IMPLICATIONS OF THE AXIOM OF CHOICE

Introduction

In this treatise we shall explore the axiom of choice and some of the implications this axiom has on mathematics. More specifically we will state the Hausdorff paradox and in turn use this to take a look at the Banach-Tarski paradox. We will also discuss the axiom of choice from a more foundational point of view. We start off with a simple question; What is the axiom of choice? We give a formal definition:

Definition (Axiom of Choice). *For every indexed family $(S_i)_{i \in I}$ of nonempty sets there exists an indexed family of elements $(x_i)_{i \in I}$ such that $x_i \in S_i$ for every $i \in I$.*

To clarify this definition it might be helpful to look at a quote from Bertrand Russell:

> The Axiom of Choice is necessary to select a set from an infinite number of socks, but not an infinite number of shoes.

The main point to take home is that left socks are equal to right socks, but that is not the case for shoes. That is, for shoes one could just choose the right shoe every time, but for socks no such "choice function" exists. Therefore we need the axiom of choice in this instance. We shall see that the axiom of choice is equivalent, necessary and sufficient for several results in mathematics. As a primer we state (without proof) that the axiom of choice is equivalent to statement that every surjective function has a right inverse. We willl now investigate this axiom a bit closer throughout the next section.

The axiom of choice

To start off this section we need to discuss our foundation for how we do mathematics. In mathematics it is required that a proof is present whenever we assert a proposition. Sometimes the propositions may be more or less complex, for instance we might have a disjunction $P \vee Q$ of two valid statements P and Q. How should we interpret the truth value of this? A very natural way is to decide if either of P or Q (or both) holds; That is, we can decide which of the statements that is true. But as it turns out this might be problematic, for what happens when $Q = \neg P$? Then we have to provide a proof that either P is true or $\neg P$ is true. There are however many examples where no such proof exist! The Riemann hypothesis is an example of this fact.

This very brief discussion would then seem to indicate that the law of the excluded middle: "Either P or $\neg P$ is true" is not a precise dichotomy and we should add the possibility that the truth value is unknown and discard it as a general law. This essentially gives rise to what is known as "intuitionistic logic". Furthermore we illustrate by a classic example that the law of the excluded middle displays a non-constructive nature:

Example. *There exists irrational numbers a, b such that a^b is rational. By the excluded middle either $\sqrt{2}^{\sqrt{2}}$ is rational in which case $a = b = \sqrt{2}$ or $\sqrt{2}^{\sqrt{2}}$ is irrational in which case we set $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.*

In this example we have no idea whether $\sqrt{2}^{\sqrt{2}}$ actually is rational or not, but we have nonetheless provided a proof for the statement. This is clearly non-constructive.

We now look back at the axiom of choice and note that it also has a similar non-constructive nature.

It actually turns out that the axiom of choice is sufficient to derive the law of the excluded middle in intuitionistic logic! This is known as Diaconescu's theorem:

Theorem (Diaconescu's theorem)**.** *The axiom of choice implies the law of the excluded middle under the assumption of extensionality.*

With this theorem it must be the case that if we are working in the context of intuitionistic logic we cannot accept the axiom of choice as we have already decided that we do not want the law of the excluded middle.

Within this discussion we would also like to give some examples of uses of the axiom of choice in classical mathematics. We start off in set theory with Zorn's lemma. This result states that if every chain in a partially ordered set P has an upper bound in P, then P contains at least one maximal element. We state without proof that Zorn's lemma is actually equivalent to the axiom of choice. This implies in turn that the axiom of choice is used in several other areas of mathematics. The extremely useful Hahn-Banach theorem in functional analysis follows from Zorn's lemma, and is therefore implied from the axiom of choice. In algebra it is needed to prove that every vector space has a basis. And finally it is used in topology to prove that the product of an arbitrary collection of compact spaces is compact (This is known as Tychonoff's theorem). We will now proceed towards the celebrated Banach-Tarski paradox as an application of what the axiom of choice can be used to.

