10. AXIOM OF CHOICE AND ZORN'S LEMMA

§10.1. The Axiom of Choice

We come now to the most important part of set theory for other branches of mathematics. Although infinite set theory is technically the foundation for all mathematics, in practice it is normal for a mathematician to ignore it – with two exceptions. Of course most of the basic set constructions as outlined in chapter 2 (unions, intersections, Cartesian products, functions etc.) are part of a mathematician's standard language. The second exception is the Axiom of Choice and Zorn's Lemma.

Zorn's Lemma, sounds like a small theorem that's preparatory to a bigger theorem. That's the usual meaning of the word 'lemma'. In fact it's not a theorem at all – it's an axiom. And the Axiom of Choice is also an axiom.

In fact these axioms are equivalent. That is, you can prove Zorn's Lemma if you assume the Axiom of Choice and you can prove the Axiom of Choice if you assume Zorn's Lemma. We'll show this a bit later.

But this axiom, for indeed they are essentially just a single axiom, is consistent with and independent from the ZF axioms. It has the same status as the Continuum Hypothesis, which is also an optional axiom.

In fact the Axiom of Choice (aka Zorn's Lemma) is consistent with, and independent from, the ZF axioms supplemented by the Continuum Hypothesis. This means that you can logically choose any one of the following four set theories:

ZF + CH + AXC
ZF + CH + notAXC
ZF + notCH + AXC
ZF + notCH + notAXC

Unlike the Continuum Hypothesis, which is only of interest to those studying infinite set theory, the Axiom of Choice, and its twin Zorn’s Lemma, impinge on mainstream mathematics.

Now the Axiom of Choice is not so called because one is logically free to choose to accept or reject it. It’s because it has to do with the possibility of choosing an element from each set in a set of non-empty sets. More accurately it’s concerned with making such choices from a *family* of non-empty sets. The difference is due to the fact that the same set may occur many times in the family.

Axiom of Choice: If $(A_i)_{i \in I}$ is a family of non-empty sets then there exists a function
$C: I \to \cup\{A_i \mid i \in I\}$ such that $C(i) \in A_i$ for each $i \in I$.

Making such a choice in the case of a finite family is easily proved. But what if we have a family of non-empty subsets of $\mathbb{R}$ indexed by the reals themselves? Are we entitled to choose an element from each one of these sets? Suppose we have an equivalence relation with uncountably many equivalence classes. Are we entitled to say “choose a representative from each of the equivalence classes”?

Intuitively it may seem obvious. But we’re supposed to be formalising our intuition so that even statements that are ‘intuitively obvious’ can be proved. And if we consider the Axiom of Choice to be ‘obvious’ we haven’t succeeded in capturing it by our ZF axioms. For the Axiom of Choice is consistent with, and independent from, the ZF axioms. If we want it to be true we must add it to our ZF axioms.

But before you accept it as something that “of course must be true” consider the consequences. We’ll prove, on the basis of the Axiom of Choice, that it’s theoretically possible to take a solid ball of radius 1 cm, in 3-dimensional space, decompose it into a small number of subsets, transform these pieces by rotations and translations, and reassemble them to form two solid balls of radius 1 cm.

Before you dismiss this as a contradiction which disproves the Axiom of Choice let me point out that you’d never be able to use this operation to double a solid ball of gold. The decomposition in the theorem is not the sort you could carry out with a lump of gold and an extremely sharp knife. Each of the subsets in the decomposition would be a sort of cloud, like the set of points in $\mathbb{R}^3$ with rational coordinates. They’re subsets that are so disconnected that their volumes can’t be defined. So we can’t conclude that the doubling of the volume gives a contradiction.

Nevertheless this consequence of the Axiom of Choice is so counter-intuitive that many mathematicians prefer to reject the axiom. You’re perfectly free to do so. But whether you accept it or reject it, it’s a “matter of faith”. Like a belief in God you can neither prove nor disprove it by pure logic. But you may have good reasons to accept or reject God that lie outside pure logic. In the same way there may be good meta-logical reasons for either accepting or rejecting the Axiom of Choice.

This is not the place for me to try to impose my religious beliefs upon you, but I feel perfectly justified in trying to persuade you to accept the Axiom of Choice. In terms of practical applications it makes no difference whether you accept it or reject it. No bridge is going to fall down because the engineer accepted or didn’t accept the Axiom of Choice. No specific example within mathematics will owe its existence to the Axiom of Choice. If that were the case the axiom wouldn’t be independent of the ZF axioms. The difference between the two positions of ‘faith’ lies simply in the way we express some of our theorems.

