SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Axiom of Choice

av

Emil Båth

2015 - No 19

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Axiom of Choice

Emil Båth

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Valentin Goranko

2015

Abstract

This thesis investigates how the Axiom of Choice (AC) is used in mathematics. Some weaker forms of AC are presented and proved to follow from AC. The Well-Ordering Theorem, Zorns Lemma and the Fundamental Theorem of Linear Algebra are proven to be equivalent to AC. Two consequences of AC are shown; the useful Boolean Prime Ideal Theorem and the counter-intuitive Banach-Tarski Paradox.

Acknowledgements

I would like to express my gratitude to my supervisor Valentin Goranko for helping me find the topic of the thesis and for his guidance during the writing process. I would also like to thank Christian Espíndola for reviewing the thesis and for helpful comments.

Contents

1 Introduction

The Axiom of Choice states that for any collection of sets we can choose exactly one element from every set. This might seem obvious and almost self-evident at first glance. However, in the case of an infinite collection of sets, where there is no rule for how to pick the elements, the statement is far from trivial. Through history many mathematicians have rejected the axiom and there is still those who look at it with distrust. Despite this, the axiom is used in many different fields of mathematics. In this thesis we will look at some of the implications and equivalents of the axiom, hopefully to shed some light over this usage.

The source of the historical remarks made below is [Moo1982].

The Axiom of Choice grew out of the problem to prove the Well-Ordering Theorem, the statement that every set can be well-ordered (see Definition 2.2.6). This was proposed as a valid ”law of thought” by George Cantor in 1883. Many contemporary mathematicians did not agree with Cantor, and it was in the context of proving the Well-Ordering Theorem that Ernst Zermelo first stated the Axiom of Choice in 1904. We will see in section 4.1 that the Well-Ordering Theorem is actually equivalent to the Axiom of Choice.

In section 2 we define some concepts and prove some results that will be used later in the thesis. In section 3 we give some different formulations of the Axiom of choice and some weaker versions of it. We prove equivalence between the Axiom of Choice, the Well-Ordering Theorem, Zorn's Lemma and the Fundamental Theorem of Linear Algebra in section 4. The Boolean Prime Ideal Theorem and the counter-intuitive Banach-Tarski Paradox is proved to follow from the Axiom of Choice in section 5.

The text requires some basic knowledge of set theory and first-order logic. Some understanding of linear algebra and group theory will be helpful when reading section 4.3, 5.1 and 5.2.

The results in this thesis are well known and I do not claim originality. My intention with this thesis is to gather interesting results which in different ways relate to the Axiom of Choice. By this I hope to give an understanding of how the axiom is used in mathematics, why it is useful and how it is sometimes the cause of unwanted consequences. From this, the reader may be able get her own intuition about the nature of the axiom. Many of the proofs in this text are highly inspired by proofs made by other authors, it is clear where this is the case. I hope that by understanding the proofs and reformulating them with my own words, I have also made them more accessible to the reader.

Now some notational remarks. Upper case letters will be used for sets, except in some cases when we want to emphasize that a set is an element of another set, where lower case letters will be used. In some cases we call a set a family when we want to emphasize that its elements are sets.

2 Preliminaries

2.1 Zermelo-Fraenkel Axioms

The formulations of the Axioms in this section are inspired by Section 1 in [Jec2006].

2.1.1. Axiom of Extensionality: Two sets are equal if they have the same elements:

$$\forall Y \forall Z (\forall X\, (X \in Y \leftrightarrow X \in Z) \rightarrow Y = Z).$$

By the axiom of extensionality a set is defined by its elements.

2.1.2. Axiom of Pairing: For any X and Y there is a set with X and Y as its only members:

$$\forall X\, \forall Y\, \exists Z\, \forall U\, (U \in Z \leftrightarrow U = X \vee U = Y).$$

2.1.3. Axiom Schema of Separation: Let $\varphi(X, P)$ be a formula. For all Y and P, there is a set $Z = \{X \in Y : \varphi(X, P)\}$:

$$\forall Y\, \forall P\, \exists Z\, \forall X\, (X \in Y \wedge \varphi(X, P) \leftrightarrow X \in Z).$$

Note that the Schema of Separation can only be used to construct subsets of a given set and not sets of the more general form $\{X : \varphi(X, P)\}$. Also note that the Axiom Schema of Separation is not one axiom but infinitely many axioms, one axiom for every formula φ.

2.1.4. Axiom of Union: For any family of sets X, there exists a set $Y = \bigcup X$:

$$\forall X\, \exists Y\, \forall Z\, (Z \in Y \leftrightarrow \exists U\, (U \in X \wedge Z \in U)).$$

2.1.5. Axiom of Power Set: For any set X there exists a set $Y = \mathcal{P}(X)$ of all subsets of X:

$$\forall X\, \exists Y\, \forall Z\, (Z \in Y \leftrightarrow \forall U\, (U \in Z \rightarrow U \in X)).$$

The set $Y = \mathcal{P}(X)$ is called the power set of X.

2.1.6. Axiom of Infinity: There exists an infinite set:

$$\exists X (\emptyset \in X \wedge \forall Y (Y \in X \rightarrow Y \cup \{Y\} \in X)).$$

2.1.7. Axiom Schema of Replacement: For any function F, if the domain of F is a set then the range of F is a set:

$$\forall X\,\forall Y\,\forall Z\,(\varphi(X,Y,P)\wedge\varphi(X,Z,P)\rightarrow Y=Z)\rightarrow$$

$$\forall X\,\exists Y\,\forall Z\,(Z\in Y\leftrightarrow\exists U\,(U\in X\wedge\varphi(U,Z,P)),$$

for each formula $\varphi(X,Y,P)$.

2.1.8. Axiom of Regularity: Every set $X\neq\emptyset$ has an element Y such that X and Y are disjoint:

$$\forall X\,(\exists Y\,(Y\in X)\rightarrow\exists Z\,(Z\in X\wedge\neg\exists U\,(U\in X\wedge U\in Z))).$$

The Axiom of Regularity implies that no set is an element of itself.

2.1.9. Axiom of Choice: *See section 3.*

2.2 Basic set theory

Many of the definitions in this section are taken more or less literally from [Jec2006].

The notion of a class is introduced on page 5 in [Jec2006].

Definition 2.2.1. If $\varphi(X,p_1,...,p_n)$ is a formula , we call $C=\{X\mid\varphi(X,p_1,...,p_n)\}$ a **class**. The members of C are all those sets X that satisfies $\varphi(X,p_1,...,p_n)$. Not all classes are sets, and we call a class that is not a set a **proper class**.

Definition 2.2.2. A set X is said to be **countable** if there is a bijection between X and the set $\mathbb{N}$ of natural numbers.

A set that is either finite or countable is said to be **at most countable.**

The following definition corresponds to Definition 2.1 in [Jec2006].

Definition 2.2.3. A **partial order** on a set X is a binary relation, denoted by $<$, with the following properties:

(i) for all $x\in X$, $x\nless x$;

(ii) for all $x, y, z \in X$, if $x < y$ and $y < z$, then $x < z$.

A partial order is a **total order** if moreover

(iii) for all $x, y \in X$ one and only one of the statements

$$x < y, \quad x = y, \quad y < x$$

is true.

If $<$ is a partial (total) order then the relation $\leq$, where $x \leq y$ if either $x < y$ or $x = y$, is also called a partial (total) order.

The following two definitions corresponds to Definition 2.2 in [Jec2006].

Definition 2.2.4. If $(X, <)$ is a partially ordered set, Y is a subset of X and $a \in X$, then:

(i) a is a **maximal** element of Y if $a \in Y$ and for all $x \in Y$, $a \not< x$;

(ii) a is a **minimal** element of Y if $a \in Y$ and for all $x \in Y$, $x \not< a$;

(iii) a is the **greatest** element of Y if $a \in Y$ and for all $x \in Y$, $x \leq a$;

(iv) a is the **least** element of Y if $a \in Y$ and for all $x \in Y$, $a \leq x$;

(v) a is an **upper bound** of Y if for all $x \in Y$, $x \leq a$;

(vi) a is a **lower bound** of Y if for all $x \in Y$, $a \leq x$;

(vii) a is the **supremum** of Y if a is the least upper bound of Y;

(viii) a is the **infimum** of Y if a is the greatest lower bound of Y.

Definition 2.2.5. A bijection f between two partially ordered sets X_1 and X_2 is an **isomorphism** if f and f^{-1} are order-preserving. If there is an isomorphism between two sets X_1 and X_2 we say that X_1 and X_2 are **isomorphic**.

The following definition corresponds to Definition 2.3 in [Jec2006].

Definition 2.2.6. A **well-ordering** on a set X is a total order on X with the property that every non-empty subset of X has a least element in this ordering. The set X together with the well-ordering is called a **well-ordered set**.

Definition 2.2.7. A **choice function** f on a set X is a function from X into $\bigcup X$ such that $f(x) \in x$ for every $x \in X$. That is, a choice f function on a set X selects one element from every element in X.

Definition 2.2.8. A filter $\mathcal{F}$ over a set S is a non-empty proper subset of the power set $\mathcal{P}(S)$ such that

(i) if $X \in \mathcal{F}$ and $X \subseteq Y$, then $Y \in \mathcal{F}$,

(ii) if $X \in \mathcal{F}$ and $Y \in \mathcal{F}$, then $X \cap Y \in \mathcal{F}$.

A set is an *ultrafilter* if

(iii) for each $X \subseteq S$, either $X \in \mathcal{F}$ or $S \backslash X \in \mathcal{F}$.

2.3 Ordinal numbers

In this section we give a definition of the ordinal numbers and show some properties of them. Not all results will be used in the text but they give a good understanding of how the ordinals numbers works. Many of the definitions and results in this section are taken more or less literally from [Jec2006].

We want to define the ordinal numbers so that

$$\alpha < \beta \text{ if and only if } \alpha \in \beta, \text{ and } \alpha = \{\beta \mid \beta < \alpha\}$$

The following two definitions corresponds to Definition 2.9 and 2.10 in [Jec2006].

Definition 2.3.1. A set X is **transitive** if every element of X is a subset of X.