The Hausdorff- and Banach-Tarski paradox

The Banach-Tarski paradox is often popularized along the way of "you can take cut up an orange and assemble the pieces to make two identical oranges as the first one". This obviously sounds absurd and this might be how it got its name. It is actually much more like a theorem, and it can be proved. Due to highly unintuitive statement it has been some controversy since the proof relies on the axiom of choice. An equivalent statement would be this:
Take the set of natural numbers and split it up into even and odd numbers. Then the cardinality of all these sets are the same. This just goes to show how limited our imagination is when the concept of infinity is discussed.
For the rest of this discussion we will consider the vector space $\mathbb{R}^3$. With this particular topic we are interested in transformations that preserve length (isometries; e.g. translations, rotations, etc.) as these will play a huge role in the proof. Since these transformations preserve length they are always injective, and they form a group G called the Euclidean group denoted by $E(3)$. Now given a subset $X \subset \mathbb{R}^3$ we get a group that "acts" on this subset. In general the action is a map (permutation) $* : G \times X \to X$ and we say that X is a G**-set** if the action is associative and the identity e of G maps $x \mapsto x$. Note that we use the short hand notation gx for $g * x$.
If $X \subset \mathbb{R}^3$ it is trivial to see that X is an $E(3)$-set. We define the **orbit of** $x \in X$ **under** G as $Gx = \{y \in X : y = gx, \text{ for some } g \in G\}$ and define the equivalence relation $x \sim y \Leftrightarrow \exists g \in G : gx = y$. In words the orbits of X under G are the equivalence classes under this relation. If $gx = x$ for all $x \in X$ implies that $g = e$ the group action is said to **act freely** on X. This is just the same as saying that the only map with fixed points is the identity map, and by the previous remarks we see that then this action partitions X into its orbits. We now wish to focus on the idea of decomposition. Roughly that means that we can take a set and cut it into a finite number of pieces. The formal definition follows:

Definition. *A set $S \subset \mathbb{R}^3$ is said to be **decomposable in** m **subsets** $D_1, \cdots, D_m$ if:*

$$1)\ S = \bigcup_{i=1}^{m} D_i$$

$$2)\ D_i \cap D_j = \emptyset\ \forall i, j$$

*The union in 1) is called a **decomposition of** S.*

With this definition it is fairly natural to create an equivalence class of sets being decomposable. To do that in our case we first need a sensible notion of equality for subsets of $\mathbb{R}^3$. In this case we set $G = E(3)$. Then this mentioned notion of equality is called congruence and defined as follows: Two subsets A and B of $\mathbb{R}^3$ are **congruent** if there exists a $g \in G$ such that $g(A) = B$. Note that this is just the same as saying that A and B are in the same orbit under G. We extend the concept of decomposition one step further:

Definition. *Two sets decomposable in m subsets $A, B \subset \mathbb{R}^3$ with*

$$A = \bigcup_{i=1}^{m} A_i,\ \ B = \bigcup_{i=1}^{m} B_i$$

*such that all A_i and all B_i are pairwise disjoint are said to be G**-equidecomposable in** m **pieces** if there are $g_1, \cdots g_m$ such that $g_i(A_i) = B_i$. If this is the case we write $A \sim_G B$*

This is just saying that the decomposed pieces of A and B are all congruent. G-equidecomposition relies on congruence and therefore defines yet another equivalence class; Hence the notation.
Now it may happen that there are several ways to decompose a given set if we "shuffle" the pieces. This is a very important concept to us as that is exactly what we will do to "double the ball". We need some terminology, so let $Y \subset X$ where X is a G-set. If A and B decomposes Y and there exists g_i, h_j such that $E = \bigcup_{i=1}^{m} g_i(A_i) = \bigcup_{j=1}^{n} h_j(B_j)$ we say that Y is G**-paradoxical**. This can also be stated with G-equidecomposition in the following way: $Y \sim_G A$ and $Y \sim_G B$. We shall now prove a result that under certain assumptions states that a paradoxical group G makes its G-set X paradoxical. This is where the non-constructiveness comes into play as we will need the axiom of choice to prove this result.

