CARDINALITY OF PERMUTATION GROUPS

ERIN O'BRIEN

COLLEGE OF WILLIAM AND MARY

Abstract. In this paper, we discuss the different behaviors between finite and infinite sets. Let $|X|$ denote the cardinality of set X. Now consider any set T. Let $P(T)$, S_T, and $\mathcal{F}_T$ denote the powerset of T, the set of all bijections on T, and the set of functions from T to T, respectively. For a finite set T where $|T| = n$, $|P(T)| < |S_T| < |\mathcal{F}_T|$ when $n > 3$. Using Zorn's Lemma, we show that for an infinite set T, the relationship is counterintuitive in comparison to the finite set: $|P(T)| = |S_T| = |\mathcal{F}_T|$. To demonstrate this, we consider the set of natural numbers, the set of real numbers, and finally, any general infinite set T.

1. Introduction. Let T be a set. We denote $P(T)$, S_T, and $\mathcal{F}_T$ as the powerset, the set of bijections on T, and the set of functions from T to T, respectively. Additionally, let $|X|$ denote the cardinality of any set X. We are interested in comparing the cardinalities of $P(T)$, S_T, and $\mathcal{F}_T$.

Finite sets are easy to consider, most likely because they eventually end. We seek to quantify ideas in a concrete manner, to assure us that we are completely correct in our assessment. It is easy to convince a child that 5 is greater than 4, 100 is greater than 20, and eventually that some huge number can be bigger than another huge number. We also, slightly less certainly but more still matter-of-factly, assert that infinity is larger than any other real number we can possibly consider. It is when we start to compare the cardinalities of different infinities that we become much less certain. It is one thing to show that the size of the set $\{1, 2, 3\}$ is larger than the set $\{4, 5\}$ but very different to convince someone that the set of real numbers between 0 and 1 is larger than the set of all natural numbers. It is when we move away from the tried-and-true task of demonstration and towards only being able to prove rather than show a concept that makes the field of mathematics esssentially counterintuitive. We will discuss one such counterintuitive argument within this paper.

It is known that if $|T| = n$, then $|P(T)| = 2^n$, $|S_T| = n!$, and $|\mathcal{F}_T| = n^n$. First, we discuss $|P(T)|$. The powerset of T, denoted $P(T)$, is the set of all of the subsets of T. Because we have n elements and each element is either in a set or it is not, it follows that the cardinality of the powerset of T is 2^n. Now consider the set of all bijections on this set T, defined as S_T. As per the definition of a bijection, the first element we map has n potential outputs. The second element has $n-1$ possibilities, the third as $n-2$, and so on. Thus, the cardinality of this set of bijections S_T is $n!$. Continuing, $|\mathcal{F}_T| = n^n$ because unlike the bijections, all elements have n possibilities to which they can map to. Thus, the set $\mathcal{F}_T$ has cardinality n^n.

Clearly, when $n > 3$, we have

$$|P(T)| < |S_T| < |\mathcal{F}_T|$$

for finite set T. However, we will show that for any infinite set T,

$$|P(T)| = |S_T| = |\mathcal{F}_T|$$

that is, there are bijections relating these sets.

2. Results for infinite sets. Let T denote an infinite set. Referencing [1], let X and Y be sets. If an injection exists such that $X \to Y$, we can conclude that $|X| \leq |Y|$. As such, for infinite sets, we can show that

$$|P(T)| \leq |S_T| \leq |\mathcal{F}_T|$$

Consider Cantor-Bernstein as an expansion on the cardinality of sets, as referenced by [2]:

CANTOR-BERNSTEIN. *Suppose two cardinal numbers A and B satisfy $A \leq B$ and $B \leq A$. Then $A = B$.*

We will use Cantor-Bernstein to prove that these cardinalities of infinite sets are actually equal, resulting in the following theorem:

THEOREM. *Let T be an infinite set. Denote the powerset of T as $P(T)$, the set of all bijections on T as S_T, and the set of all functions from T to T as $\mathfrak{F}_T$. Let $|X|$ denote the cardinality of any set X. Then*

$$|P(T)| = |S_T| = |\mathfrak{F}_T|$$

We will illustrate this identity with the set of natural numbers and the set of real numbers. We will then provide the general case to prove that this equality holds for any infinite set.