Assuming the axiom of choice gives simpler and cleaner theorems in some cases. If one denied the Axiom of Choice, or were simply agnostic, the statement of some theorems would be unnecessarily complicated.

Perhaps the simplest example where the Axiom of Choice leads to a better theorem is the one about the existence of a basis in a vector space. You'll have seen a proof that every finite-dimensional vector space has a basis.

If you assume the Axiom of Choice you'll be able to prove that *every* vector space has a basis. If you don't you'd have to rephrase the statement to include additional wording that in effect amounts to assuming the axiom of choice in this particular context.

Either way the two statements of the theorem would have the same consequences when it came to any specific example, because in a specific example we'd be able to make the required choices explicitly.

So it comes down to a matter of convenience. Where it's relevant, assuming the Axiom of Choice gives a simpler theorem that's equivalent, for all practical purposes, to the one you'd have if you didn't accept it.

So what if you have to accept its bizarre consequences such as doubling the sphere? In a way it's exciting to be able to contemplate such curiosities even though they lie outside what's achievable in a material world.

Having discussed the Axiom of Choice at length let's now turn our attention to Zorn's Lemma. That is, as we shall see, essentially a restatement of the Axiom of Choice. It's often the version of that axiom that we actually use. Zorn's Lemma is a statement about the way a set can be ordered, so let us turn our attention to orderings on a set.

§10.2. Partial Ordering

Real numbers are ordered by the relation $\leq$. The subsets of $\mathbb{R}$ are ordered by the relation $\subseteq$. Both are examples of a partial order. In what follows, unless otherwise stated, the symbol $\leq$ will be used for an arbitrary order relation. But what is a partial order?

- A relation $\leq$ is **reflexive** if $x \leq x$ for all x.
- It's **transitive** if $x \leq y$ and $y \leq z$ implies $x \leq z$.
- It's **antisymmetric** if $x \leq y$ and $y \leq x$ implies that $x = y$.
- A relation is a **partial order** if it has all three properties.
- A **partially ordered set** (**POS**) is a set X, together with a partial order. We denote it by **(X, ≤)**.

Let X be a partially ordered set. We make the following definitions. Note that they don't always exist.

- An element $m \in X$ is the **least** element of X if $m \leq x$ for all $x \in X$. If it exists it's denoted by **min X**.
- The **greatest** element is defined similarly and is denoted by **max X**.
- An element $m \in X$ is a **minimal** element of X if for all x, $x \leq m$ implies that $x = m$
  (in other words there is nothing smaller than m).
- A **maximal** element is defined similarly.
- The element $b \in X$ is a **lower bound** for $Y \subseteq X$ if $b \leq y$ for all $y \in Y$.
- An **upper bound** is defined similarly.

- The **least upper bound** of Y $\subseteq$ X is the smallest upper bound. denoted by **lub(Y)**.
- The **greatest lower bound** of Y $\subseteq$ X is the smallest upper bound, denoted by **glb(Y)**.

Examples 1:

(1) ($\mathbb{R}$, $\leq$) is a POS. The closed interval [0, 1] has both a least and a greatest. The half-open interval [0, 1) has a least but not a greatest.

(2) $\{x \in \mathbb{R} \mid 2 < x^2 \leq 4\}$ has a greatest but no least.

(3) $\{x \in \mathbb{Q} \mid 2 \leq x^2 < 3\}$ has a no least or greatest.

(4) ($\wp\mathbb{R}$, $\subseteq$) is a POS: min $\wp\mathbb{R} = \varnothing$ and max $\wp\mathbb{R} = \mathbb{R}$.

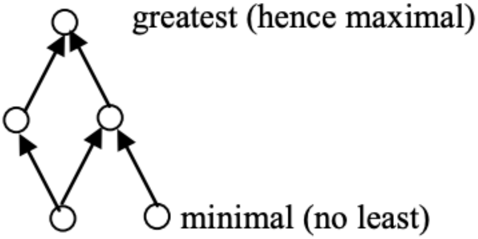
(5) $\{S \in \wp\mathbb{R} \mid S \neq \varnothing\}$ has minimal elements but min S doesn't exist. Max S = $\mathbb{R}$.

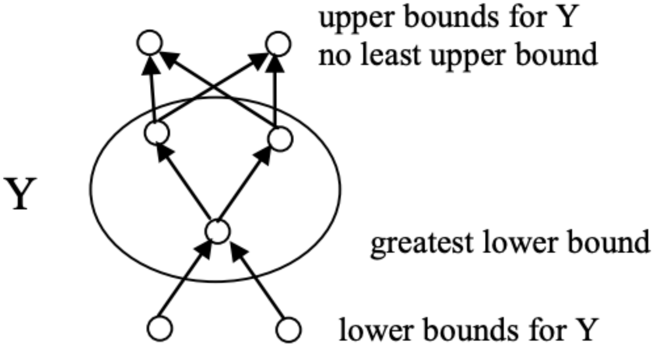
(6) If X = {{1}, {0, 1}, {1, 2}, {0, 1, 2}, {1, 2, 3}} then (X, $\subseteq$) is a POS. {1} is the least. There's no greatest but {0, 1, 2} and {1, 2, 3} are maximal elements.

