT?

1. Useful and essential for infinite processes.
   Example: Bases in infinite dimensional vector spaces.
2. Nonconstructive.
   Asserts existence only.
   Sometimes, it is enough to know that something *exists.*
   Other times, we need to *find* it explicitly.
3. Surprising ("paradoxical") consequences.

Useful, but dangerous.

The Vitali Partition

$$A_r = r + \mathbb{Q} \subseteq \mathbb{R} \ (r \in \mathbb{R})$$

The Vitali Partition

$$A_r = r + \mathbb{Q} \subseteq \mathbb{R} \ (r \in \mathbb{R})$$

Lemma

If A_r meets A_s then $A_r = A_s$. Thus the sets A_r partition $\mathbb{R}$.

The Vitali Partition

$$A_r = r + \mathbb{Q} \subseteq \mathbb{R} \ (r \in \mathbb{R})$$

Lemma

If A_r meets A_s then $A_r = A_s$. Thus the sets A_r partition $\mathbb{R}$.

Proof.

The relation

$$x - y \in \mathbb{Q}$$

is an *equivalence relation* on $\mathbb{R}$.
The sets A_r are the equivalence classes for this relation. □

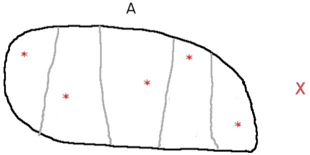
The Vitali Partition

$$A_r = r + \mathbb{Q} \subseteq \mathbb{R} \; (r \in \mathbb{R})$$

Lemma

If A_r meets A_s then $A_r = A_s$. Thus the sets A_r partition $\mathbb{R}$.

AC: There is a cross section X for this partition.



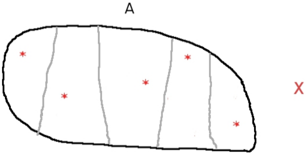
The Vitali Partition

$$A_r = r + \mathbb{Q} \subseteq \mathbb{R} \ (r \in \mathbb{R})$$

Lemma

If A_r meets A_s then $A_r = A_s$. Thus the sets A_r partition $\mathbb{R}$.

AC: There is a cross section X for this partition.



Can you find one?

$$X + q \ (q \in \mathbb{Q}) \text{ should partition } \mathbb{R}$$

Length

Axioms for Length

$\ell : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$

Length

Axioms for Length

$\ell : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$

1. $0 \leq \ell(A) \leq \infty$.

Length

Axioms for Length

$\ell : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.

Length

Axioms for Length

$\ell : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity: $\ell(\dot{\bigcup}_{i=0}^{\infty} A_i) = \sum_i \ell(A_i)$

Length

Axioms for Length

$\ell : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity: $\ell(\dot{\bigcup}_{i=0}^{\infty} A_i) = \sum_i \ell(A_i)$
4. Translation invariance: $\ell(A + r) = \ell(A)$.

Length

Axioms for Length

$\ell : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity: $\ell(\dot{\bigcup}_{i=0}^{\infty} A_i) = \sum_i \ell(A_i)$
4. Translation invariance: $\ell(A + r) = \ell(A)$.

Proposition (Vitali (1905))

There is no such notion of length.

Length

Axioms for Length

$\ell : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity: $\ell(\dot{\bigcup}_{i=0}^{\infty} A_i) = \sum_i \ell(A_i)$
4. Translation invariance: $\ell(A + r) = \ell(A)$.

Let X be a cross section for the Vitali partition *contained in* $[0, 1]$.
Claim: X cannot have a length.

The Vitali Cross Section

A Vitali cross section $X \subseteq [0, 1]$ cannot have a length.

The Vitali Cross Section

A Vitali cross section $X \subseteq [0, 1]$ cannot have a length.

(Properties of Length)

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity $\ell(\dot{\bigcup}_i A_i) = \sum_i \ell(A_i)$
4. Translation invariance $\ell(A + r) = \ell(A)$.

The Vitali Cross Section

A Vitali cross section $X \subseteq [0, 1]$ cannot have a length.

(Properties of Length)

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity $\ell(\dot{\bigcup}_i A_i) = \sum_i \ell(A_i)$
4. Translation invariance $\ell(A + r) = \ell(A)$.

Proof.

- If $\ell(X) > 0$:

The Vitali Cross Section

A Vitali cross section $X \subseteq [0,1]$ cannot have a length.