Definition 2.3.2. A set α is an **ordinal number** (an **ordinal**) if α is transitive and well-ordered by $\in$.

We will denote ordinal numbers with lowercase Greek letters $\alpha, \beta, \gamma...$ and the class of all ordinal numbers with *Ord*. We define

$$\alpha < \beta \text{ if and only if } \alpha \in \beta.$$

The following lemma and proof corresponds to Lemma 2.11 in [Jec2006]

Lemma 2.3.3.

(i) $0 = \emptyset \in Ord$

(ii) *If α is an ordinal and $\beta \in \alpha$, then β is an ordinal.*

(iii) *If α and β are ordinals, $\alpha \neq \beta$ and $\alpha \subset \beta$, then $\alpha \in \beta$.*

(iv) *If α and β are ordinals, then either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.*

Proof. (i) and (ii) by definition.

(iii) Suppose $\alpha \subset \beta$ and consider the set $\beta \backslash \alpha = \{\xi \in \beta \mid \xi \notin \alpha\}$. Since β is totally ordered by $\in$, we have that $\beta \backslash \alpha = \{\xi \in \beta \mid \alpha \in \xi \text{ or } \alpha = \xi\}$ and since β is well-ordered, $\beta \backslash \alpha$ has a least element γ. It follows that $\gamma = \alpha$ and thus $\alpha \in \beta$.

(iv) Suppose α and β are ordinals, then $\gamma = \alpha \cap \beta$ is clearly an ordinal. It follows that either $\gamma = \alpha$ or $\gamma = \beta$ for otherwise $\gamma \in \alpha$ and $\gamma \in \beta$ by (iii) and thus $\gamma \in \gamma$ which contradicts the definition of an ordinal.

□

The following proposition corresponds to Proposition 2.12 in [Jec2006], where it is given without a proof.

Proposition 2.3.4.

(i) *Ord is totally ordered by $<$.*

(ii) *For each α, $\alpha = \{\beta \mid \beta < \alpha\}$.*

(iii) *If C is a non-empty class of ordinals, then $\bigcap C$ is an ordinal, $\bigcap C \in C$ and $\bigcap C = \inf C$.*

(iv) *If X is a non-empty set of ordinals, then $\bigcup X$ is an ordinal and $\bigcup X = \sup X$.*

(v) *For each α, $\alpha \cup \{\alpha\}$ is an ordinal and $\alpha \cup \{\alpha\} = \inf \{\beta \mid \alpha < \beta\}$.*

Proof. (i) and (ii) Follows from definition and Lemma 2.3.3.

(iii) For every $\alpha \in C$, α is a set and $\bigcap C \subset \alpha$, hence $\bigcap C$ is a set by the Axiom Schema of Separation 2.1.3.

Let $\alpha \in \bigcap C$, then for every $\beta \in C$, $\alpha \in \beta$ and since β is an ordinal, $\alpha \subset \beta$. It follows that $\alpha \subset \bigcap C$. Thus $\bigcap C$ is transitive.

Let $\alpha, \beta \in \bigcap C$, then $\alpha, \beta \in \mathit{Ord}$ by Lemma 2.3.3. It follows from (i) that either $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$. Thus $\bigcap C$ is totally ordered.

Let B be a non-empty subset of $\bigcap C$ and let $\alpha \in C$, then $B \subseteq \alpha$. Since $\alpha \in \mathit{Ord}$ it is well-ordered and thus B has a least element. So $\bigcap C$ is well-ordered and transitive and thus an ordinal.

We need to show that $\bigcap C$ is the infimum if C. It is a lower bound of C since for all $\alpha \in C$, $\bigcap C \subseteq \alpha$ and thus for all $\alpha \in C$, either $\bigcap C = \alpha$ or $\bigcap C \in \alpha$ by Lemma 2.3.3. It remains to show that $\bigcap C$ is the greatest lower bound of C. Assume, aiming at a contradiction that there is a lower bound β of C such that $\bigcap C \in \beta$. Then since β is a lower bound of C, $\beta \in \alpha$ for all $\alpha \in C$. Thus $\beta \in \bigcap C$ which contradicts the fact that $\bigcap C \in \beta$. So $\bigcap C = \inf C$.

(iv) $\bigcup X$ is a set by the Axiom of Union 2.1.4. Let $\alpha \in \bigcup X$, then for some $\beta \in X$, $\alpha \in \beta$ and, since β is an ordinal, $\alpha \subset \beta \subseteq \bigcup X$. Thus $\bigcup X$ is transitive.

For every $\alpha \in \bigcup X$, there is a $\beta \in X$ such that $\alpha \in \beta$ and since $\beta \in \mathit{Ord}$, $\alpha \in \mathit{Ord}$ by Lemma 2.3.3. Let $\alpha, \beta \in \bigcup X$ such that $\alpha \neq \beta$, then $\alpha, \beta \in \mathit{Ord}$. By Lemma 2.3.3, either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$. Without loss of generality let $\alpha \subseteq \beta$, then $\alpha \in \beta$ by Lemma 2.3.3. Thus $\bigcup X$ is totally ordered.

Let B be a non-empty subset of $\bigcup X$ and let $\alpha \in B$. Consider the set $C = \{\beta \in B \mid \beta < \alpha\} \subseteq \alpha$. If C is empty α is the least element of C

and we are done. Otherwise C has a least element γ since $C \subseteq \alpha$ and α is well-ordered. It follows that γ is the least element of B. So $\bigcup X$ is well-ordered and transitive and thus an ordinal.

For all $\alpha \in X$, $\alpha \subseteq \bigcup X$. Hence, for all $\alpha \in X$, either $\alpha = \bigcup X$ or $\alpha \in \bigcup X$ by Lemma 2.3.3 and thus $\bigcup X$ is an upper bound of X. It remains to show that $\bigcup X$ is the least upper bound of X. Assume, aiming at a contradiction, that β is an upper bound of X such that $\beta \in \bigcup X$. Then β is on ordinal by Lemma 2.3.3. Let $\alpha \in \bigcup X$, then there is some $\gamma \in X$ such that $\alpha \in \gamma$. Since β is an upper bound of X, either $\gamma = \beta$ or $\gamma \in \beta$ and hence $\gamma \subseteq \beta$ by definition. It follows that $\alpha \in \beta$ and thus that $\bigcup X \subseteq \beta$ which contradicts the assumption that $\beta \in \bigcup X$. So $\bigcup X = \sup X$.

(v) $\alpha \cup \{\alpha\}$ is a set by the Axiom of Union 2.1.4. Let $\beta \in \alpha \cup \{\alpha\}$, then either $\beta \in \alpha$ or $\beta = \alpha$. If $\beta \in \alpha$, then $\beta \subset \alpha \subset \alpha \cup \{\alpha\}$, but if $\beta = \alpha$ clearly $\beta \subset \alpha \cup \{\alpha\}$. Thus $\alpha \cup \{\alpha\}$ is transitive.

For every $\beta \in \alpha \cup \{\alpha\}$, $\beta \in Ord$. Hence if $\beta, \gamma \in \alpha \cup \{\alpha\}$ and $\beta \neq \gamma$, then either $\beta \in \gamma$ or $\gamma \in \beta$ by Lemma 2.3.3. Thus $\alpha \cup \{\alpha\}$ is totally ordered.

Let B be a non-empty subset of $\alpha \cup \{\alpha\}$ and let $\beta \in B$. Consider the set $C = \{\gamma \in B \mid \gamma \in \beta\} \subseteq \beta$. If C is empty, then β is the least element if B. Otherwise C has a least element δ since β is an ordinal and thus well-ordered. This element δ is clearly the least element of B. Thus $\alpha \cup \{\alpha\}$ is well-ordered and transitive, i.e $\alpha \cup \{\alpha\}$ is an ordinal.

It remains to show that $\alpha \cup \{\alpha\} = \inf \{\beta \mid \alpha \in \beta\}$. If $\beta \in \{\beta \mid \alpha \in \beta\}$, then $\alpha \in \beta$ and by definition $\alpha \subset \beta$, i.e. for all $\gamma \in \alpha$, $\gamma \in \beta$. Hence $\alpha \cup \{\alpha\} \subseteq \beta$, and it follows from Lemma 2.3.3 that either $\alpha \cup \{\alpha\} = \beta$ or $\alpha \cup \{\alpha\} \in \beta$. Thus $\alpha \cup \{\alpha\}$ is a lower bound of $\{\beta \mid \alpha \in \beta\}$. Since $\alpha \in \alpha \cup \{\alpha\}$, we have that $\alpha \cup \{\alpha\} \in \{\beta \mid \alpha \in \beta\}$. Thus, if b is any lower bound of $\{\beta \mid \alpha \in \beta\}$ different from $\alpha \cup \{\alpha\}$, then $b \in \alpha \cup \{\alpha\}$, i.e $\alpha \cup \{\alpha\} = \inf \{\beta \mid \alpha \in \beta\}$ and the proof is done.

□

In view of this we define the successor of an ordinal α as $\alpha + 1 = \alpha \cup \{\alpha\}$.

An important property of the class of ordinals Ord is that it does not form a set, i.e Ord is a proper set. We prove this below.

Proposition 2.3.5. *The class of ordinals Ord is a proper class.*

Proof. Assume, aiming at a contradiction that Ord is a set. Let $\alpha \in Ord$, then for every $\beta \in \alpha$, $\beta \in Ord$ by Lemma 2.3.3. Thus $\alpha \subset Ord$, i.e Ord is transitive. Ord is totally ordered by Proposition 2.3.4. Let B be a non-empty subset of Ord and let $\alpha \in B$. Consider the set $C = \{\beta \in B \mid \beta \in \alpha\} \subseteq \alpha$. If C is empty, α is the least element of B. Otherwise C has a least element, γ since α is well-ordered. It follows that γ is the least element of B. So Ord is a transitive and well-ordered set and thus $Ord \in Ord$, which contradicts a consequence of the Axiom of Regularity 2.1.8. Hence Ord is a proper class. □

3 The Axiom of Choice and weaker versions

3.1 Axiom of Choice

The Axiom of Choice can be expressed in many different ways. A common form of the axiom, based on the concept of choice functions, can be expressed as follows:

3.1.1. Axiom of Choice (AC): Let X be a family of non-empty sets. Then there is a choice function f on X.

Unless stated otherwise, this is the form of the axiom that will be used throughout this text.