(7) In $\mathbb{R}$, lub $\{x \in \mathbb{Q} \mid x^2 < 3\}$ is $\sqrt{3}$. There is no lower bound (remember negative *x*'s)

The least and greatest elements of a set X, where they exist, are clearly unique. Minimal and maximal elements need not be unique. Likewise lower and upper bounds are not unique, but least upper bounds and greatest lower bounds, where they exist, must be unique.

Examples 2:





In a POS two elements x, y are **comparable** if either $x \leq y$ or $y \geq x$.

A **chain** is a POS in which every two elements are comparable.

Suppose X is a partially ordered set.

- The element $x \in$ X is a **predecessor** of y if $x < y$.
- A **successor** is defined similarly.
- An **immediate predecessor** is a greatest predecessor, denoted by $\boldsymbol{x}^{-}$.
- An **immediate successor**, denoted by $\mathbf{x}^{+}$ is defined similarly. This is a different meaning to $x \cup \{x\}$, though

if $\leq$ represents 'subset' it can also be 'immediate successor'. (An exception would be if we reject the Axiom of Foundation, and allow $x \in x$ in our set theory – see Chapter 12)

Examples 3:

(1) $(\mathbb{R}, \leq)$ is a chain.

The set, S, of proper subsets of {0, 1, 2, 3} is not a chain under the subset relation because neither {0, 1} nor {1, 2} is a subset of the other. The empty set is min S. There's no greatest element but any subset of size 3 is maximal.

(2) Consider the POS X = ($\wp$3, $\subseteq$). Remember that we have defined 3 to be {0, 1, 2}. The elements of X are:

$\varnothing$, {0}, {1}, {2}, {0, 1}, {0, 2}, {1, 2}, {0, 1, 2}.

Let Y = {$\varnothing$, {1}, {2}}. Then {1, 2} and {0, 1, 2} are upper bounds for Y, but {1, 2} is the least upper bound.

(3) If S is any set and X = ($\wp$(S), $\subseteq$) and Y $\subseteq$ X then $\cup$Y is the least upper bound.

(4) In $(\mathbb{Q}, \leq)$, the set $Y = \{x \mid x^2 < 2\}$ has no largest element, plenty of upper bounds but no least upper bound. But in $(\mathbb{R}, \leq)$, though it still has no largest element, it has a least upper bound, namely $\sqrt{2}$.

In any partially ordered set we define ***x* < *y*, *x* ≥ *y*** and ***x* > *y*** in the same way that we do in ordinary arithmetic.

Example 6: If $a \in \mathbb{R}$ then $\{x \mid x \leq a\}$ is an initial segment. So is $\{x \mid x < a\}$ and also $\mathbb{R}$ itself.

Example 7: Let Y = {1, 2, 3} and let X = $\wp$(Y).
If a = {2, 3} then X_a = {{2}, {3}, ∅}.
The subset S = {{1, 2}, {1, 3}, {1}, {2}, {3}, ∅} is an initial segment, but isn't X_a for any a ∈ X.

Suppose X and X are partially ordered sets. They may well have quite different partial orders, but we'll use the same notation, ≤, for each. A function f:X→Y is **order-preserving** if $x_1 \leq x_2$ implies that $f(x_1) \leq f(x_2)$. A **similarity** is an order-preserving bijection.

Examples 8:
(1) f:ℕ→ℕ, defined by f(x) = 2x, is order-preserving but it is not a similarity.

(2) f:ℝ→ℝ, defined by f(x) = x^3 is a similarity.

(3) f:ℝ→$\wp$ℝ, defined by f(a) = $\{x \mid x < a\}$ is order-preserving but is not a similarity.

A subset S ⊆ X is an **initial segment** of X if, whenever an element belongs to S, so do all its predecessors. An obvious example of an initial segment is $\mathbf{X}_{\boldsymbol{a}} = \{x \in X \mid x < a\}$.

§10.3. Well Ordering

A partially ordered set is **well-ordered** if every non-empty subset has a least. We'll call a well-ordered set a WOS.