(Properties of Length)

1. $0 \le \ell(A) \le \infty$.
2. $\ell[a,b] = b - a$.
3. Countable additivity $\ell(\dot{\bigcup}_i A_i) = \sum_i \ell(A_i)$
4. Translation invariance $\ell(A + r) = \ell(A)$.

Proof.

- If $\ell(X) > 0$:
  $X + q \subseteq [0,2]$ when $q \in \mathbb{Q} \cap [0,1]$.

The Vitali Cross Section

A Vitali cross section $X \subseteq [0,1]$ cannot have a length.

(Properties of Length)

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a,b] = b - a$.
3. Countable additivity $\ell(\dot{\bigcup}_i A_i) = \sum_i \ell(A_i)$
4. Translation invariance $\ell(A + r) = \ell(A)$.

Proof.

- If $\ell(X) > 0$:
  $X + q \subseteq [0,2]$ when $q \in \mathbb{Q} \cap [0,1]$.
  $2 = \ell([0,2]) \geq \ell(X) + \ell(X) + \ell(X) + \ldots$

The Vitali Cross Section

A Vitali cross section $X \subseteq [0, 1]$ cannot have a length.

(Properties of Length)

1. $0 \le \ell(A) \le \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity $\ell(\dot{\bigcup}_i A_i) = \sum_i \ell(A_i)$
4. Translation invariance $\ell(A + r) = \ell(A)$.

Proof.

- If $\ell(X) = 0$:

The Vitali Cross Section

A Vitali cross section $X \subseteq [0, 1]$ cannot have a length.

(Properties of Length)

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity $\ell(\dot{\bigcup}_i A_i) = \sum_i \ell(A_i)$
4. Translation invariance $\ell(A + r) = \ell(A)$.

Proof.

- If $\ell(X) = 0$:
  $[0, 1] \subseteq \bigcup_q (X + q)$

The Vitali Cross Section

A Vitali cross section $X \subseteq [0, 1]$ cannot have a length.

(Properties of Length)

1. $0 \leq \ell(A) \leq \infty$.
2. $\ell[a, b] = b - a$.
3. Countable additivity $\ell(\dot{\bigcup}_i A_i) = \sum_i \ell(A_i)$
4. Translation invariance $\ell(A + r) = \ell(A)$.

Proof.

- If $\ell(X) = 0$:
  $[0, 1] \subseteq \bigcup_q (X + q)$
  $1 = \ell([0, 1]) \leq 0 + 0 + 0 + \dots$

□

Nonconstructivity - Philosophical Interlude

There is a good theory of length (Lebesgue measure).
All axioms hold, but it is not defined for every set.

Nonconstructivity - Philosophical Interlude

There is a good theory of length (Lebesgue measure). All axioms hold, but it is not defined for every set.

$\langle$philosophy$\rangle$

Nonconstructivity - Philosophical Interlude

There is a good theory of length (Lebesgue measure).
All axioms hold, but it is not defined for every set.

⟨philosophy⟩
In practice, if a set of reals can be defined explicitly, it *does* have a well-defined length (Lebesgue measure).

Nonconstructivity - Philosophical Interlude

There is a good theory of length (Lebesgue measure).
All axioms hold, but it is not defined for every set.

⟨philosophy⟩
In practice, if a set of reals can be defined explicitly, it *does* have a well-defined length (Lebesgue measure).

Conclusion: Vitali cross sections cannot be defined explicitly.

Nonconstructivity - Philosophical Interlude

There is a good theory of length (Lebesgue measure).
All axioms hold, but it is not defined for every set.

⟨philosophy⟩

In practice, if a set of reals can be defined explicitly, it *does* have a well-defined length (Lebesgue measure).

Conclusion: Vitali cross sections cannot be defined explicitly.

⟨/philosophy⟩

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, . . .

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, ...

What is “dimension”? What is a “basis”?
Maximal linearly independent set.

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, ...

What is "dimension"? What is a "basis"?
Maximal linearly independent set.
But do they exist?
$f_1, f_2, \ldots$

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, ...

What is “dimension”? What is a “basis”?
Maximal linearly independent set.
But do they exist?
$f_1, f_2, \ldots; g_1, g_2, \ldots;$

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, . . .

What is "dimension"? What is a "basis"?
Maximal linearly independent set.
But do they exist?
$f_1, f_2, \ldots; g_1, g_2, \ldots; \ldots$

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, . . .