The Axiom of Choice is different from the other axioms in ZF in the sense that it postulates the existence of a set without defining it. This makes AC questionable from a constructive point of view. It can be proved that AC is independent of the other axioms of ZF (for a proof of this see [Jec1973]) and that many mathematical theorems are unprovable in ZF without it.

The question about the existence of a choice function from a family of finitely many non-empty sets is unproblematic, you can just manually pick one element from every set in the family. Even in some cases where we have a family of infinitely many non-empty sets, the existence of a choice function follows from ZF alone. For example, consider the power set $\mathcal{P}(\mathbb{N})$ of the natural numbers. Since the natural numbers are well-ordered by the usual ordering we can define a choice function f on $\mathcal{P}(\mathbb{N})\backslash\{\emptyset\}$ by letting it choose the smallest member from every subset:

$$f : \mathcal{P}(\mathbb{N})\backslash\{\emptyset\} \ \rightarrow \ \mathbb{N},$$

$$f(X) = \min X.$$

The problem arises when it is unclear how, or even impossible to formulate a rule that decides which elements to pick. Consider the problem of defining a choice function from every non-empty subset of the real numbers. The real numbers are not well-ordered by the usual ordering so we cannot just let the function pick the smallest member from every subset. Actually no one has yet found any such rule and there are reasons to believe that no one ever will. It is in cases like this that we need the Axiom of Choice. As Bertrand Russel so elegantly put it;

> The Axiom of Choice is necessary to select one sock from each of infinitely many pairs of socks, but not to select one shoe from each of infinitely many pairs of shoes.

Here, Russel points to the fact that for shoes we can define a rule for which shoe to pick from every pair, since we can just choose the left show from every pair. This rule cannot not be applied for socks since the left and right sock are identical in every pair.

Another formulation of the axiom, equivalent to AC, which instead of the existence of a choice function states the existence of a choice set, can be expressed as follows:

3.1.2. AC': Let $X = \{X_i \mid i \in I\}$ be a family of non-empty sets indexed by some set I. Then there is a set Y such that $|X_i \cap Y| = 1$ for all $i \in I$. The set Y is called a *choice set* on X.

We will not show the equivalence between AC and AC', but it is easily seen by letting $f(X_i)$ be the unique element in $X_i \cap Y$ and the other way around by letting Y be the image of the choice function f.

The following choice principle that states the existence of a function that selects a non-empty and finite subset of every set in a family of non-empty set is also equivalent to AC.

3.1.3. Axiom of Multiple Choice (AMC): Let $X = \{X_i \mid i \in I$ be a family of non-empty sets indexed by some set I. Then there is a function f such that for all $i \in I$, $f(X_i)$ is a non-empty and finite subset if X_i.

The implication from AC to AMC is trivial but the other direction is less well-known. A proof of this can be found in [Jec1973] and will be omitted in this text.

3.2 Weaker versions

In this section some weaker versions of AC will be presented. To prove many of the important consequences of AC, a weaker form of the axiom is sufficient.

3.2.1 Axiom of Dependent Choice

3.2.1. Axiom of Dependent Choice (ADC): Suppose X is a set with a binary relation R such that for every $x \in X$ there is a $y \in X$ such that $x\ R\ y$. Then there is a sequence in $x_0, x_1, ..., x_n, ...$ in X such that $x_n\ R\ x_{n+1}$ for all $n \in \mathbb{N}$.

The following theorem and proof is inspired by the first part of Theorem 2.12 in [Her2006].

Theorem 3.2.2. *AC ⇒ ADC.*

Proof. Let X be a non-empty set and let R be an entire binary relation on X. Then for every $x \in X$, the set $S_x = \{y \in X \mid xRy\}$ is non-empty. By AC, there is a choice function f from the set $\{S_x \mid x \in X\}$ into X such that $f(S_x) \in S_x$ for every $x \in X$. We can define a sequence in X by letting x_0 be an arbitrary element in X and $x_{n+1} = f(x_n)$. Then the sequence (x_n) has the desired property. □

3.2.2 Axiom of Countable Choice

3.2.3. Axiom of Countable Choice (ACC): Any countable family of non-empty sets has a choice function.

The following theorem and proof is inspired by the second part of Theorem 2.12 in [Her2006].

Theorem 3.2.4. *ADC ⇒ ACC.*

Proof. Let $X = \{A_n \mid n \in \mathbb{N}\}$ be a countable family of non-empty sets. For every $n \in \mathbb{N}$ let F_n be the set of all choice functions on $X_n = \{A_i \mid i \leq n\}$ (F_n is non-empty since X_n is finite) and let $F = \bigcup_{n\in\mathbb{N}} F_n$.

We define a relation R on F as follows: Let $f_n \in F_n$ and $f_m \in F_m$. Then $f_n R f_m$ if and only if $m = n + 1$ and for all $i \leq n$, $f_m(A_i) = f_n(A_i)$. The relation R is obviously entire and hence, by DC, there exists a sequence (f_n) in F with $f_n R f_{n+1}$ for all $n \in \mathbb{N}$.

Let $f = \bigcup_{n\in\mathbb{N}} f_n$ (if we view the functions f_n as sets of ordered pairs, this definition makes sense), then f is a choice function on X. □

The implications in Theorem 3.2.2 and 3.2.4 can not be reversed, that is ACC does not imply ADC and ADC does not imply AC. For proof of this, see Chapter 8 in [Jec1973].

Next we show an example of a result where the full strength of AC is not necessary but ACC is sufficient.

Theorem 3.2.5. *A countable union of countable sets is countable.*

Proof. For every $n \in \mathbb{N}$, let X_n be a countable set,

$$X = \bigcup_{n\in\mathbb{N}} X_n,$$

and let F_n be the set of all bijections from X_n into $\mathbb{N}$. It follows from the definition of countable sets that F_n is non-empty.

By ACC we can choose one function f_n from each of the sets F_n.

Now, let $\phi : X \to \mathbb{N} \times \mathbb{N}$ be defined as $\phi(x) = (n, f_n(x))$, where n is the smallest number such that $x \in X_n$. This number n exists and is unique since $\mathbb{N}$ is well-ordered by the usual ordering.

Suppose $x \neq y$, and $\phi(x) = (n, f_n(x))$ and $\phi(y) = (m, f_m(y))$. If $m = n$ then $\phi(x) \neq \phi(y)$ since f_n is injective by assumption. If $m \neq n$, then obviously $\phi(x) \neq \phi(y)$. So ϕ is injective and it follows that X is at most countable and since $X_n \subseteq X$ is infinite, X is countable. □

4 Equivalent statements

4.1 The Well-Ordering Theorem

4.1.1. The Well-Ordering Theorem (WOT): Every set can be well-ordered.

Theorem 4.1.2. *AC ⇒ WOT.*

The following proof is inspired by the proof of Theorem 5.1 in [Jec2006].

Proof. Let X be an arbitrary set and let $\mathcal{P}(X)$ be the power set of X. By the Axiom of Choice, there is a choice function f defined on $\mathcal{P}(X)\backslash\{\emptyset\}$. We can use f to enumerate X with a sequence of ordinals, this we do by transfinite induction:

$$\text{for } \alpha = 0, \text{ let } x_0 := f(X).$$

Suppose x_β has been defined for all $\beta < \alpha$. If $X\backslash\{x_\beta : \beta < \alpha\}$ is empty , we stop. Otherwise

$$x_\alpha := f(X\backslash\{x_\beta : \beta < \alpha\}).$$

Let θ be the least ordinal such that $X = \{x_\alpha : \alpha < \theta\}$. This θ exists since, if it did not we would have constructed an isomorphism between the set X and Ord contradicts the Axiom of Schema of Replacement 2.1.7 since Ord is a proper class. Hence we have constructed an isomorphism between X and the ordinal θ, and we can use the well-ordering of θ to define a well-ordering on X. □

Theorem 4.1.3. *WOT ⇒ AC.*

Proof. Assume that every set can be well-ordered. Let $X = \{X_i \mid i \in I\}$, where I is some set, be a family of non-empty sets, and consider $Y = \bigcup_{i\in I} X_i$. By assumption Y can be well-ordered. It follows that there is a ordering of Y such that every element in X has a least member. Now we can define a function f on X such that for all $X_i \in X$, $f(X_i) = x_i$, where x_i is the least member in X_i. This f is a choice function and the implication is shown. □

4.2 Zorn's lemma

4.2.1. Zorn's Lemma (ZL): Suppose a partial ordered set X has the property that every totally ordered subset has an upper bound in X. Then the set X has at least one maximal element.

Theorem 4.2.2. *$AC \Rightarrow ZL$.*

The following proof is inspired by the proof of Theorem 5.4 in [Jec2006].