Lemma 1. *If G acts freely on X and G is paradoxial, then X is G-paradoxical.*

Proof. Let $g_i, h_j \in G$ and $A_i, B_j \subset G$ for $1 \leq i \leq n, 1 \leq j \leq m$ such that $A = \bigcup_{i=1}^{n} A_i,\ B = \bigcup_{j=1}^{m} B_j$ and $A \sim_G G$ and $B \sim_G G$. We now use the axiom of choice to construct a set M that contains exactly one element from each orbit of G in X. We use this set to partition X in the sets $M_g = \{g(M) : g \in G\}$. We need to prove that these sets cover X and that they are disjoint. To see that $X = \bigcup_{g \in G} M_g$ note that for a given $m \in M \subset X$ the value of $M_g(m)$ is the orbit of m under g and since we iterate over all $g \in G$ we use the fact that the orbits of G cover the set it acts on. Assume that M_g is not disjoint. Then there are $h, g \in G$ with $h \neq g$ and $m, n \in M$ such that $g(m) = h(n) \Rightarrow m = g^{-1}h(n) = f(n)$ where $f = g^{-1}h$. This implies that m and n is in the same orbit, but by construction it must then be the case that $m = n$. This, however, is a contradiction as G acts freely on X and therefore have no nontrivial fixed points! Therefore M_g is a partition of X.
Now since $A_i \cap B_j = \emptyset$ for all i, j and M_g is disjoint the sets $A'_i = \bigcup_{g \in A_i} M_g$ and $B'_j = \bigcup_{h \in B_i} M_h$ are also disjoint for all i, j. Now since $G = \bigcup_{i=1}^{n} A_i$ and M_g partitions X the set:
$\bar{A} = \bigcup_{i=1}^{n} g_i\left(A'_i\right) = \bigcup_{i=1}^{n} g_i\left(\bigcup_{g \in A_i} M_g\right)$ is a decomposition of X and similarly $\bar{B} = \bigcup_{j=1}^{n} h_j\left(A'_j\right) = X$ so that $\bar{A} \sim_G X$ and $\bar{B} \sim_G X$ proving that X is G-paradoxical. □

To prepare for an important result that leads up to the anticipated result we need one more concept. That is the notion of a **free group** (not to be confused with a group that acts freely on a set!). We

say that a group F is **free** if there is a subset $S \subset F$ such that every element in F can be written as a *unique* finite product of elements in S and their inverses, called a **word**. If it should happen that an element is followed or preceeded by its inverse we substitute that combination by the empty string e. If none of these combinations appear in a word we say that the word is **reduced**. We therefore see that the the free group F consists of all reduced words in S, where the group multiplication is concatenation of words, and possibly reducing "illegal" combinations. We also note that the cardinality of the generating set S is called the rank of F. There is a result that states that if we have two free groups of equal rank, then they are isomorphic.
In the following proof we will be interested in the free group generated by two elements, and we denote it by F_2.

Lemma 2. *F_2 is paradoxically decomposable.*

Proof. Say the generators of F_2 are a and b. Then F_2 is all finite reduced words consisting of a, b, a^{-1}, b^{-1}. We write concatenation of two words as $w_1 \cup w_2$. Define the set $F(a)$ as all words starting with a and similarly for $F(a^{-1}), F(b)$ and $F(b^{-1})$. Now note that $F_2 = \{e\} \cup F(a) \cup F(a^{-1}) \cup F(b) \cup F(b^{-1})$. Furthermore we have $F_2 = \{a\} \cup F(a^{-1}) \cup F(a)$ as we can write every word in this way by choosing suitable values (possibly empty!) in the sets. Similarly we also have $F_2 = \{b\} \cup F(b^{-1}) \cup F(b)$. This shows that F_2 is paradoxical as we have found two different decompositions. $\square$

The proof of this Lemma illustrates the technique we will be using in the proof of the Banach-Tarski paradox; Split the ball up in pieces, then "do something" with the pieces and patch them together in such a way that we get a paradoxical decomposition. We now make this idea more specific by showing that we can find a paradoxical decomposition of the rotation group $SO(3) \subset E(3)$ in $\mathbb{R}^3$.