What is "dimension"? What is a "basis"?
Maximal linearly independent set.
But do they exist?
$f_1, f_2, \ldots; g_1, g_2, \ldots; \ldots$

- How to continue?
- How to stop?

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, ...

What is "dimension"? What is a "basis"?
Maximal linearly independent set.
But do they exist?
$f_1, f_2, \ldots; g_1, g_2, \ldots; \ldots$

- How to continue? AC
- How to stop?

The Basis Problem

Infinite dimensional vector spaces.

Example: $F(\mathbb{R}, \mathbb{R})$—all functions from $\mathbb{R}$ to $\mathbb{R}$.
Subspaces: continuous, differentiable, ...

What is "dimension"? What is a "basis"?
Maximal linearly independent set.
But do they exist?
$f_1, f_2, \ldots; g_1, g_2, \ldots; \ldots$

- How to continue?
- How to stop? (ordinals)

The Basis Problem (Continued)

$$V \text{ a vector space}$$
$$\mathcal{I} = \{X \subseteq V : X \text{ is linearly independent}\}$$
$$X \leq Y \iff X \subseteq Y$$

The Basis Problem (Continued)

$$V \text{ a vector space}$$
$$\mathcal{I} = \{X \subseteq V : X \text{ is linearly independent}\}$$
$$X \leq Y \iff X \subseteq Y$$

Definition

- A partially ordered set (p.o.s.) is a set I together with a relation $\leq$ on I which is *reflexive, antisymmetric, transitive*.

The Basis Problem (Continued)

$$V \text{ a vector space}$$
$$\mathcal{I} = \{X \subseteq V : X \text{ is linearly independent}\}$$
$$X \le Y \iff X \subseteq Y$$

Definition

- A partially ordered set (p.o.s.) is a set I together with a relation $\le$ on I which is *reflexive, antisymmetric, transitive*.
- A linearly ordered set is a p.o.s. whose order relation is total: any two elements are comparable.

The Basis Problem (Continued)

$$\mathcal{I} = \{X \subseteq V : X \text{ is linearly independent}\}$$
$$X \leq Y \iff X \subseteq Y$$

Definition

- A partially ordered set (p.o.s.) is a set I together with a relation $\leq$ on I which is *reflexive, antisymmetric, transitive*.
- A linearly ordered set is a p.o.s. whose order relation is total: any two elements are comparable.
- A chain in a p.o.s. is a linearly ordered subset.

The Basis Problem (Continued)

$$X \leq Y \iff X \subseteq Y$$

Definition

- A partially ordered set (p.o.s.) is a set I together with a relation $\leq$ on I which is *reflexive, antisymmetric, transitive*.
- A linearly ordered set is a p.o.s. whose order relation is total: any two elements are comparable.
- A chain in a p.o.s. is a linearly ordered subset.
- A subset X of a p.o.s. $(I, \leq)$ is bounded above if there is an element a of I with

$$x \leq a \text{ (all } x \in X)$$

The Basis Problem (Continued)

Definition

- A partially ordered set (p.o.s.) is a set I together with a relation $\leq$ on I which is *reflexive, antisymmetric, transitive*.
- A linearly ordered set is a p.o.s. whose order relation is total: any two elements are comparable.
- A chain in a p.o.s. is a linearly ordered subset.
- A subset X of a p.o.s. $(I, \leq)$ is bounded above if there is an element a of I with

$$x \leq a \text{ (all } x \in X)$$

Example: Independent subsets of V, with $\subseteq$. An *increasing sequence* of independent subsets of $\mathcal{I}$ would form a chain—and their union is an *upper bound* for the chain.

Maximal Elements of p.o.s.

Zorn's Lemma

Let $(I, \leq)$ be a p.o.s. in which every chain has an upper bound. Then I has a maximal element.

Maximal Elements of p.o.s.

Zorn's Lemma

Let $(I, \leq)$ be a p.o.s. in which every chain has an upper bound. Then I has a maximal element.

Examples

- Independent subsets of vector spaces.
- Proper ideals in a commutative ring with 1.

Maximal Elements of p.o.s.

Zorn's Lemma

Let $(I, \leq)$ be a p.o.s. in which every chain has an upper bound. Then I has a maximal element.

Examples

- Independent subsets of vector spaces.
- Proper ideals in a commutative ring with 1.

First Applications

First Applications

Zorn's Lemma

Let $(I, \leq)$ be a p.o.s. in which every chain has an upper bound. Then I has a maximal element.