Proof. Let X be a set satisfying the conditions in the lemma. We use a choice function f, defined on $\mathcal{P}(X)\backslash\{\emptyset\}$ where $\mathcal{P}(X)$ is the power set of X, to form a totally ordered subset of X that leads to a maximal element in X. We do this by induction:

$$\text{for } \alpha = 0 \text{ let } x_0 = f(X),$$

and if the set $\{y \in X \mid x_\beta < y \quad \text{for all } \beta < \alpha\}$ is non-empty (otherwise x_β is a maximal element and we are done), let

$$x_\alpha = f(\{y \in X \mid x_\beta < y \quad \text{for all } \beta < \alpha\}).$$

This forms a sequence where $x_\beta < x_\alpha$ if $\beta < \alpha$. If α is a limit ordinal, then $\{x_\beta \mid \beta < \alpha\}$ is a totally ordered set, and x_α exists by the assumption that every totally ordered subset of X is bounded above in X. There is an ordinal θ such that there is no $x_{\theta+1} \in S$ such that $x_\theta < x_{\theta+1}$. If there was no such θ we would have defined a bijection between Ord and a subset of X, which contradicts the Axiom of Schema of Replacement 2.1.7 since Ord is a proper class. Thus x_θ is a maximal element of S. □

Theorem 4.2.3. *$ZL \Rightarrow AC$.*

Proof. Let X be a family of non-empty sets and let

$$F = \{f \mid f \text{ is a choice function on some } A \subseteq X\}.$$

F is non-empty, since if A contains a finite number of sets we can define a choice function by manually choosing one element from each set in A. We define an order $\leq$ on F as

$$f_1 \leq f_2 \text{ if and only if } A_1 \subseteq A_2 \text{ and } f_2|_{A_1} = f_1.$$

First we show that $(F, \leq)$ is a partial ordered set. We have that

(i) $f_1 \leq f_1$ since $A_1 \subseteq A_1$ and $f_1|_{A_1} = f_1$,

(ii) if $f_1 \leq f_2$ and $f_2 \leq f_1$, then $A_1 = A_2$, $f_2|_{A_1} = f_1$ and $f_1|_{A_2} = f_2$, so $f_1 = f_2$,

(iii) if $f_1 \leq f_2$ and $f_2 \leq f_3$, then $A_1 \subseteq A_2$, $A_2 \subseteq A_3$, $f_2|_{A_1} = f_1$ and $f_3|_{A_2} = f_2$, so $A_1 \subseteq A_3$ and $f_3|_{A_1} = f_1$, i.e. $f_1 \leq f_3$.

Thus F is partially ordered by $\leq$.

We now show that every totally ordered subset of F has an upper bound in F. Consider a totally ordered subset $G = \{f_i \in P \mid i \in I \text{ for some set } I\}$ of F. We can define a function f on $A = \bigcup_{i \in I} A_i$ such that for all $i \in I$, $f|_{A_i} = f_i$, by $f = \bigcup_{i \in I} f_i$. This function f is an upper bound of G and $f \in F$ since $A \subseteq X$. So every totally ordered set in F has an upper bound in F and we can apply Zorn's lemma to say that F has a maximal element g.

We claim that g is a choice function on X. Assume not, then there is a set $A \in X$ such that g is not defined on A. Let a be an element in A (A is not empty by assumption) and define h as

$$h(B) = \begin{cases} a, & \text{if } B = A \\ g(B), & \text{if } B \neq A \text{ and } B \text{ is in the domain of } g. \end{cases}$$

Then $g < h$, contradicting the fact that g is a maximal element in F. Thus g is a choice function on X and since X was chosen arbitrarily every family of non-empty sets has a choice function. □

4.3 The Fundamental Theorem of Linear Algebra

The following four definitions are taken more or less literally from Appendix A.7 in [BeBl2006].

Definition 4.3.1. A **vector space** over a field F is a set V with a binary operation $+$ defined for all $u, v \in V$ and a **scalar multiplication** $a \cdot v \in V$ defined for all $a \in F$ and $v \in V$ such that the following conditions hold:

(i) $u + v \in V$, for all $u, v \in V$;

(ii) $u + (v + w) = (u + v) + w$, for all $u, v, w \in V$;

(iii) V contains an element 0 such that $0 + v = v$ for all $v \in V$;

(iv) for each $v \in V$ there exists and element $-v$ such that $-v + v = 0$;

(v) $u + v = v + u$, for all $u, v \in V$;

(vi) $a \cdot v \in V$, for all $a \in F$ and all $v \in V$;

(vii) $a(b \cdot v) = (ab) \cdot v$, for all $a, b \in F$ and all $v \in V$;

(viii) $(a + b) \cdot v = a \cdot v + b \cdot v$, for all $a, b \in F$ and all $v \in V$;

(ix) $a \cdot (u + v) = a \cdot u + a \cdot v$, for all $a \in F$ and all $u, v \in V$;

(x) $1 \cdot v = v$, for all $v \in V$.

Definition 4.3.2. Let V be a vector space over the field F, and let S be a set $\{v_1, v_2, ..., v_n\}$ of vectors in V. Any vector of the form $v = \sum_{i=1}^{n} a_i \cdot v_i$, for scalars $a_i \in F$, is called a **linear combination** of the vectors in S. The set of all linear combinations of vectors in S is called the **span** of S, denoted by span(S). The set S is said to span V if span$(S) = V$.

Definition 4.3.3. Let V be a vector space over the field F, and let S be a set of vectors in V. The vectors in S are said to be **linearly dependent** if one of the vectors can be expressed as a linear combination of the others. If not, then S is said to be a **linearly independent** set.

Definition 4.3.4. A subset S of a vector space V is said to be a **basis** of V if S spans V and S is linearly independent.

4.3.5. The Fundamental Theorem of Linear Algebra (FTLA): Every vector space has a basis.

Theorem 4.3.6. *$AC \Rightarrow FTLA$.*

We will prove that ZL implies FTLA, but since ZL is equivalent to AC (as shown in previous section) this is equivalent the fact that AC implies FTLA.

The following proof is inspired by the proof in [I-PW1].

Proof. Let V be a vector space over a field F and let $\mathcal{L}$ be the set of all linear independent subsets of V. The set $\mathcal{L}$ is partially ordered by inclusion.

Let $\mathcal{K}$ be a totally ordered subset of $\mathcal{L}$ and let $K = \bigcup \mathcal{K}$. Assume, aiming at a contradiction, that K is linearly dependent. Then there exists $v_1, v_2, ..., v_n \in K$ and $r_1, r_2, ..., r_n \in F$ such that $r_1 \neq 0$ and $\sum_{k=1}^{n} r_k v_k = 0$. For each such v_i there is some set $K_i \in \mathcal{K}$ such that $v_i \in K_i$. Since $\mathcal{K}$ is totally ordered by inclusion, $K_1 \cup K_2 \cup ... \cup K_n$ must equal K_m for some $m \in \{1, 2, ..., n\}$. But then $K_m = K_1 \cup K_2 \cup ... \cup K_n \in \mathcal{K}$ and so K_m is linearly independent, a contradiction. Thus K is linearly independent and by the construction of K, it is an upper bound of $\mathcal{K}$ in $\mathcal{L}$. Since $\mathcal{K}$ was chosen arbitrarily it follows that every totally ordered subset of $\mathcal{L}$ has an upper bound in $\mathcal{L}$.

By ZL, $\mathcal{L}$ has a maximal element, call it M. We claim that M spans V. Suppose the contrary that there exists an element v of V such that $v \notin \text{span}(M)$. Then $M \cup \{v\}$ is linearly independent and thus $M \subset M \cup \{v\} \in \mathcal{L}$, contradicting the maximality of M. Thus M is a basis for V. □

Theorem 4.3.7. *FTLA ⇒ AC.*

We will use that AC is equivalent to AMC, and prove that FTLA implies AMC.

We need to introduce some notation before we begin with the proof.

The following notational remarks and proof is inspired by the proof in [I-FL]

Let F be a field and X a set and let $F(X)$ be the field of rational functions over F with the elements of X as indeterminates. Then F is a subfield of $F(X)$ and X is a subset of $F(X)$.

Consider a monomial

$$y = ax_1^{r_1}...x_n^{r_n} \text{ with } a \in F\ ,\ x_1, ..., x_n \in X \text{ and } r_1, ..., r_n \in \mathbb{N}.$$

If A is a subset of X then the A-degree of y is the sum of all the exponents r_i for which $x_i \in A$. If y is an arbitrary element in $F(X)$, then we say that y is A-homogeneous of degree d if y is the quotient

$$y = \frac{f(x_1, ...x_n)}{g(x_1, ..., x_n)}$$

of two polynomials such that every monomial of f has the same A-degree d_1 and such that every monomial of g has the same A-degree d_2 with $d_1 - d_2 = d$.

If $\{X_i \mid i \in I\}$ is a family of subsets of X indexed by some index set I, then for $i \in I$ we understand by the i-degree of a monomial its X_i-degree. Similarly we say that an element $y \in F(X)$ is of i-homogeneous degree d if it is of X_i-homogeneous degree d.

Note that the elements of i-homogeneous degree 0 for all $i \in I$ form a subfield of $F(X)$ which we denote by $F_I(X)$.

We are now ready to begin with the proof.

Proof. Let $\{X_i \mid i \in I\}$ be a family of non-empty sets indexed by some set I. We want to show that we can construct a family $\{F_i \mid i \in I\}$ of non-empty and finite sets such that $F_i \subset X_i$ for all $i \in I$.

Without loss of generality we may assume that the sets X_i are pairwise disjoint. We set $X = \bigcup_{i \in I} X_i$.

Let F be any field and $F(X)$ the field of rational functions over F with the elements in X as indeterminants. $F(X)$ is a vector space over the subfield $K = F_I(X)$ and $X \subset F(X)$. Let V be the K-vector space generated by X. By FTLA V has a basis B.

For every $i \in I$ and $x \in X_i$, $x \neq 0$ and thus by the property of a basis there exists a unique non-empty and finite subset $B(x)$ of B such that

$$x = \sum_{b \in B(x)} a_b(x) b$$

with $a_b(x)$ being unique non-zero elements of K. If $x, y \in X_i$, then y/x is j-homogeneous of degree 0 for every $j \in I$ and thus $y/x \in K$. Thus we can multiply x by y/x and obtain

$$y = \sum_{b \in B(x)} (y/x) a_b(x) b = \sum_{b \in B(y)} a_b(y) b.$$

So, we have that $B(x) = B(y)$ and $(y/x)a_b(x) = a_b(y)$ for all $b \in B(x) = B(y)$. Thus $B(x)$ is independent of the choice of x in X_i and the elements $a_b(x)/x$ depend only on $b \in B(x)$. For every $i \in I$ we set $B_i = B(x)$ for some element $x \in X_i$ and for every $b \in B_i$ we set $\beta_b^i = a_b(x)/x$ which are then elements in the field $F(X)$.