Lemma 3. *There exists a paradoxical subset H_G of $SO(3)$.*

Proof. Let $\mathbb{R}^3$ be given its orthonormal basis and then consider rotations λ and ϕ which are one third of a rotation around the z and x axes correspondingly (Note: It is not important which axes one chooses here) and set $G = \{\lambda, \phi\}$. We will now show that the group $H_G \subset SO(3)$ that G generates is paradoxical by showing it is isomorphic to F_2. Since the rotations of any point in $\mathbb{R}^3$ can be represented by a matrix with respect to the orthonormal basis, so can the rotations in G. Furthermore, there exists a basis for G consisting of:

$$\lambda = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix}, \phi = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

We now show that H_G is a free group by showing that no nontrivial word consisting of $\{\lambda, \phi, \lambda^{-1}, \phi^{-1}\}$ is the identity (which is to say that G generates the whole of H_G). So let ω be a word in $\{\lambda, \phi, \lambda^{-1}, \phi^{-1}\}$. We can without loss of generality assume that ω ends with λ (the same argument works with any other element as well). We now proceed by induction on the word length to show that $\omega(0,0,1) = \frac{1}{2^n}(a, \sqrt{3}b, c)$ where $a, b, c \in \mathbb{Z}$ and $2 \not| b$. When the length is 1 we have $\omega = \lambda$ and $\lambda(0,0,1) = \frac{1}{2}(1, \sqrt{3}, 0)$ which checks out. Now assume the proposition holds for a word ω of length k, let $\omega' \in \{\lambda, \phi, \lambda^{-1}, \phi^{-1}\}$ and form the word $\omega'\omega$. By the induction hypothesis we know that $\omega(0,0,1) = \frac{1}{2^k}(a, \sqrt{3}b, c)$ so we assume that $\omega' = \{\lambda, \lambda^{-1}\}$ and compute:

$$\omega'\omega(0,0,1) = \frac{1}{2^k} \begin{bmatrix} \frac{1}{2} & \mp\frac{\sqrt{3}}{2} & 0 \\ \pm\frac{\sqrt{3}}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix} (a, \sqrt{3}b, c)^T = \frac{1}{2^{k+1}}(a \mp 3b, \sqrt{3}(b \pm a), c)^T$$

Since a, b, c are integer and from the induction hypothesis $2|a$ we have that $2 \not| \sqrt{3}(b \pm a)$ since $2 \not| b$. Similarly for $\omega' = \{\phi, \phi^{-1}\}$ we have:

$$\omega'\omega(0,0,1) = \frac{1}{2^k} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \mp\frac{\sqrt{3}}{2} \\ 0 & \pm\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} (a, \sqrt{3}b, c)^T = \frac{1}{2^{k+1}}(a, \sqrt{3}(b \mp c), c \pm 3b)^T$$

With the same divisibility argument as over, this concludes the induction and we have proved that an arbitrary word ω cannot be the identity. Therefore it must be the case that H_G is a free group of rank 2 and therefore isomorphic to F_2 which implies that H_G is paradoxical. □

We now want to combine Lemma 3 with Lemma 1 to show a result known as the Hausdorff paradox. A quick note before we state the theorem and its proof is that if a set X is G-paradoxical where G is a subgroup of F it will also be the case that X is F-paradoxical. This just follows by extension of the elements in G.