First Applications

Zorn's Lemma

Let $(I, \leq)$ be a p.o.s. in which every chain has an upper bound. Then I has a maximal element.

Theorem

The Axiom of Choice and Zorn's Lemma are equivalent.

First Applications

Zorn's Lemma

Let $(I, \leq)$ be a p.o.s. in which every chain has an upper bound. Then I has a maximal element.

Theorem

The Axiom of Choice and Zorn's Lemma are equivalent.

Applications

- Every vector space has a basis.

First Applications

Zorn's Lemma

Let $(I, \leq)$ be a p.o.s. in which every chain has an upper bound. Then I has a maximal element.

Theorem

The Axiom of Choice and Zorn's Lemma are equivalent.

Applications

- Every vector space has a basis.
- Every commutative ring with 1 has a maximal ideal.

AC and Zorn

Theorem

The Axiom of Choice and Zorn's Lemma are equivalent.

AC and Zorn

Theorem

The Axiom of Choice and Zorn's Lemma are equivalent.

Proof.

$\Longleftarrow$: To build a cross section X for a partition $(A_i)_{i \in I}$, let Ξ be the p.o.s. consisting of sets X satisfying

$$|X \cap A_i| \leq 1 \quad \text{(all } i \in I)$$

ordered by inclusion.

AC and Zorn

Theorem

The Axiom of Choice and Zorn's Lemma are equivalent.

Proof.

$\Longleftarrow$: To build a cross section X for a partition $(A_i)_{i \in I}$, let Ξ be the p.o.s. consisting of sets X satisfying

$$|X \cap A_i| \leq 1 \quad \text{(all } i \in I\text{)}$$

ordered by inclusion.
By Zorn's Lemma, there is a maximal $X \in \Xi$. It must be a cross section! □

AC and Zorn

Theorem

The Axiom of Choice and Zorn's Lemma are equivalent.

Proof.

$\Longrightarrow$ *(sketch):*

If a p.o.s. I has no maximal element, use *AC* to find a function $f : I \to I$ such that

$$f(x) > x \text{ for } x \in I$$

Use f to build a *very long* increasing sequence (a chain)—which has no upper bound. $(\ldots)$. □

Well-Ordering

Definition

A linear ordering $(L, \leq)$ is a well ordering, if every nonempty subset of L has a minimum.

Well-Ordering

Definition

A linear ordering $(L, \leq)$ is a well ordering, if every nonempty subset of L has a minimum.

Some well ordered subsets of $\mathbb{R}$:

$\mathbb{N}$; $\{1/n : n \in \mathbb{N}\}$, with the reverse ordering

Well-Ordering

Definition

A linear ordering $(L, \leq)$ is a well ordering, if every nonempty subset of L has a minimum.

Some well ordered subsets of $\mathbb{R}$:

$\mathbb{N}$; $\{1/n : n \in \mathbb{N}\}$, with the reverse ordering

$\{1/m + 1/n : m, n \in \mathbb{N}\}$, with the reverse ordering;

Well-Ordering

Definition

A linear ordering $(L, \leq)$ is a well ordering, if every nonempty subset of L has a minimum.

Some well ordered subsets of $\mathbb{R}$:
$\mathbb{N}$; $\{1/n : n \in \mathbb{N}\}$, with the reverse ordering
$\{1/m + 1/n : m, n \in \mathbb{N}\}$, with the reverse ordering;

Some not well-ordered subsets of $\mathbb{R}$:
$\mathbb{R}$, $\mathbb{Q}$, $[0, 1]$.

Well-Ordering

Definition

A linear ordering $(L, \leq)$ is a well ordering, if every nonempty subset of L has a minimum.

Some well ordered subsets of $\mathbb{R}$:
$\mathbb{N}$; $\{1/n : n \in \mathbb{N}\}$, with the reverse ordering
$\{1/m + 1/n : m, n \in \mathbb{N}\}$, with the reverse ordering;
Some not well-ordered subsets of $\mathbb{R}$:
$\mathbb{R}$, $\mathbb{Q}$, $[0, 1]$.

Remark

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

Well-Ordering

Definition

A linear ordering $(L, \leq)$ is a well ordering, if every nonempty subset of L has a minimum.