Since the elements $a_b(x)$ have i-homogeneous degree 0 we have that β^i_b has i-homogeneous degree -1. Thus, whenever we write β^i_bas a quotient

$$\beta^i_b = \frac{f^i_b(x_1, x_2, ..., x_n)}{g^i_b(x_1, x_2, ..., x_n)}$$

of two polynomials, then some of the finitely many variables $x_1, x_2, ..., x_n \in X$ that are elements in X_i, must appear in the polynomial g^i_b. This is in particular true if we write β^i_b in reduced form. Since the reduced form of an element in $F(X)$ is unique we obtain well defined subsets $F_i \subset X_i$ when we set

$$F_i = \{x \in X_i \mid x \text{ appears in } g^i_b \text{ in reduced form for some } b \in B_i\}.$$

These sets are clearly non-empty and finite and the proof is done. □

5 Consequences

5.1 The Boolean Prime Ideal Theorem

The definitions in this section are taken more or less literally from Chapter 7 in [Jec2006].

Definition 5.1.1. A *Boolean algebra* is a set B with binary operations $+$ and $\cdot$, an unary operation $-$ and two constants 0 and 1. The Boolean operators satisfies the following axioms:

(i) $u + v = v + u$, $\quad u \cdot v = v \cdot u$, (commutativity)

(ii) $u + (v + w) = (u + v) + w$, $\quad u \cdot (v \cdot w) = (u \cdot v) \cdot w$, (associativity)

(iii) $u \cdot (v + w) = (u \cdot v) + (u \cdot w)$, $\quad u + (v \cdot w) = (u + v) \cdot (u + w)$, (distributivity)

(iv) $u \cdot (u + v) = u$, $\quad u + (u \cdot v) = u$, (absorption)

(v) $u + (-u) = 1$, $\quad u \cdot (-u) = 0$, (complementation)

From the axioms of Boolean algebras we can derive additional algebraic rules. Among others we have

$u + u = u,\ u \cdot u = u,\ u + 0 = u,\ u \cdot 0 = 0,\ u + 1 = 1,\ u \cdot 1 = u,\ -(-u) = u,$

and De Morgan's laws

$$-(u + v) = (-u) \cdot (-v) \qquad -(u \cdot v) = (-u) + (-v).$$

We define an ordering $\leq$ on a Boolean algebra as:

$$u \leq v \text{ if and only if } u \cdot (-v) = 0.$$

Definition 5.1.2. An *ideal* on a Boolean algebra B is a non-empty subset I of B such that

(i) if $u \in I$ and $v \leq u$, then $v \in I$,

(ii) if $u \in I$ and $v \in I$, then $u + v \in I$.

If I is a proper subset of B we say that I is a *proper ideal.* A proper ideal I is called a *prime ideal* if moreover

(iii) for all $u \in B$, either $u \in I$ or $-u \in I$.

Definition 5.1.3. A proper ideal I on B is called a *maximal ideal* if for all ideals J such that $I \subseteq J \subseteq B$, either $J = I$ or $J = B$.

Definition 5.1.4. A *filter* $\mathcal{F}$ on a Boolean algebra B is a non-empty proper subset of B such that

(i) if $u \in \mathcal{F}$ and $u \leq v$, then $v \in \mathcal{F}$,

(ii) if $u \in \mathcal{F}$ and $v \in \mathcal{F}$, then $u \cdot v \in \mathcal{F}$.

$\mathcal{F}$ is an *ultrafilter* if

(iii) for all $u \in B$, either $u \in \mathcal{F}$ or $-u \in \mathcal{F}$.

Theorem 5.1.5 (The Boolean Prime Ideal Theorem)**.** *Every proper ideal I on a Boolean algebra B can be extended to a prime ideal.*

Proof. Let B be a Boolean algebra, I a proper ideal on B and let S be the set of all proper ideals on B that contains I. Since $I \in S$, S is non-empty. S is partially ordered by inclusion. Let T be a totally ordered subset of S and let $U = \bigcup T$. Then U contains I.

Let $u \in U$ and $v \leq u$, then there is some ideal $J \in T$ such that $u \in J$ which implies that $v \in J$. Hence $v \in U$.

Let $u, v \in U$, then there is some ideals $J_1, J_2 \in T$ such that $u \in J_1$ and $v \in J_2$, and since T is totally ordered by inclusion either $J_1 \subseteq J_2$ or $J_2 \subseteq J_1$, thus $u, v \in J_i$ for some $i \in \{1, 2\}$, which gives that $u + v \in J_i$. Hence $u + v \in U$.

It follows that U is a proper ideal on B and U is an upper bound of T in S. By ZL, T has a maximal element, call it M.

We need to show that M is a prime ideal on B (This part of the proof is inspired by the proof of Proposition 1.4.1 in [Gon1997]). Assume that M is not a prime ideal, aiming at a contradiction, then there is some element $u \in B$ such that $u \notin M$ and $-u \notin M$. Consider the sets

$$M_u = \{x \in B \mid x \leq u + m \text{ for some } m \in M\}$$

and

$$M_{-u} = \{x \in B \mid x \leq (-u) + m \text{ for some } m \in M\}.$$

We claim that M_u and M_{-u} are ideals, to see this we show that M_u and M_{-u} satisfies the conditions in Def. 5.2.2.;

(i) If $x \in M_u$, $y \in B$ and $y \leq x$, then there exists some $m \in M$ such that $x + (u + m) = u + m$ and $y + x = x$. Thus

$$y + (u + m) = y + (x + (u + m)) = x + (u + m) = u + m,$$

i.e. $y \leq u + m$ which implies that $y \in M_u$

(ii) If $x, y \in M_u$, then there exists some $m_1, m_2 \in M$ such that $x + (u + m_1) = u + m_1$ and $y + (u + m_2) = u + m_2$. Thus

$$x+y+(u+(m_1+m_2)) = x+(u+m_1)+y+(u+m_2) = (u+m_1)+(u+m_2) =$$

$$= u + (m_1 + m_2),$$

i.e. $x + y \leq u + (m_1 + m_2)$ which implies that $x + y \in M_u$

Hence, M_u is an ideal and we can prove in a similar way that M_{-u} is an ideal. Clearly, $M \subsetneq M_u$ and $M \subsetneq M_{-u}$ and since M is maximal we have that $M_u = M_{-u} = B$. Hence, there exists $a, b \in M$ such that $a + u = 1$ and $b + (-u) = 1$ and therefore

$$\begin{aligned} &a + b = (a + b) + 0 = (a + b) + (u \cdot (-u)) = \\ &= ((a + b) + u) \cdot ((a + b) + (-u)) = (b + 1) \cdot (a + 1) = 1 \cdot 1 = 1. \end{aligned}$$

This implies that $1 \in M$ but M is proper, i.e. $1 \notin M$. A contradiction! Thus M is prime and the proof is done.

□

The Boolean Prime Ideal Theorem is equivalent to the statement that every filter on a Boolean algebra can be extended to an ultrafilter, since filters and ultrafilters is the dual notion of ideals and prime ideals. Note that if S is a non-empty set, the power set $\mathcal{P}(S)$ together with the set theoretical operations $\cup$, $\cap$ and $S\setminus$ is a Boolean algebra with $0 = \emptyset$ and $1 = S$. In this special case, the notion of filters and ultrafilters coincide with Definition 2.2.8. Thus we have:

Theorem 5.1.6 (The Ultrafilter Theorem)**.** *Every proper filter over a set S can be extended to an ultrafilter.*

The Ultrafilter Theorem is equivalent to the Boolean Prime Ideal Theorem, this is proved without use of AC in Theorem 2.2 in [Jec1973].

The Boolean Prime Ideal Theorem does not imply AC, for a proof of this see Theorem 7.1 in [Jec1973]. However it has a lot of interesting equivalents and implications. For example it is equivalent to The Compactness Theorem which is the following statement:

Theorem 5.1.7 (The Compactness Theorem)**.** *A set of sentences Σ in first-order logic has a model if and only if every finite subset of Σ has a model.*

The equivalence between the Boolean Prime Ideal Theorem and the Compactness Theorem is proved in Theorem 2.2 in [Jec1973].

An example of an implication of the Boolean Prime Ideal Theorem is

Theorem 5.1.8 (The Order Extension Principle)**.** *Every partial ordering of a set X can be extended to a total ordering of X.*

A proof of the Order Extension Principle from the Boolean Prime Ideal Theorem can be found in section 2.3 in [Jec1973].

5.2 The Banach-Tarski Paradox

The method of proving the Banach-Tarski Paradox that is used in this section is inspired by Appendix G in [Coh2013] and many definitions and formulations are taken more or less literally from it.

The Banach-Tarski Paradox is usually stated informally as:

> A three-dimensional ball can be decomposed into a finite number of pieces which can be reassembled into two copies of the original ball.

First we need to define some concepts and prove some statements that are used in the proof of the paradox.

5.2.1 Equidecomposability and Paradoxical Sets

Definition 5.2.1. Let G be a group and let X be a set. A multiplication of elements of X by elements of G, defined by a function from $G \times X \to X$, is called a **group action** of G on X provided that for each $x \in X$:

(i) $g_1(g_2x) = (g_1g_2)x$ for all $g_1, g_2 \in G$, and

(ii) $ex = x$ where e is the identity element of G.

If G acts on X, $g \in G$ and $A \subseteq X$, then gA is the set $\{ga \mid a \in A\}$.

The following definition corresponds to Definition 7.3.3 in [BeBl2006].

Definition 5.2.2. Let G be a group acting on a set X. For each element $x \in X$, the set

$$Gx = \{gx \mid g \in G\}$$

is called the **orbit** of x under G, and the set

$$G_x = \{g \in G \mid gx = x\}$$

is called the **stabilizer** of x in G.

Definition 5.2.3. Let G be a group acting on a set X and let A and B be subsets of X. Then A and B are called G**-equidecomposable** if there exists a positive integer n, partitions $\{A_1, A_2, ..., A_n\}$ of A and $\{B_1, B_2, ..., B_n\}$ of B and elements $g_1, g_2, ..., g_n$ of G such that $B_i = g_iA_i$, for $i = 1, 2, ..., n$.

If the sets A and B are G-equidecomposable we write $A \sim_G B$

Note that A and B are G-equidecomposable if and only if there are partitions of A and B and elements of G ,defined as in the definition, and a bijection $f : A \to B$ defined piecewise as $f(x) = g_i x$ if $x \in A_i$ for $i = 1, 2, ..., n$.

The following proposition corresponds to Proposition G.2 in [Coh2013].