Theorem (The Hausdorff paradox)**.** *Let K be a countable subset of the sphere $S^2 \subset \mathbb{R}^3$. Then $S^2 \setminus K$ is $SO(3)$-paradoxical.*

Proof. We Let G be the subgroup of $SO(3)$ constructed in Lemma 3, then G is a free group of rank 2. Now since every axis of rotation intersects the sphere in two points we have two fixed points for every rotation. Since the group G is generated by two elements it can at most be countable. This implies that the points that are left fixed by any rotation in G also at most is countable. Call the set of all these intersections K. Then the set $S^2 \setminus K$ has no nontrivial fixed points and so G acts freely on it. Then by Lemma 1 $S^2 \setminus K$ is G-paradoxical and by the remark before the theorem it is also $SO(3)$-paradoxical. □

Now that this result is proved the hardest and most tedious part working up to the paradox is done. Our last result is actually not so far from what we would like to prove. There is however that countable set K that we need to get rid off. It turns out that $S^2 \setminus K \sim_{SO(3)} S^2$:

Theorem. *Let $K \subset S^2$ be countable, then $S^2 \setminus K \sim_{SO(3)} S^2$*

Proof. Since $SO(3)$ is uncountable and K is countable it is possible to find a rotation τ such that $\tau(K) \cap K = \emptyset$. By applying τ again we see that $\tau^2(K) \cap K = \emptyset$ and similarly for any $n > 2 \in \mathbb{N}$. Therefore $\tau^n(K) \cap \tau^m(K) = \emptyset$ for any $n > m \in \mathbb{N}$ follows since $\tau^{n-m}(K) \cap K = \emptyset$. That is, the set $\{\tau^n(K) : n > 0 \in \mathbb{N}\}$ is pairwise disjoint.
Now let $\bar{K} = \bigcup_{n=1}^{\infty} \tau^n(K)$ for some $a \in \mathbb{N}$. We then note that $\tau(\bar{K}) = \bar{K} \setminus K$ which is to trivially say that $\tau(\bar{K}) \sim_{SO(3)} (\bar{K} \setminus K)$. Now $S^2 = (S^2 \setminus \bar{K}) \cup \bar{K} \sim_{SO(3)} (S^2 \setminus \bar{K}) \cup (\bar{K} \setminus K) = (S^2 \setminus K)$. □

This theorem in some way states that the class of $SO(3)$-equidecompositions "don't care" for sufficiently small sets. This theorem combined with the Hausdorff paradox and the way paradoxicality as a property depend in equidecompositions we automatically get the result that S^2 is $SO(3)$-paradoxical. Nowhere is the spheres radius used and therefore the result actually holds for any radius. To finish the discussion we only need to extend this to the solid ball. We use the trick to interpret the ball as an infinite number of spheres of increasing, bounded radii; Much like an onion.

Theorem (The Banach-Tarski paradox)**.** *The unit ball $\mathbb{D}^3 \subset \mathbb{R}^3$ is $E(3)$-paradoxical.*

Proof. Consider the unit sphere, and for every point on it connect it by a ray to the origin. By the previous two theorems we know that S^2 is $SO(3)$-paradoxical, say $S^2 = \bigcup_{i=1}^m g_i(A_i) = \bigcup_{j=1}^n h_j(B_j)$, now set $A_i^* = \{tx : t \in (0,1], x \in A_i\}$ and $B_j^* = \{tx : t \in (0,1], x \in B_j\}$, then $A_i^* \cap B_j^* = \emptyset$ for all i, j. It follows that $D^3 \setminus \{0\} = \bigcup_{i=1}^m g_i(A_i^*) = \bigcup_{j=1}^n h_j(B_j^*)$ and therefore $D^3 \setminus \{0\}$ is $SO(3)$-paradoxical.

Now we again need to remove some set to get the result we really want and here is where we turn to $E(3)$. We use exactly the same trick as in the theorem above by choosing a suitable rotation not through the origin. We end up with $\mathbb{D}^3 \sim_{E(3)} D^3 \setminus \{0\}$ and therefore D^3 is $E(3)$-paradoxical. $\square$

This proves the anticipated result. As a final notice the property of the balls radius is not used anywhere in this discussion so we can simply extend the result to hold for any solid ball. If it is not centered at the origin we can also use the translations of $E(3)$ to extend the argument in that case also. It is therefore very much possible to extend the proof to the whole of $\mathbb{R}^3$!