Some well ordered subsets of $\mathbb{R}$:
$\mathbb{N}$; $\{1/n : n \in \mathbb{N}\}$, with the reverse ordering
$\{1/m + 1/n : m, n \in \mathbb{N}\}$, with the reverse ordering;
Some not well-ordered subsets of $\mathbb{R}$:
$\mathbb{R}$, $\mathbb{Q}$, $[0, 1]$.

Remark

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

Problem

Can $\mathbb{R}$ be well-ordered?

The Well Ordering Principle

Theorem (Zermelo)

Any set S can be well ordered.

In fact:

The Well Ordering Principle

Theorem (Zermelo)

Any set S can be well ordered.

In fact:

Theorem

The following are equivalent.

- *The Axiom of Choice.*
- *Zorn's Lemma*
- *The Well Ordering Principle*

The Well Ordering Principle

Theorem (Zermelo)

Any set S can be well ordered.

In fact:

Theorem

The following are equivalent.

- *The Axiom of Choice.*
- *Zorn's Lemma*
- *The Well Ordering Principle*

The Axiom of Choice is obviously true; the Well Ordering Principle is obviously false; and who can tell about Zorn's Lemma?—Jerry Bona

The Well Ordering Principle

Theorem (Zermelo)

Any set S can be well ordered.

In fact:

Theorem

The following are equivalent.

- *The Axiom of Choice.*
- *Zorn's Lemma*
- *The Well Ordering Principle*

Fréchet: An implication between two known truths is not a new result.
Lebesgue: An implication between two false statements is of no interest.

From *WO* to *AC*

Theorem

The following are equivalent.

- *The Axiom of Choice.*
- *Zorn's Lemma*
- *The Well Ordering Principle*

From *WO* to *AC*

Theorem

The following are equivalent.

- *The Axiom of Choice.*
- *Zorn's Lemma*
- *The Well Ordering Principle*

From *WO* to *AC*: $f(A) = \min(A)$!

From *WO* to *AC*

Theorem

The following are equivalent.

- *The Axiom of Choice.*
- *Zorn's Lemma*
- *The Well Ordering Principle*

From *WO* to *AC*: $f(A) = \min(A)$!

From Zorn to *WO* ...

Zorn $\implies$ *WO*

To show: *S can be well ordered.*

$I = \{(X, \leq_X) : X \subseteq S, \leq$ is a well ordering of $X\}$

Zorn $\implies$ *WO*

To show: *S can be well ordered.*

$I = \{(X, \leq_X) : X \subseteq S, \leq$ is a well ordering of $X\}$
How do we compare $(X, \leq_X)$ and $(Y, \leq_Y)$?

Zorn $\implies$ *WO*

To show: *S can be well ordered.*

$I = \{(X, \leq_X) : X \subseteq S, \leq$ is a well ordering of $X\}$
How do we compare $(X, \leq_X)$ and $(Y, \leq_Y)$?

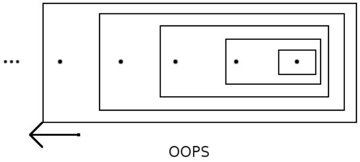
First try: $X \subseteq Y$ and $\leq_Y$ agrees with $\leq_X$ on X.

Zorn $\implies$ *WO*

To show: *S can be well ordered.*

$I = \{(X, \leq_X) : X \subseteq S, \leq \text{ is a well ordering of } X\}$
How do we compare $(X, \leq_X)$ and $(Y, \leq_Y)$?

First try: $X \subseteq Y$ and $\leq_Y$ agrees with $\leq_X$ on X.
Does not work.
The sets $X_n = \{-n, -n+1, \ldots, 0\}$ with the usual ordering are well ordered (finite!) and form a chain. Their union gives the usual ordering of $-\mathbb{N}$. Not a WO.



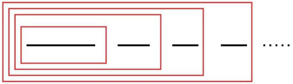
Zorn $\implies$ *WO*

To show: *S can be well ordered.*

$I = \{(X, \leq_X) : X \subseteq S, \leq \text{ is a well ordering of } X\}$
How do we compare $(X, \leq_X)$ and $(Y, \leq_Y)$?

First try: $X \subseteq Y$ and $\leq_Y$ agrees with $\leq_X$ on X.
The sets $X_n = \{-n, -n+1, \ldots, 0\}$ with the usual ordering are well ordered (finite!) and form a chain. Their union gives the usual ordering of $-\mathbb{N}$. Not a WO.

Second try: $X \subseteq Y$; $\leq_Y$ agrees with $\leq_X$ on X; and
$Y \setminus X > X$.