Since, in a WOS, $\{x, y\}$ has a least for all x, y, every WOS is a chain. The converse isn't true since the set of real numbers is a chain but it is not well-ordered. However it's obvious that finite chains *are* well-ordered.

Six million and four... Oh fudge! How can I count them if they refuse to be well-ordered!

Subsets of well-ordered sets are clearly well-ordered. Any POS that's similar to a WOS is itself a WOS. In a WOS every element, x, except the greatest element if there is one, has a unique successor, namely $\min\{y \mid y > x\}$.

Theorem 1: If X is a WOS, $Y \subseteq X$ and $f{:}X \to Y$ is a similarity then $x \le f(x)$ for all x.

Proof: If $a = \min\{x \mid f(x) < x\}$, then $f(f(a)) < f(a)$, a contradiction. ✋☺

Theorem 2: If X, Y are similar well-ordered sets there is a unique similarity $F{:}X \to Y$.

Proof: If F, G are similarities then $FG^{-1}{:}X \to X$ is a similarity. Thus for all x we have:

$$x \le FG^{-1}(x),$$

and so $G(x) \leq F(x)$.

Similarly $F(x) \leq G(x)$ and so $F(x) = G(x)$ for all x. ✋☺

Theorem 3: If A, B are well-ordered sets and A is an initial segment of B then A = B or

$$A = B_a \text{ for some } a \in B.$$

Proof: Suppose $A \subset B$. Let $a = \min(B - A)$.

If $x < b$ then $x \in A$ so $B_a \subseteq A$.

If $x \in A$ and $x \geq a$ then $a \in A$, a contradiction.

So $x < a$ and hence $A \subseteq B_b$.

Theorem 4: If Y is an initial segment of the well-ordered set X and Y is similar to X then Y = X.

Proof: Suppose $Y \subset X$. Then by Theorem 3, $Y = X_a$ for some $a \in X$. Suppose $F:X \rightarrow Y$ is a similarity.

Then $F(a) < a$, contradicting Theorem 1. ✋☺

Corollary: Similar initial segments of a well-ordered set X are equal.

§10.4. Zorn's Lemma

Many proofs involve a partially ordered set, usually a set of subsets X of some set S that is partially ordered by inclusion (that is using the relation $\subseteq$) and we would like to be able to conclude that there is a maximal element of X.

For example we can define linear independence for subsets of any vector space, not just finite-dimensional ones. If we can find a maximal linearly independent subset then it must be a basis, because if it doesn't span the space we can find one extra element that can be added to our linearly independent subset to get an even bigger one, contradicting the fact that it was already maximal.

Zorn's Lemma: If (S, ≤) is a non-empty partially ordered set in which every chain has an upper bound then S has a maximal element.

Proof: Of course we can't prove it, at least not from the ZF axioms alone. But here's a pseudo proof that can help us to understand the nature of the lemma.

Take an element $s_0 \in$ S. If it's maximal, then we've finished.

Suppose s_0 is not maximal. Then there exists $s_1 \in$ S such that $s_0 < s_1$.

If s_1 is maximal, we've finished. Suppose s_1 is not maximal. Then there exists $s_2 \in$ S such that $s_0 < s_1 < s_2$.

Proceeding in this way (by induction) we conclude that there's a chain $s_0 < s_1 < s_2 < s_3 < \ldots\ldots\ldots$

By our assumption this chain has an upper bound. That is, there's some $t_0 \in$ S such that $s_n < t_0$ for all n. By the above argument, if t_0 is not maximal we can find $t_1 \in$ S with
$t_0 < t_1$.

If we assume that there is no maximal element we would thus have $s_0 < s_1 < s_2 < \ldots < t_0 < t_1 < t_2 < \ldots$

Again we have a chain, which must therefore have an upper bound. "Surely this process must eventually terminate with a maximal element." This last statement is the weak point in the 'proof '.

So now we turn our attention to proving the equivalence of the Axiom of Choice and Zorn's Lemma. In the process we include a number of other equivalent statements and the proof consists of a round robin where each statement is shown to imply the next, with the last implying the first. This material is based on notes prepared by Ross Street, in turn based on material by Max Kelly.

§10.5. The Left Inverse Principle

The **Left Inverse Principle** states that if a function $F:A\rightarrow B$ is onto then it has a **left inverse** $G:B\rightarrow A$ (meaning that $GF = 1_B$, the identity function from B to B). I'll show that the Left Inverse Principle implies Zorn's Lemma. In what follows let $(X, \leq)$ be a POS, $Ch(X) = \{\text{chains in } X\}$ and let $\sigma:Ch(X)\rightarrow X$ be some fixed function.