2.1. The set of natural numbers. We begin by proving $|P(\mathbb{N})| \leq |S_{\mathbb{N}}|$. Consider injection $g : P(\mathbb{N}) \to S_{\mathbb{N}}$. We define set $A \subseteq \mathbb{N}$, and define g such that $g(A) = f_A$, where f_A is a bijection. There is at least one bijection f_A such that $f_A(x) = x$ for all $x \in A$ and $f_A(x) \neq x$ for all $x \notin A$ by Zorn's Lemma, which [3] states as:

ZORN'S LEMMA. *Let A be a partially ordered set. If every totally ordered subset of A has an upper bound, then A contains a maximal element.*

We need to use Zorn's Lemma to show that we are able to create a derangement such that $f_A(x) \neq x$ for all $x \notin A$. We do this with the following lemma, referenced from [4]:

LEMMA 2.1. *Given an infinite set T, there is a function f such that $f_T(x) \neq x$ for all $x \notin T$.*

Proof. Let T be an infinite set. Consider the bijection functions $f : T \to T$. Order these functions such that $f \leq g$ if all of the fixed points of g are also the fixed points of f. Additionally, f and g agree on all elements that are not fixed points of f. By defining a chain on this partial order, we find an upper bound given by the function that has fixed points where all of the elements of this chain have fixed points. This function will map all other elements to the unique element that some elements of the chain map it to.

By Zorn's Lemma, there is a maximal element k from this partial order. If k has at least two fixed points, map those two fixed points to each other to create a greater element. Continuing in this fashion, our new maximal element defined f has at most one fixed point x. Select another element a and define a bijection g to coincide with f except $g(a) = x$ and $g(x) = f(a)$. This bijection g has no fixed points and is thus a full derangement. ■

Let $\overline{C}$ denote the complement of any set C. Lemma 2.1 allows us to form a derangement in $\overline{A}$, assuring that there exists a function f_A such that $f_A(x) \neq x$ for all $x \in \overline{A}$. Thus, if $A \subseteq \mathbb{N}$, $B \subseteq \mathbb{N}$, and $A \neq B$, we can define distinct bijections such that $f_A \neq f_B$. As we have shown that the injection g exists, and it follows that $|P(\mathbb{N})| \leq |S_{\mathbb{N}}|$.

Now consider $|S_{\mathbb{N}}| \leq |\mathfrak{F}_{\mathbb{N}}|$. Clearly the set of all bijections is a subset of the set of all functions such that $S_{\mathbb{N}} \subseteq \mathfrak{F}_{\mathbb{N}}$. It follows that $|S_{\mathbb{N}}| \leq |\mathfrak{F}_{\mathbb{N}}|$.

Finally, we show that $|\mathfrak{F}_{\mathbb{N}}| = |P(\mathbb{N})|$. We will use the following lemma, referenced from [5]:

LEMMA 2.2. *Let κ and μ denote infinite, non-zero cardinal numbers. Then $\kappa \cdot \mu = \max\{\kappa, \mu\}$.*

Note that $|\mathcal{F}_{\mathbb{N}}| = |\mathbb{N}^{\mathbb{N}}|$ and $|P(\mathbb{N})| = 2^{|\mathbb{N}|}$. As we showed above, $|P(\mathbb{N})| \leq |S_{\mathbb{N}}| \leq |\mathcal{F}_{\mathbb{N}}|$, meaning $|P(\mathbb{N})| = 2^{|\mathbb{N}|} \leq |\mathbb{N}^{\mathbb{N}}| = |\mathcal{F}_{\mathbb{N}}|$. But, $2^{|\mathbb{N}|} = |\mathbb{R}| \geq |\mathbb{N}|$. Now consider

$$|\mathbb{N}^{\mathbb{N}}| \leq |\mathbb{R}^{\mathbb{N}}| = \left(2^{|\mathbb{N}|}\right)^{|\mathbb{N}|} = 2^{|\mathbb{N}\times\mathbb{N}|} = 2^{|\mathbb{N}|}$$

by Lemma 2.2. Thus, we have shown

$$|P(\mathbb{N})| = 2^{|\mathbb{N}|} \leq |\mathbb{N}^{\mathbb{N}}| = |\mathcal{F}_{\mathbb{N}}| \leq 2^{|\mathbb{N}|} = |P(\mathbb{N})|$$

Using Cantor-Berstein, we demonstrate that $|\mathcal{F}_{\mathbb{N}}| = |P(\mathbb{N})|$.

We have shown that for the set of natural numbers, $|P(\mathbb{N})| \leq |S_{\mathbb{N}}| \leq |\mathcal{F}_{\mathbb{N}}| = |P(\mathbb{N})|$, concluding that

$$|P(\mathbb{N})| = |S_{\mathbb{N}}| = |\mathcal{F}_{\mathbb{N}}|$$

2.2. The set of real numbers. The proofs that $|P(\mathbb{R})| \leq |S_{\mathbb{R}}|$ and $|S_{\mathbb{R}}| \leq |\mathcal{F}_{\mathbb{R}}|$ are equivalent to the corresponding ones in **2.1**. We thus consider the proof that $|\mathcal{F}_{\mathbb{R}}| = |P(\mathbb{R})|$.