Better

Additive functions of one variable

Functional equation: $f(x+y) = f(x) + f(y)$.—*Solve for f.*

Additive functions of one variable

Functional equation: $f(x+y) = f(x) + f(y)$.—*Solve for* f.

Theorem

Any function $f : \mathbb{R} \to \mathbb{R}$ *which satisfies*

$$f(x+y) = f(x) + f(y) \text{ all } x, y \in \mathbb{R}$$

is either of the form $f(x) = mx$ *or is discontinuous everywhere.*

Additive functions of one variable

Functional equation: $f(x+y) = f(x) + f(y)$.—*Solve for f.*

Theorem

Any function $f : \mathbb{R} \to \mathbb{R}$ *which satisfies*

$$f(x+y) = f(x) + f(y) \text{ all } x, y \in \mathbb{R}$$

is either of the form $f(x) = mx$ *or is discontinuous everywhere.*

Example

Fix a basis X for $\mathbb{R}$ as a vector space over $\mathbb{Q}$ with $1 \in X$. For $r \in \mathbb{R}$, let $f(r)$ be the coefficient of 1 in the expansion of r with respect to the basis X.

Additive functions of one variable

Functional equation: $f(x+y) = f(x) + f(y)$.—*Solve for f.*

Theorem

Any function $f : \mathbb{R} \to \mathbb{R}$ which satisfies

$$f(x+y) = f(x) + f(y) \text{ all } x, y \in \mathbb{R}$$

is either of the form $f(x) = mx$ or is discontinuous everywhere.

Example

Fix a basis X for $\mathbb{R}$ as a vector space over $\mathbb{Q}$ with $1 \in X$. For $r \in \mathbb{R}$, let $f(r)$ be the coefficient of 1 in the expansion of r with respect to the basis X. ($f(1) = 1$, and $f(x) = 0$ for $x \in X$, $x \neq 1$)

Additive functions of one variable

Functional equation: $f(x+y) = f(x) + f(y)$.—*Solve for f.*

Theorem

Any function $f : \mathbb{R} \to \mathbb{R}$ which satisfies

$$f(x+y) = f(x) + f(y) \text{ all } x, y \in \mathbb{R}$$

is either of the form $f(x) = mx$ or is discontinuous everywhere.

Example

Fix a basis X for $\mathbb{R}$ as a vector space over $\mathbb{Q}$ with $1 \in X$. For $r \in \mathbb{R}$, let $f(r)$ be the coefficient of 1 in the expansion of r with respect to the basis X. ($f(1) = 1$, and $f(x) = 0$ for $x \in X$, $x \neq 1$)

These functions *exist,* but none has ever been *constructed.*

Something for Nothing

Theorem (Hausdorf, Banach, Tarski)

A sphere of radius 1 may be decomposed into finitely many pieces which can be reassembled to make two spheres of radius 1.

Something for Nothing

Theorem (Hausdorf, Banach, Tarski)

A sphere of radius 1 may be decomposed into finitely many pieces which can be reassembled to make two spheres of radius 1.

(Some vague idea . . . :)

A variation on the Vitali decomposition, using rotations instead of translations!

Something for Nothing

Theorem (Hausdorf, Banach, Tarski)

A sphere of radius 1 may be decomposed into finitely many pieces which can be reassembled to make two spheres of radius 1.

(Some vague idea . . . :)

A variation on the Vitali decomposition, using rotations instead of translations!

Less vague:

Stan Wagon, *The Banach-Tarski Paradox*, Cambridge University Press, 1985 (paperback, 1993). ISBN 0-521-45704-1 (paperback).

Length, Area, Volume

Measures on subsets of $\mathbb{R}^n$: countably additive, invariant under translation and rotation, normalized on the unit cube. What about: finitely additive?

Theorem

- *There is no finitely additive invariant measure on* $\mathbb{R}^3$.
- *There is a finitely additive invariant measure on* $\mathbb{R}^1$ *and on* $\mathbb{R}^2$.

Length, Area, Volume

Measures on subsets of $\mathbb{R}^n$: countably additive, invariant under translation and rotation, normalized on the unit cube.
What about: finitely additive?

Theorem

- *There is no finitely additive invariant measure on $\mathbb{R}^3$.*
- *There is a finitely additive invariant measure on $\mathbb{R}^1$ and on $\mathbb{R}^2$.*

Proof.

For $n = 3$: Banach-Tarski.