$A \in Ch(X)$ is called **special** if A is well-ordered by $\leq$ and $\sigma(A_a) = a$ for all $a \in A$.
Define **Sp(X)** = {special chains in X}.

Lemma 1: If $A, B \in Sp(X)$ with $B \subseteq A$ then B is an initial segment of A.
Proof: Suppose $B \subset A$.
Let $a = \min(A - B)$. Then $A_a \subseteq B$.
Suppose $A_a \subset B$ and let $b = \min(B - A_a)$.
Since $b \notin A_a$, $b \geq a$.
Clearly $B_b \subseteq A_a$. Let $x \in A_a$. Then $x < a \leq b$ so $x \in B_b$.

Since A, B are special $a = \sigma(A_a) = \sigma(B_b) = b$, a contradiction. Hence $A_a = B$. ✋☺

Lemma 2: Sp(X) is totally ordered by $\subseteq$.
Proof: Suppose A is not a subset of B and
let $a = \min(A - B)$. Clearly $A_a \subseteq B$.
Since A_a is a special chain, it’s an initial segment of B.
If $A_a = B_b$ for some $b \in B$, $a = \sigma(A_a) = \sigma(B_b) = b$, a contradiction. Hence $B = A_a \subseteq A$. ✋☺

Lemma 3: $\cup$Sp(X) $\in$ Sp(X).
Proof: Let M = $\cup$Sp(X). It’s well-ordered by $\leq$.
If $a \in M$ then $a \in A \in$ Sp(X) for some A, so $M_a = A_a$ and $\sigma(M_a) = \sigma(A_a) = a$. ✋☺

Lemma 4: There’s no σ:Ch(X)$\rightarrow$X such that $\sigma(A) > a$ whenever $a \in A \in$ Ch(X).
Proof: Suppose such a σ exists and define ‘special’ accordingly.
Let M = $\cup$Sp(X).
Then since $\sigma(M)$ is greater than every element of M,

$$A = M \cup \{\sigma(M)\} \text{ is a chain.}$$

Since $A_{\sigma(M)} = M$, $\sigma(A_{\sigma(M)}) = \sigma(M)$ so $A \in$ Sp(X).
Thus $A \subseteq M$ whence $\sigma(M) \in M$, a contradiction. ✋☺

Theorem 5: The Left Inverse Principle implies Zorn's Lemma.

Proof: Suppose X is a partially ordered set where every chain has an upper bound. Suppose X has no maximal element.

Let $Y = \{(A, x) \mid x \in X, A \in Ch(X) \text{ and } a < x$
for all $a \in A\}$.

Define $H:Y \rightarrow Ch(X)$ by $H(A, x) = A$ and $P:Y \rightarrow X$ by:
$P(A, x) = x$.

We now show that H is onto.

Let $A \in Ch(X)$. If $m = \max(A)$ exists there exists $M > m$.
If A has no maximum let M be an upper bound for A.
In either case $(A, M) \in Y$ and $H(A, M) = A$.
Let $K:Ch(X) \rightarrow Y$ be a left inverse for H.
Then $H(K(A)) = A$ for all $A \in Ch(X)$.
Then $\sigma = KP:Ch(X) \rightarrow X$ has the property that $\sigma(A) > a$ for all $a \in A$, a contradiction. ✋☺

§10.6. Hausdorff's Maximal Principle

The **Hausdorff Maximal Principle** states that every partially ordered set has a maximal chain.

Theorem 6: Zorn's Lemma implies the Hausdorff Maximal Principle.

Proof: Let X be a partially ordered set and let
$C = Ch(X)$, ordered by $\subseteq$.
Let $D \in Ch(C)$ and $E = \cup D$.

Then $E \in \mathrm{Ch}(X)$.
E is an upper bound for D so, by Zorn’s Lemma, C has a maximal element. ✋☺

§10.7. The Well-Ordering Principle

The **Well-ordering Principle** states that every set can be well-ordered.

Theorem 7: The Hausdorff Maximal Principle implies the Well-ordering Principle.

Proof: Let X be a set and let $W = \{(A, \leq) \mid A \subseteq X$ and $\leq$ is a well-ordering for $A\}$.
Define $\leq$ on W: $(A, \leq) \leq (A', \leq')$ if A is an initial segment of A' with $\leq$ compatible with $\leq'$.
Since $(W, \leq)$ is a partially ordered set it has, by the Hausdorff Maximal Principle, a maximal chain C.
Let $Y = \cup C$. Now $(Y, \leq)$ is a partially ordered set.
Let Z be a non-empty element of Y.
Then there exists $z \in A \in C$.
Let $m = \min Z \cap A_z = \min Z \cap Y_z = \min Z$.
Thus $(Y, \leq)$ is a well-ordered set.
Since $C \cup \{Y\} \in \mathrm{Ch}(W)$, $Y \in C$.
Suppose $Y \subset X$ and let $x \in X - Y$.
Let $Y' = Y \cup \{x\}$ with $\leq$ extended to make $x = \max Y$.
Then $C \cup \{Y'\} \in \mathrm{Ch}(W)$, and so $Y' \in C$,
a contradiction. ✋☺

§10.8 Well-Ordering and The Axiom of Choice

Theorem 8: The Well-ordering Principle implies the Axiom of Choice.