Proposition 5.2.4. *Suppose that the group G acts on the set X and that A and B are subsets of X. If A is G-equidecomposable with a subset of B and if B is G-equidecomposable with a subset of A, then $A \sim_G B$.*

Proof. Let A be G-equidecomposable with $B' \subseteq B$ and let B be G-equidecomposable with $A' \subseteq A$. Then there exists bijections $f : A \to B'$ and $g : B \to A'$ defined piecewise by the action of G on X.

Consider the function $h : A \to B$ defined as:

$$h(x) = \begin{cases} f(x), & \text{if } x \in A \backslash A' \text{ or } g^{-1}(x) \in B' \\ g^{-1}(x), & \text{if } x \in A' \text{ and } g^{-1}(x) \in B \backslash B'. \end{cases}$$

The function h is well defined since it is defined for all $x \in A$ and the conditions for which function to use never coincide. It is surjective since if $y \in B'$ then there is an element x in A such that $f(x) = y$ and if $y \in B \backslash B'$ then there is an element x in $A' \subseteq A$ such that $g^{-1}(x) = y$. Finally, h is injective since if $h(x) = h(y)$ then either $f(x) = f(y)$ which implies that $x = y$ since f is bijective, $g^{-1}(x) = g^{-1}(y)$ which also implies that $x = y$ since g is bijective or $f(x) = g^{-1}(y)$ which cannot be the case since if it were, then $h(x) = f(x) \in B \backslash B'$ which contradicts the definition of f. So h is a bijection and since f and g are bijective and defined piecewise by the action of G on X, so is h. It follows that $A \sim_G B$. □

Definition 5.2.5. Let G be a group acting on a set X. A subset A of X is called **G-paradoxical** if it can be partitioned into two disjoint subsets A_1 and A_2 such that both A_1 and A_2 are G-equidecomposable with A.

The following corollary to Proposition 5.2.4 provides an easier way to show that a set A is paradoxical, we only have to look at disjoint subsets of A without the condition that the subsets partitions A. The corollary corresponds to Corollary G.4. in [Coh2013].

Corollary 5.2.6. *Let G be a group acting on a set X. Then a subset A of X is G-paradoxical if it has two disjoint subsets A_1 and A_2, each of which is G-equidecomposable with A.*

Proof. Suppose A, A_1 and A_2 are as in the statement of the corollary. Then the set $A \backslash A_1$ is G-equidecomposable with a subset of A, namely it is G-equidecomposable with itself, and A is G-equidecomposable to a subset of $A \backslash A_1$, namely A_2. So, by Proposition 5.3.4., A is G-equidecomposable with $A \backslash A_1$ and since A_1 and $A \backslash A_1$ are disjoint and partitions A, it follows that A is paradoxical. □

5.2.2 The Free Group of two Generators and the Special Orthogonal Group

Definition 5.2.7. The free group F_2 of two generators a and b is the set of all finite words with the letters a, a^{-1}, b and b^{-1} such that a and a^{-1} are never adjacent and neither are b and b^{-1}.

If $x = x_0x_1...x_n$ and $y = y_0y_1...y_m$ are elements of F_2, then we get the product xy by joining the two words together and removing all adjacent pairs of letters of the form $\{a, a^{-1}\}$ or $\{b, b^{-1}\}$ until we have achieved a reduced word.

The empty word is the identity element of F_2.

The following proposition corresponds the Proposition G.5. in [Coh2013].

Proposition 5.2.8. *The free group F_2 of two generators is paradoxical under the action of F_2.*

Proof. We can define a paradoxical decomposition of F_2 as follows: let $S(a)$ be the set of all elements of F_2 starting with a, and let $S(a^{-1})$, $S(b)$ and $S(b^{-1})$ be defined similarly. Then the two sets $A_1 = S(a) \cup S(a^{-1})$ and $A_2 = S(b) \cup S(b^{-1})$ are disjoint. We have that $S(a) \cup aS(a^{-1}) = F_2$ and that $S(b) \cup bS(b^{-1}) = F_2$. Thus $A_1 \sim_{F_2} F_2$ and $A_2 \sim_{F_2} F_2$. So, by Corollary 5.1.5., F_2 is F_2-paradoxical . □

Definition 5.2.9. For some positive integer n, the set of all $n \times n$ matrices whose rows and columns are orthogonal unit vectors (i.e. orthogonal matrices) with determinant 1 is called **the special orthogonal group** and is denoted $SO(n)$.

Every element of $SO(3)$, when interpreted as an action on $\mathbb{R}^3$, is a rotation around a line through the origin and every such rotation is represented by an element in $SO(3)$.

The following proposition corresponds to Proposition G.6. in [Coh2013].

Proposition 5.2.10. *The special orthogonal group $SO(3)$ has a subgroup that is free on two generators.*

Proof. To prove that two elements a and b of $SO(3)$ freely generates a subgroup of $SO(3)$, it is sufficient to show that any two distinct reduced words x and y in the letters a, a^{-1}, b and b^{-1} represents different elements of $SO(3)$. Assume that x and y are two distinct such words, but that they represents the same element of $SO(3)$. We can assume that the first letter (from the left) of x is different from the first letter of y, since if the x and y begins with the same letter we can, by the cancellation property of groups, remove elements from the left until the words begins with different letters. So, we want to find two elements a and b of $SO(3)$ such that the elements of $SO(3)$ represented by two distinct reduced words x and y in the letters a, a^{-1}, b and b^{-1} with different first letters (from the left) are always distinct.

If we can find two elements $a, b \in SO(3)$, one element $u \in \mathbb{R}^3$ and four disjoint subsets A_+, A_-, B_+ and B_- of $\mathbb{R}^3$ such that the following conditions holds:

$$\begin{aligned}
u &\notin A_+ \cup A_- \cup B_+ \cup B_- \\
a \cdot (A_+ \cup A_- \cup B_+ \cup B_- \cup \{u\}) &\subseteq A_+ \\
a^{-1} \cdot (A_+ \cup A_- \cup B_+ \cup B_- \cup \{u\}) &\subseteq A_- \\
b \cdot (A_+ \cup A_- \cup B_+ \cup B_- \cup \{u\}) &\subseteq B_+ \\
b^{-1} \cdot (A_+ \cup A_- \cup B_+ \cup B_- \cup \{u\}) &\subseteq B_-,
\end{aligned}$$

then the proof is done, since operating on u with elements of $SO(3)$ represented by distinct reduced words with different first letter will give elements in different disjoint subsets of $\mathbb{R}^3$.

Let $a, b \in SO(3)$, $u \in \mathbb{R}^3$ and the subsets A_+, A_-, B_+, B_- of $\mathbb{R}^3$ be defined as follows:

$$a = \begin{pmatrix} 3/5 & 4/5 & 0 \\ -4/5 & 3/5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3/5 & -4/5 \\ 0 & 4/5 & 3/5 \end{pmatrix},$$

$$u = (0,1,0)^t,$$

$$A_+ = \left\{ \frac{1}{5^k}(x,y,z)^t \mid k \geq 1,\ x \equiv 3y \bmod 5,\ x \not\equiv 0 \bmod 5,\ z \equiv 0 \bmod 5 \right\},$$

$$A_- = \left\{ \frac{1}{5^k}(x,y,z)^t \mid k \geq 1,\ x \equiv -3y \bmod 5,\ x \not\equiv 0 \bmod 5,\ z \equiv 0 \bmod 5 \right\},$$

$$B_+ = \left\{ \frac{1}{5^k}(x,y,z)^t \mid k \geq 1,\ z \equiv 3y \bmod 5,\ z \not\equiv 0 \bmod 5,\ x \equiv 0 \bmod 5 \right\},$$

$$B_- = \left\{ \frac{1}{5^k}(x,y,z)^t \mid k \geq 1,\ z \equiv -3y \bmod 5,\ z \not\equiv 0 \bmod 5,\ x \equiv 0 \bmod 5 \right\},$$

where k, x, y and z are integers.

First we show that the subsets A_+, A_-, B_+ and B_- are disjoint. To simplify the notation we omit mod5 in the rest of the proof. Assume$1/5^k(x,y,z) \in A_+ \cap A_-$, then we have that

$$x \equiv 3y \equiv -3y \Rightarrow 6y \equiv 0 \Rightarrow y \equiv 0 \Rightarrow x \equiv 0,$$

contradicting $x \not\equiv 0$, so $A_+ \cap A_- = \emptyset$. By the same argument $B_+ \cap B_- = \emptyset$, and finally $A_+ \cap B_+ = A_+ \cap B_- = A_- \cap B_+ = A_- \cap B_- = \emptyset$ since otherwise $x \equiv 0$ and $x \not\equiv 0$.

Since $u = (0,1,0)^t = 1/5^k(0,5^k,0)^t$ and $0 \equiv 0 \bmod 5$, u is not in any of the subsets A_+, A_-, B_+, B_-, i.e. $u \notin A_+ \cup A_- \cup B_+ \cup B_-$.

To prove $a \cdot (A_+ \cup A_- \cup B_+ \cup B_- \cup \{u\}) \subseteq A_+$, consider a operating on the element $v = 1/5^k(x,y,z)$

$$a \cdot \frac{1}{5^k}(x,y,z)^t = \frac{1}{5^{k+1}}(3x+4y, -4x+3y, 5z).$$

If $v \in A_+$, then

$$\begin{cases} x \equiv 3y \\ x \not\equiv 0 \\ z \equiv 0 \end{cases} \Rightarrow \begin{cases} 3x + 4y \equiv 3x + 9y \equiv 3x + 3x = 3 \cdot 2x \\ -4x + 3y \equiv x + x = 2x \not\equiv 0 \\ 5z \equiv 0 \end{cases} \Rightarrow a \cdot v \in A_+.$$

We can use similar arguments to prove that $a \cdot v \in A_+$ for $v \in A_-$, $v \in B_+$ and $v \in B_-$ or $v = u$. Showing the rest of the required conditions can be done in a similar manner and the proposition is proved. □

5.2.3 Paradoxicality of the Unit-Ball

The following proposition corresponds to Proposition G.7. in [Coh2013].