Length, Area, Volume

Measures on subsets of $\mathbb{R}^n$: countably additive, invariant under translation and rotation, normalized on the unit cube. What about: finitely additive?

Theorem

- *There is no finitely additive invariant measure on* $\mathbb{R}^3$.
- *There is a finitely additive invariant measure on* $\mathbb{R}^1$ *and on* $\mathbb{R}^2$.

Proof.

For $n = 3$: Banach-Tarski.
For $n = 1, 2$ see Wagon. This also uses *AC*! □

More applications

- A countable union of countable sets is countable. (Needs *AC*!!?!)

More applications

- A countable union of countable sets is countable. (Needs AC!!?!)
- If G is a group, $A \leq G$ an abelian subgroup, then there is a subgroup B with

$$A \leq B \leq G$$

and $C_G(B) = B$. (Exercise)

More applications

- A countable union of countable sets is countable. (Needs *AC*!!?!)
- If G is a group, $A \leq G$ an abelian subgroup, then there is a subgroup B with

$$A \leq B \leq G$$

and $C_G(B) = B$. (Exercise)
- If $h : (A, +) \to (\mathbb{R}, +)$ is a homomorphism, and $A \leq B$ abelian, then h extends to $h' : B \to \mathbb{R}$.

More applications

- A countable union of countable sets is countable. (Needs *AC*!!?!)
- If G is a group, $A \leq G$ an abelian subgroup, then there is a subgroup B with

$$A \leq B \leq G$$

and $C_G(B) = B$. (Exercise)
- If $h : (A, +) \to (\mathbb{R}, +)$ is a homomorphism, and $A \leq B$ abelian, then h extends to $h' : B \to \mathbb{R}$.
- R a commutative ring with 1. Suppose every prime ideal of R is f.g. Then every ideal of R is f.g. (Tricky)

More applications

- A countable union of countable sets is countable. (Needs AC!!?!)
- If G is a group, $A \leq G$ an abelian subgroup, then there is a subgroup B with

$$A \leq B \leq G$$

  and $C_G(B) = B$. (Exercise)
- If $h : (A, +) \to (\mathbb{R}, +)$ is a homomorphism, and $A \leq B$ abelian, then h extends to $h' : B \to \mathbb{R}$.
- R a commutative ring with 1. Suppose every prime ideal of R is f.g. Then every ideal of R is f.g. (Tricky)

More applications

- A countable union of countable sets is countable. (Needs *AC*!!?!)
- If G is a group, $A \leq G$ an abelian subgroup, then there is a subgroup B with
$$A \leq B \leq G$$
and $C_G(B) = B$. (Exercise)
- If $h : (A, +) \to (\mathbb{R}, +)$ is a homomorphism, and $A \leq B$ abelian, then h extends to $h' : B \to \mathbb{R}$.
- R a commutative ring with 1. Suppose every prime ideal of R is f.g. Then every ideal of R is f.g. (Tricky)

Lemma

Let $\mathcal{I}$ be the set of ideals in R which are not f.g. If $\mathcal{I}$ is nonempty, it contains a maximal element.

Famous Applications

Hahn-Banach: Extension of (bounded) linear functions from subspaces.

Tychonoff: A product of compact topological spaces is compact.

Major Contributors, References

Georg Cantor: Theory of ordinals, cardinals, well ordering (ca. 1883, work on sets of uniqueness for trigonometric functions).
Ernst Zermelo, Adolf Fraenkel: axioms for set theory (1908, 1910).
Felix Hausdorff, Stefan Banach, Alfred Tarski: Paradoxical decompositions (1914,1924).
Kazimierz Kuratowski, Max Zorn: Zorn's Lemma (1922,1935).
Paul Cohen: *AC* is not derivable from *ZF* (1963). (Cf. AMS Notices August 2010.)
Hugh Woodin: Under appropriate set theoretic hypotheses, all definable sets of reals are Lebesgue measurable (1984).

References

Thomas J. Jech, *The Axiom of Choice*, North-Holland 1973 and Dover Publications 2008. ISBN-13: 978-0-486-46624-8 (Dover paperback).

Kenneth Ross, *Informal Introduction to Set Theory*, 22 pages, http://math.uoregon.edu/people/ross/SetTheory.pdf

To choose one sock from each of infinitely many pairs of socks requires the Axiom of Choice, but for shoes the Axiom is not needed.—Bertrand Russell.