Proof: If (A, φ) is a family of sets we well-order $\cup\{\varphi(a) \mid a \in A\}$ and let $F(a) = \min \varphi(a)$ for each $a \in A$. Then $F \in \Pi(A, \varphi)$. ✋☺

Theorem 9: The Axiom of Choice implies the Left Inverse Principle.

Proof: Suppose $F{:}A \to X$ is onto.
Then for $x \in X$, $\{a \mid F(a) = x\} \neq \varnothing$.
By AXC $\Pi(A, F) \neq \varnothing$. If $G \in \Pi(A, F)$ then $FG = 1_A$. ✋☺

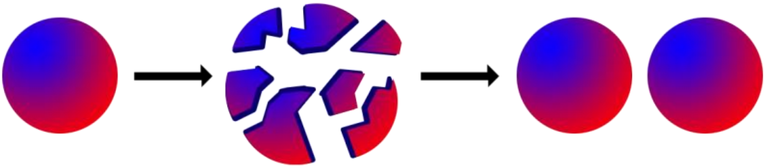
Theorem 10: Every vector space V over a field F has a basis.

Proof: Let S be the set of all linearly independent subsets. Since $0 \in S$, $S \neq 0$. S is partially ordered by $\subseteq$. The union of every chain of linearly independent subsets is linearly independent so by Zorn's lemma there is a maximal linearly independent subset B. If B doesn't span V then let $v \in V - \langle B\rangle$ and so $B \cup \{v\} \in S$, a contradiction. ✋☺

§10.9. The Banach-Tarski Paradox

This material in the rest of this chapter is based on Stromberg: *The Banach-Tarski Paradox*, American Mathematical Monthly, March 1979.

The Axiom of Choice is intuitively reasonable. Given any family of non-empty sets it is possible to choose one element from each set. However it has been proven that this axiom can’t be proved from the ZF axioms. The natural thing to do is to add this axiom to the ZF collection. However I am about to show you that, assuming the axiom of choice, I can prove that a solid sphere can be decomposed into a finite number of pieces and reassembled into two spheres each with the same radius of the original sphere! The theorem is the Banach-Tarski Paradox.

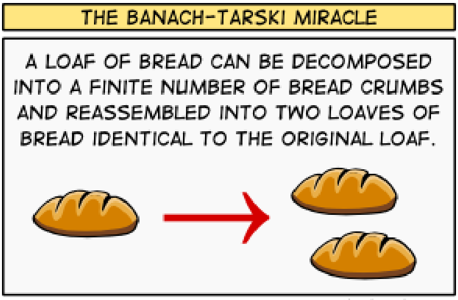


This result is so counter-intuitive that many mathematicians regard it as a good reason to reject the Axiom of Choice. However we don’t actually get a contradiction. But wouldn’t it mean doubling the volume? Not really. You see the volume of a set of points in $\mathbb{R}^3$ can’t be defined for all subsets. For example, what is the volume of the set of points whose *x*- and *y*- coordinates are rational?

I CARVED AND CARVED, AND THE NEXT THING I KNEW I HAD TWO PUMPKINS.
I TOLD YOU NOT TO TAKE THE AXIOM OF CHOICE.

The pieces into which we ‘cut’ the sphere are so highly disconnected that they don’t have volumes. It is as if they are just clouds of points. So any thought of going into production converting spheres of solid gold into twice as many identical spheres must be ruled out. Remember that a real sphere of gold is not a mathematical sphere. It consists of lots of empty space and, more importantly, a finite number of atoms.

You can get a feeling for the process involved if you consider taking the positive *x*-axis and cutting off the interval (0, 1]. What's left can be translated one unit to the left to exactly cover the positive *x*-axis. We have effectively created a unit interval from nothing.