Proposition 5.2.11. *Let G be a group for which the action of G on itself is paradoxical, let $(g, x) \mapsto g \cdot x$ be an action on a set X, and suppose that the stabilizer G_x of every $x \in X$ in G is trivial. Then the action of G on X is paradoxical.*

Proof. Define a relation $\dot{\sim}$ on X by $x \dot{\sim} y$ if $y = g \cdot x$ for some $g \in G$. Then we have that for all $x, y, z \in X$

(i) $x = e \cdot x$,

(ii) if $y = g \cdot x$, then $x = g^{-1} \cdot y$,

(iii) if $y = g_1 \cdot x$ and $z = g_2 \cdot y$, then $z = g_2 g_1 \cdot x$,

showing that $\dot{\sim}$ is reflexive, symmetric and transitive and thus an equivalence relation. The equivalence class of each element $x \in X$ is the orbit of x under G. We can now use the Axiom of Choice to form a set C containing one element from each orbit in X.

Since G is G-paradoxical there is a partition of G into two sets A and B such that $A \sim_G G$ and $B \sim_G G$. Then $A \cdot C \cup B \cdot C = X$ since $G \cdot C = X$ and $A \cdot C \cap B \cdot C = \emptyset$, since if $u \in A \cdot C \cap B \cdot C$ then $u = ac = bc$ for some $a \in A$, $b \in B$ and $c \in C$ which implies that $a = b$, since the stabilizer of c is trivial by assumption, but that is impossible since A and B are disjoint. Thus $A \cdot C$ and $B \cdot C$ partitions X. Since $G \sim_G A$ we must have that $G \cdot C \sim_G A \cdot C$ and hence $X \sim_G A \cdot C$. A similar argument shows that $X \sim_G B \cdot C$ and the proof is done. □

Lemma 5.2.12. *The free group F_2 of two generators is countable.*

Proof. For every $n \in \mathbb{N}$ there are finitely many different words of length n in four letters and since F_2 is the union of such words over $\mathbb{N}$ it follows from Theorem 3.2.5 that F_2 is countable. □

The following proposition corresponds to Proposition G.8. in [Coh2013].

Proposition 5.2.13. *Let F be a subgroup of $SO(3)$ that is free on two generators. Then there is a countable subset D of the unit-sphere S such that $S \backslash D$ is F-paradoxical and hence $SO(3)$-paradoxical.*

Proof. Since the elements of $SO(3)$ are distance preserving as operators on $\mathbb{R}^3$, so are the elements of F, and hence we can view them as acting on S. All elements of F but the identity element is a non-trivial rotation about a line through the origin and so has exactly two fixed points on S. Let D be the collection of all fixed points on S of elements of F other than the identity element. Since F is countable by Lemma 5.2.12, so is D.

The elements of F have no fixed points in $S \backslash D$. $S \backslash D$ is closed under action of elements of F, since if $f \in F$, $x \in S \backslash D$ and $fx \in D$ then there would exist some non-trivial element $f' \in F$ such that $f'fx = fx$ from which it follows that $f^{-1}f'fx = x$ and hence that $f^{-1}f'f = e$ which implies that $f' = e$ contrary to our assumption that $f' \neq e$. It follows from Proposition 5.2.11. that $S \backslash D$ is F-paradoxical and since $F \subseteq SO(3)$, $S \backslash D$ is $SO(3)$-paradoxical. □

The following proposition corresponds to Proposition G.9. in [Coh2013].

Proposition 5.2.14. *The unit-sphere S is $SO(3)$-paradoxical.*

Proof. Let F be a subgroup of $SO(3)$ that is free on two generators, and let D be a countable subset of S such that $S \backslash D$ is F-paradoxical.

There is a line L that goes through the origin but not through any of the points in D. This line L exists since D is countable, and hence there are only countably many lines that go through the origin and a point of D, but S is uncountable and so L must exist. All non-trivial rotations about L can be described in terms of values in the interval $(0, 2\pi)$. For each pair of points $x, y \in S$ there is at most one rotation that takes x to y. Thus there are only countable many rotations ρ about L such that $D \cap \rho(D) \neq \emptyset$. By the same argument we can show that for any $n \in \mathbb{N}$ there are only countably many rotations ρ about L such that $D \cap \rho^n(D) \neq \emptyset$. Since there are uncountably many rotations about L we can choose one, say ρ_0, such that for every positive integer n, $D \cap \rho^n(D) = \emptyset$. It follows that for any positive integers n and k, $\rho^n(D) \cap \rho^{n+k}(D) = \emptyset$, and hence that the sequence $D, \rho(D), \rho^2(D), ...$ consists of disjoint sets.

Let $D^{1,\infty} = \bigcup_{i=1}^{\infty} \rho^i(D)$ and let $D^{0,\infty} = \bigcup_{i=0}^{\infty} \rho^i(D)$. Then $S = (S \backslash D^{0,\infty}) \cup D^{0,\infty}$ and $S \backslash D = (S \backslash D^{0,\infty}) \cup D^{1,\infty}$. Since $D^{1,\infty} = \rho D^{0,\infty}$, it follows that S and $S \backslash D$ are $SO(3)$-equidecomposable. Since $S \backslash D$ is F-paradoxical it follows from Corollary 5.2.6. that S is F-paradoxical and hence $SO(3)$-paradoxical. □

The following proposition corresponds to Proposition G.10. in [Coh2013].

Proposition 5.2.15. *The unit-ball B with its center removed,*
$\{x \in \mathbb{R} \mid 0 < |x| \leq 1\}$ is $SO(3)$-paradoxical.

Proof. Let S be the unit-sphere and for each subset $E \subseteq S$ let $c(E)$ be the conical piece of the unit-ball B defined by

$$c(E) = \{ts \in \mathbb{R}^3 \mid t \in (0,1] \text{ and } s \in E\}.$$

Then $c(S)$ is B with its center removed. Let A and B be subsets of S such that A and B partitions S, $S \sim_{SO(3)} A$ and $S \sim_{SO(3)} B$ (such subsets exists since S is $SO(3)$-paradoxical by Proposition 5.1.14). Then $c(A)$ and $c(B)$ partitions $c(S)$, $c(S) \sim_{SO(3)} c(A)$ and $c(s) \sim_{SO(3)} c(B)$. We can show that $c(S) \sim_{SO(3)} c(A)$ by considering a bijection $f : S \to A$ that is piecewise defined by the action of $SO(3)$ on S, and note that $g : c(S) \to c(A)$ defined by $tx \mapsto tf(x)$ is also a bijection defined piecewise by the same group action. Thus $c(S) \sim_{SO(3)} c(A)$, and by the same argument we can show that $c(S) \sim_{SO(3)} c(B)$. Since $c(S)$ is the unit-ball B with its center removed, the proof is done. □

Definition 5.2.16. The **group of rigid motions G_3** is the set consisting of all functions $T : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $T(x) = Sx + b$, where $S \in SO(3)$ and $b \in \mathbb{R}^3$.

The set G_3 is a group under function compositions, every element in G_3, when viewed as an action on $\mathbb{R}^3$, represents a rigid motion in $\mathbb{R}^3$ and conversely every rigid motion in $\mathbb{R}^3$ can be represented by an element in G_3

The following proposition corresponds to Proposition G.11. in [Coh2013].

Proposition 5.2.17. *The unit-ball B is G_3-paradoxical.*

Proof. Let L be a line that does not pass through the origin but is close enough so that every rotation about L maps 0 to a point in B. Note that the rotations about L are elements of G_3 but not $SO(3)$. Now, let ρ be a rotation about L through an angle $\theta \in (0, 2\pi)$ such that $\frac{\theta}{2\pi}$ is irrational, in which case the elements in the sequence $0, \rho(0), \rho^2(0), ...$ are distinct. This can be shown by assuming the contrary, that is for some non-negative integers i and j such that $j < i$, $\rho^i(0) = \rho^j(0)$. Then $\rho^{i-j}(0) = 0$ and hence ρ^{i-j} is a rotation about L through an angle $2n\pi$, for some positive integer n. So we have that ρ is a rotation through an angle $\theta = \frac{2n\pi}{i-j}$, but then $\frac{\theta}{2\pi} = \frac{n}{i-j} \in \mathbb{Q}$ which contradicts that $\frac{\theta}{2\pi}$ is irrational.

Let $D^0 = \{0\} \cup \{\rho^n(0) \mid n \geq 1\}$ and $D^1 = \{\rho^n(0) \mid n \geq 1\}$, then $B = (B \backslash D^0) \cup D^0$ and $B \backslash \{0\} = (B \backslash D^0) \cup D^1$. Since $D^1 = \rho D^0$, it follows that $B \sim_{g_3} B \backslash \{0\}$ and so, by Proposition 5.1.15 and Corollary 5.1.6., B is G_3-paradoxical. □

5.2.4 Proof of the Paradox

We can now formulate and prove the precise version of the Banach-Tarski Paradox. The theorem corresponds to Theorem G.3. in [Coh2013].

Theorem 5.2.18 (The Banach-Tarski Paradox)**.** *Let A and B be subsets of $\mathbb{R}^3$ that are bounded and have non-empty interiors. Then A and B are G_3-equidecomposable.*

Note that this version of the paradox is much more general than the informal statement, but that the informal statement clearly follows.

Proof. Since the unit-ball B is G_3-paradoxical it follows that any ball in $\mathbb{R}^3$ is G_3-paradoxical. This is intuitively clear but to prove it, for each subset E of B let $c(E)$ be the set

$$c(E) = \{rx + c \mid x \in E \text{ , } r \in \mathbb{R} \text{ and } c \in \mathbb{R}^3\}.$$

Then the ball $B_{r,c}$ with radius r and center in c is equal to $c(B)$. Now, let X and Y be subsets of B such that X and Y partitions B and such that both X and Y are G_3-equidecomposable with B. Then $c(B) = c(X) \cup c(Y)$ and $c(X) \cup c(Y) = \emptyset$ and both $c(X)$ and $c(Y)$ is G_3-equidecomposable with $c(B)$. We can show that $c(B) \sim_{G_3} c(X)$ by considering a bijection $f : B \to X$ that is piecewise defined by the action of G_3 on B, and note that $g : c(B) \to c(X)$ defined by $rx + c \mapsto rf(x) + c$ is also a bijection defined piecewise by the same group action. Thus $c(B) \sim_{G_3} c(X)$, and by the same argument we can show that $c(B) \sim_{G_3} c(Y)$. Since $c(B) = B_{c,r}$ for arbitrary c and r, every ball in $\mathbb{R}^3$ is paradoxical.