As with finite sets, it is clear that $|\mathcal{F}_{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}|$ and $|P(\mathbb{R})| = 2^{|\mathbb{R}|}$. Additionally, we know $|\mathbb{R}| = 2^{|\mathbb{N}|}$, meaning

$$|\mathcal{F}_{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}| = \left(2^{|\mathbb{N}|}\right)^{|\mathbb{R}|} = 2^{|\mathbb{N}\times\mathbb{R}|} = 2^{|\mathbb{R}|} = |P(\mathbb{R})|$$

by Lemma 2.2. Thus, we have proven that

$$|P(\mathbb{R})| = |S_{\mathbb{R}}| = |\mathcal{F}_{\mathbb{R}}|$$

2.3. The general case of an infinite set. Let T denote any infinite set. We show that $|P(T)| \leq |S_T|$ and $|S_T| \leq |\mathcal{F}_T|$. The proof of these inequalities mirrors those of the set of natural numbers (and in turn, the set of real numbers).

To continue, consider the following lemma:

LEMMA 2.3. *Let κ and μ denote infinite, non-zero cardinal numbers. Then $\kappa^{\mu} \leq \max\{2^{\kappa}, 2^{\mu}\}$.*

Proof. By [6], the cardinality of the powerset of an infinite set A is larger than this infinite set A. Thus, if κ denotes the cardinality of this infinite set A, then $\kappa < 2^{\kappa}$, meaning

$$\kappa^{\mu} < (2^{\kappa})^{\mu} = 2^{\kappa\cdot\mu} = 2^{\max\{\kappa,\mu\}}$$

by Lemma 2.2. However, by [7], we know the logarithm of an infinite cardinal number κ is defined as at least the cardinal number μ such that $\kappa \leq 2^{\mu}$. Following our pattern, $\kappa^{\mu} \leq (2^{\mu})^{\mu} = 2^{\mu}$. Therefore, we can conclude that $\kappa^{\mu} \leq \max\{2^{\mu}, 2^{\kappa}\}$. ■

We know $|P(T)| = 2^{|T|} \leq |T^T| = |\mathcal{F}_T|$; we show that $|P(T)| \geq |\mathcal{F}_T|$. Now using Lemma 2.3, we see that

$$|T^T| \leq \max\{2^{|T|}, 2^{|T|}\} = 2^{|T|}$$

So, because $|\mathcal{F}_T| = |T^T| \leq 2^{|T|} = |P(T)|$, we have proven that

$$|P(T)| \leq |S_T| \leq |\mathcal{F}_T| \leq |P(T)|$$

and therefore

$$|P(T)| = |S_T| = |\mathcal{F}_T|$$

for any infinite set T.

3. Conclusion. As an undergraduate student studying the applications of mathematics, the notion of researching a theoretical component of the subject was daunting. However, I appreciated the challenge and how the proof was merely an expansion on introductory theory. The individual concepts are elementary: the cardinality of infinite sets, the meaning of the powerset, permutations on a set. Considering these items in regards to a finite set is trivial, but it is the realization that the infinite set behaves differently certainly complicates what was once "elementary" and presents a topic of discussion.

I would like to thank Professor Chi-Kwong Li for teaching me this elementary theory from the beginning of my undergraduate career at the College and advising me for the duration of this research.

References

[1] Wofsey, Eric, "Set Theory: Counting the Uncountable",
URL = <http://www.math.harvard.edu/˜waffle/settheory.pdf>

[2] Nagy, Gabriel, "Cardinal Arithmetic",
URL = <https://www.math.ksu.edu/˜nagy/real-an/ap-b-card.pdf>.

[3] Conrad, Keith, "Zorn's Lemma and Some Applications",
URL = <http://www.math.uconn.edu/˜kconrad/blurbs/zorn1.pdf>.

[4] "Prove that every set with more than one element has a permutation",
URL = <http://math.stackexchange.com/questions/134152/prove-that-every-set-with-more-than-one-element-has-a-permutation-without-fixed>.

[5] Monk, Don, "Cardinals",
URL = <http://euclid.colorado.edu/˜monkd/m6730/gradsets06.pdf>

[6] Enderton, Herbert B., "Cantor's Theorem",
URL = <http://www.math.ucla.edu/˜hbe/resource/general/131a.3.06w/cantor.pdf>.

[7] Vladimirov, D. A., "Boolean Algebras in Analysis", page 109,
URL = <https://books.google.com/books?id=Y9ryCAAAQBAJ&pg>.