THE BANACH-TARSKI MIRACLE
A LOAF OF BREAD CAN BE DECOMPOSED INTO A FINITE NUMBER OF BREAD CRUMBS AND REASSEMBLED INTO TWO LOAVES OF BREAD IDENTICAL TO THE ORIGINAL LOAF.

spikedmath.com
© 2010

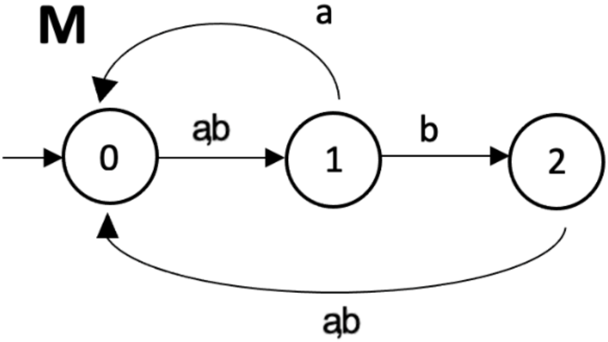
The Banach-Tarski Paradox has been pounced on by many people as supporting certain beliefs. The biblical miracle of the five loaves and three fish feeding a crowd of thousands has been said to be a practical application of the Banach-Tarski Paradox. It has been said to be the mechanism for the big-bang process in the way the universe came about.

Of course nothing in mathematics, by itself, proves or disproves anything in the real world. It may be that the universe was created out of nothing in a big bang, either by a creator God or by laws of physics. It may be true that the loaves and fishes in the miracle were multiplied. But other factors would be at work, not the Axiom of Choice.

In fact the Axiom of Choice has been proved to be both consistent with, and independent of, the other axioms of set theory.

To Prove the Banach-Tarski Theorem, for it really is a theorem, we need to use some Group Theory. (See my notes *Group Theory volume 1*.) Consider the group $G = \langle a, b \mid a^2 = b^3 = 1\rangle$. G is the set of words on $\{a, b\}$ with no substring "*aa*" or "*bbb*" where two such 'reduced' words are multiplied by concatenating and reducing, eliminating or inserting any substring '*aa*' or '*bbb*'.

Consider the following finite-state machine. (See my notes *Languages and Machines*.)



I'll use this to classify the elements of G into three sets, according to the final state of the machine, when it starts in state 0 and reads the given string.

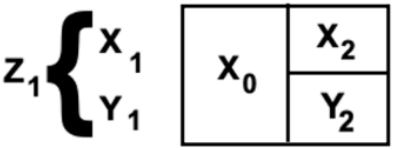
For $i = 0, 1, 2$ let Z_i be the set of elements of G which cause this finite-state machine to end in state i. Denoting disjoint unions by ‘+’ we can write:

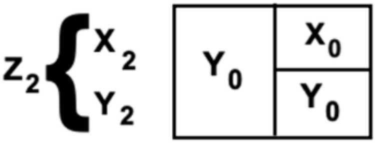
$$G = Z_0 + Z_1 + Z_2.$$

Now $Z_0 = Z_1a + Z_2a + Z_2b + \{1\}$
$Z_1 = Z_0a + Z_0b$ and
$Z_2 = Z_1b$.
Let $X_0 = Z_0abb + Z_1a + \{1\}$,
$X_1 = Z_0a + Z_1ab + \{b\}$,
$X_2 = Z_0ab + Z_1abb + \{bb\}$ and
$Y_0 = Z_2a$,
$Y_1 = Z_2ab$,
$Y_2 = Z_2abb$.
So $X_0 = \{1, abb, ba, bbaba, \ldots\}$
$X_1 = \{a, b, bab, abba, \ldots\}$
$X_2 = \{ab, bb, babb, \ldots\}$
$Y_0 = \{bba, aba, \ldots\}$
$Y_1 = \{bbab, \ldots\}$ and
$Y_2 = \{bbabb, \ldots\}$.
Then $Z_0 = X_0 + Y_0$,
$Z_1 = X_1 + Y_1$ and
$Z_2 = X_2 + Y_2$.

The effect of a, b on these subsets is as follows
(eg $X_0a = Z_1$):

		a	***b***
Z_0	X_0	Z_1	X_1
	Y_0	Z_2	Y_1





§10.10. Groups of Rotations in $\mathbb{R}^3$

Take two axes through the origin having an angle θ between them. Let A be the 180° rotation about axis 1 and let B be a 120° rotation about axis 2. Let H be the group generated by A, B. Define a group homomorphism σ: $G \to H$ by $\sigma(w)$ = the rotation obtained by substituting A for *a* and B for *b*.

So $\sigma(w_1 w_2) = \sigma(w_1)\sigma(w_2)$ and $\sigma(w^{-1}) = \sigma(w)^{-1}$.

For certain values of θ, σ will not be 1-1, and in fact it is possible for H to be finite. For example if $\theta = 0$ then $ab = ba$ and H consists of rotations through multiples of 60°. And if $\theta = 90°$ then H is the rotation group of a triangular prism, with order 6.