Let A and B be bounded subsets of $\mathbb{R}^3$ with non-empty interiors and let B_0 be a ball with radius r that is contained in A. Let $B_1, B_2, ...$ be disjoint balls each with radius r. Since B_0 is paradoxical, by the argument above, it follows that B_0 is G_3-equidecomposable with $B_1 \cup B_2$. By repeating this argument we can conclude that B_0 is G_3-equidecomposable with $B_1 \cup B_2 \cup ... \cup B_n$, for some positive integer n. Since B is bounded there is an positive integer n such that B can be covered by n balls of radius r. It follows that B is G_3-equidecomposable with a subset of $B_1 \cup B_2 \cup ... \cup B_n$ and hence with B_0 which is a subset of A. So B is G_3-equidecomposable with a subset of A and with a similar argument we can show that A is G_3-equidecomposable with a subset of B. This implies, by Proposition 5.1.6., that $A \sim_{G_3} B$ and the proof is complete. □

5.2.5 Summary of the Proof

We now summarize the proof of the Banach-Tarski Paradox.

What the paradox is really saying is that any two bounded subsets A and B of $\mathbb{R}^3$ with non-empty interior are G_3-equidecomposable. That is, A and B can be partitioned into a finite number of subsets $A = A_1 \cup A_2 \cup ... \cup A_n$ and $B = B_1 \cup B_2 \cup ... \cup B_n$, and for each i there is an element $g_i \in G_3$ such that $g_i A_i = B_i$. Here G_3 is the group of rigid motions acting on $\mathbb{R}^3$ by taking an element x to $rx + t$, where $r \in SO(3)$ and $t \in \mathbb{R}^3$. $SO(3)$ is, when interpreted as a group acting on $\mathbb{R}^3$, the group of rotations about lines that goes through the origin. So the action of G_3 on $\mathbb{R}^3$ takes an object, rotates it and translates it.

We started by showing that a free group F_2 on two generators is F_2-paradoxical

(Proposition 5.2.8), that is F_2 can be partitioned into two disjoints subsets, both of which are F_2-equidecomposable to F_2. Then we showed that $SO(3)$ has a subgroup that is free on two generators (Proposition 5.2.10), and thus the subgroup is paradoxical. This was used to prove, in the given order, that, $S \backslash D$, where S is the unit-sphere and D is a countable subset of S, the unit-sphere S itself and the unit-ball B with its center removed are all $SO(3)$-paradoxical (Proposition 5.2.13, 5.2.14 and 5.2.15).

By showing that $B \backslash \{0\}$ is G_3-equidecomposable to B, and by the previous results we concluded that B is G_3-paradoxical (Proposition 5.2.17). It follows that any ball in $\mathbb{R}^3$ is G_3-paradoxical and furthermore that any bounded subsets A and B of $\mathbb{R}^3$ with non-empty interior are G_3-equidecomposable.

A consequence of the Banach-Tarski Paradox is that not every bounded subset of $\mathbb{R}$ is Lebesgue-measurable.

6 Outroduction

6.1 A Stronger Statement

An example of a statement that is stronger than AC, is the Generalized Continuum hypothesis.

The Continuum Hypothesis states that there is no set with cardinality strictly between the cardinality of $\mathbb{N}$ and the cardinality of $\mathbb{R}$. A cardinal is the generalized concept of "the number of elements" in a finite set and can be seen as the "size" of a set. The Continuum Hypothesis can be expressed as follows:

6.1.1. The Continuum Hypothesis: If $\aleph_0 \leq b < 2^{\aleph_0}$, then $b = \aleph_0$, where $\aleph_0$ is the cardinality of $\mathbb{N}$.

The Generalized Continuum Hypothesis is the following statement:

6.1.2. The Generalized Continuum Hypothesis: For any two infinite cardinals a and b, if $a \leq b < 2^a$, then $a = b$.

The definitions of the Continuum Hypothesis and the Generalized Continuum Hypothesis are inspired by Definition 2.19 in [Her2006].

The following theorem we state without proof, a proof of the theorem can be found in [Jec1973].

Theorem 6.1.3. *The Generalized Continuum Hypothesis implies AC.*

The implication does not go the other way around, AC does not even imply the weaker Continuum Hypothesis, this was proved be Paul J. Cohen in [Coh1963].

6.2 An Alternative to the Axiom of Choice

This section is inspired by Section 7.2 in [Her2006].

An alternative to AC is the Axiom of Determinateness. The Axiom of Determinateness states that a special type of infinite games of two players is determined, that is one of the players has a winning strategy.

For a set $A \subseteq \mathbb{N}^{\mathbb{N}}$, imagine a game where two players I and II successively choose natural numbers:

$$\begin{array}{llllll} \text{I:} & x_0 & & x_1 & & x_3 \ \ ... \\ \text{II:} & & y_0 & & y_1 & & y_3 \ \ ... \end{array}$$

At the end of the game, player I wins if the resulting sequence $(x_0, y_0, x_1, y_1, x_2, y_2, ...)$ is in A, otherwise player II wins. We call this game G_A and we say that it is determined if one of the players has a winning strategy. A strategy is a rule for how to choose every element, depending of which elements have been chosen before by both players and a winning strategy is strategy which ensures that the player wins, regardless of how the other player plays.

The Axiom of Determinateness is the following statement:

6.2.1. The Axiom of Determinateness (AD): For every $A \in \mathbb{N}^{\mathbb{N}}$, G_A is determined.

AC and AD are inconsistent, this is proved in Theorem 7.15 in [Her2006]. Thus WOT, ZL and FTLA are all false under AD. However, AD and ADC are consistent. This is proven in [Kec1984].

The following theorem corresponds to Theorem 7.13 in [Her2006].

Theorem 6.2.2. *AD implies that every subset of* $\mathbb{R}$ *is Lebesgue-measurable.*

This is not case for AC, which is proved in Disaster 5.6 in [Her2006].

Another consequence of AD is:

Theorem 6.2.3. *AD implies the Continuum Hypothesis.*

This is proved in [Myc1964].

6.3 Discussion

In section 3 we looked at how AC can be expressed in different forms and at some weaker versions of it and how the full strength of AC is not always necessary. This together with the counter-intuitive consequences of AC motivates us the consider rejecting AC but accept one of the weaker versions of the axiom. However, we saw in section 4 how WOT, ZL and FTLA are equivalent to AC, and thus by rejecting AC we would have to accept the negation of those.

In section 5.1 the Boolean Prime Ideal theorem was proven to follow from AC, and we saw how it in turn has interesting and useful results in mathematics.

Maybe the most interesting result of the thesis is that the highly counter-intuitive Banach-Tarski Paradox follows from AC, which was proven in section 5.2. Even though, one could say, it loses some of its counter-intuitiveness by going through the proof, this alone gives us a reason to be hesitant about AC.

One alternative would be to, instead of AC, accept AD. Then we would get the desired result that every subset of $\mathbb{R}$ is Lebesgue-measurable. This is also not unproblematic, since if every subset of $\mathbb{R}$ is Lebesgue-measurable, then there is a partition of $\mathbb{R}$ into strictly more parts than elements (for a proof of this, see [Kom2006] and [Sie1947]).

So, from where comes this feeling that everywhere we turn, seemingly paradoxical results emerges? Is the axiom that we choose to use the culprit? Or might it be that we overestimate our capacity to have intuition about something as far away from our everyday lives as infinity? Or even worse; uncountable infinity? And if so, how could we decide whether or not to accept the axioms?

References

Articles

[Coh1963] P. J. Cohen, *The Independence of the Continuum Hypothesis*, Proceedings of the National Academy of Sciences of the United States of America 50 (6), 1963.

[Kec1984] A.S. Kechris, *The axiom of deteminancy implies dependent choices in L($\mathbb{R}$).* J. Symb. Logic, 49:161173, 1984.

[Myc1964] J. Mycielski, *On the axiom of determinateness*, Fund. Math., 53:205224, 1964.

[Sie1947] Sierpinski: *Sur une proposition qui entrane lexistence des ensembles non mesurables*, Fund. Math. 34, 1947.

Books

[BeBl2006] J. A. Beachy & W. D. Blair, *Abstract Algebra*, 3rd ed. 2006, ISBN: 1577664434, Waveland Press, Inc.

[Coh2013] D. L. Cohn, *Measure Theory*, 2nd ed. 2013, ISBN: 978-1-4614-6956-8 Springer New York Heidelberg Dordrecht London.

[Gon1997] S. S. Goncharov, *Countable Boolean Algebras and Decidability*, 1997, ISBN: 0-306-11061-X, Consultants Bureau New York.

[Her2006] H. Herrlich, *Axiom of Choice*, Electronic edition 2006, ISSN: 16179692, Springer-Verlag Berlin Heidelberg New York.

[Jec2006] T. Jech, *Set Theory*, The Third Millennium Edition revised and expanded, corrected 4th printing 2006, ISBN: 978-3-540-37097-0, SpringerVerlag Berlin Heidelberg New York.

[Jec1973] T. Jech, *The Axiom of Choice*, 1973, ISBN: 0486466248, North-Holland Publishing Company.

[Kom2006] P. Komjth & V. Totik, *Problems and Theorems in Classical Set Theory*,ISBN-10 3-540-44085-2, 2006, Springer Science+Business Media.

[Moo1982] G. H. Moore, *Zermelos Axiom of Choice : Its Origins, Development and Inuence*, 1982, ISBN: 0-540-90670-3, Springer-Verlag Berlin Heidelberg New York.

Internet

[I-FL] `https://www.math.uni-bielefeld.de/~mfluch/docs/2008-11.pdf`

[I-KA] `http://boolesrings.org/asafk/2014/anti-anti-banach-tarski-arguments/`

[I-PW1] `https://proofwiki.org/wiki/Vector_Space_has_Basis`