If $\theta = \tan^{-1} \sqrt{2}$, H is the rotation group of a cube and $|H| = 24$. However if $\cos \theta$ is transcendental (this is the case for all but a countable number of values, and in particular it can be shown that this is so for $\theta = 1$) σ is

1-1. In such cases every rotation in H can be uniquely represented by a reduced word in G. We suppose that θ is such a value.

Let S be the surface of a unit sphere and for all $P \in S$ let $G(P) = \{\sigma(g)(P) \mid g \in G\}$ denote the G-orbit of P.
Then S splits into uncountably many orbits.

By the **Axiom of Choice** we may choose a set C of representatives from these orbits, and so for every $P \in S$, $P = \sigma(g)(Q)$ for some unique $Q \in C$. Is g also unique?

A **pole** of a rotation R is a point on the unit sphere which is fixed by R. Every non-trivial rotation has exactly 2 poles. For a rotation group H, a **pole** is a point on the unit sphere which is the pole of some $1 \neq h \in H$. Every other point on the unit sphere is a **non-pole**.

If $P = \sigma(g)(Q) = \sigma(h)(Q)$ for $g \neq h$ then Q is a pole of the rotation $\sigma(g)\sigma(h)^{-1} = \sigma(gh^{-1})$, and this is non-trivial since σ is 1-1. Let $\pi(G)$ be the set of poles for the rotation group G.

Each non-pole is $\sigma(g)(Q)$ for some unique $Q \in C$ and some unique $g \in G$. The non-poles can thus be partitioned into subsets according to the partition of G and so the surface S is thus decomposed into 7 subsets:

$$\pi(G), X_0, X_1, X_2, Y_0, Y_1, Y_2.$$

By the rotation *a*:	By the rotation *bbab*:	By the rotation *babb*:
$X_0 \rightarrow X_1 + Y_1$	$X_1 \rightarrow X_2 + Y_2$	$X_2 \rightarrow X_0 + Y_0$
$Y_0 \rightarrow X_2 + Y_2$	$Y_1 \rightarrow X_0 + Y_0$	$Y_2 \rightarrow X_1 + Y_1$

These seven pieces can therefore be rotated by suitable rotations and reassembled to give one complete copy of S plus a second copy, excluding the poles. We have to work a little harder to get another copy of π(G).

§10.11. The Finale

Theorem 11 (BANACH-TARSKI): The surface of a unit sphere can be decomposed into finitely many pieces and be reassembled into two unit spheres (using only rigid motions).

Proof: Let c be a rotation through ϕ about a third axis and choose ϕ so that π, $c(\pi)$, $c^2(\pi)$, … are disjoint (this is possible because there are countably many angles between the elements of $\pi(G)$ and uncountably many possible values of ϕ).

Let U = $c(\pi) + c^2(\pi) + \ldots$

V = S – π – U.

Thus S = π(G) + U + V. Note that c^{-1}(U) = π(G) + U.

Cut S into these 3 pieces. Rotate U by c^{-1} to give π(G) + U. We now have the original sphere plus a second copy of π(G).

We now cut this new sphere into the 7 pieces as above and, with the second copy of $\pi(G)$, assemble them into two complete unit spheres.

#	**piece**	**rotated by**	**gives**
1	$\pi(G)$	1	(1)
2	$U \cap X_0$	$c^{-1}a$	(1) + [(3) + (6)] + [(4) + (7)] + [(2) + (5)] + [(4) + (7)] + [(2) + (5)] + [(3) + (6)]
3	$U \cap X_1$	$c^{-1}babb$	
4	$U \cap X_2$	$c^{-1}bbab$	
5	$U \cap Y_0$	$c^{-1}a$	
6	$U \cap Y_1$	$c^{-1}babb$	
7	$U \cap Y_2$	$c^{-1}bbab$	
8	$V \cap X_0$	$c^{-1}a$	(10) + (13)
9	$V \cap X_1$	$c^{-1}babb$	(8) + (11)
10	$V \cap X_2$	$c^{-1}bbab$	(9) + (12)
11	$V \cap Y_0$	$c^{-1}a$	(10) + (13)
12	$V \cap Y_1$	$c^{-1}babb$	(8) + (11)
13	$V \cap Y_2$	$c^{-1}bbab$	(9) + (12)
TOTAL	**S**		**S + S**

In fact (R.M. Robinson 1947) it can be done with just five pieces. A solid sphere can likewise be decomposed into finitely many pieces and reassembled to form two spheres of the same size. Simply replace each point on the surface S by the corresponding ray and include the origin with the poles.