Cardinal Number

KENNETH HALPERN

May 21, 2015

CONTENTS

Part 1. Cardinality of Sets

1. Our Purpose

In many fields, one encounters large sets whose cardinalities are of interest. While there are a number of excellent textbooks on the subjects of set theory and cardinality, it is difficult to find a compendium of practical results. The majority of treatments focus on rigorous derivations and set-theoretic issues such as the axiom of choice and the continuum hypothesis. Though most calculations are not particularly difficult, some require care and an explicit listing of them can be useful.

Our purpose is to provide a brief discussion of the salient features of Cardinal Arithmetic, along with proof sketches and various tables enumerating practical cases. Though many of the latter are obvious, some are not – and we choose to provide a comprehensive reference rather than solely focus on the interesting cases. We do not pretend to a mathematically rigorous development and shamelessly ignore certain subtleties, though we attempt to identify the major pitfalls one may encounter in reasoning about Cardinality. The reader is presumed familiar with basic set theory, but in the interest of accessibility we define some mathematical terms in Appendix A.

In addition to the cardinality of sets, we discuss a number of other aspects of cardinality that arise in practical endeavor – such as bases for vector spaces and integrals – as well as a few digressions to clarify relevant topics.

For those in a hurry, the majority of results are contained in tables 1-3, table 4, and section 11.

The reader is directed to the bibliography for a number of more detailed treatments of set theory and cardinality as well as some of the key papers in the field.

2. Introduction

Cardinality can be thought of as a generalization of our notion of ”size”, applicable to ”large” sets. The precise definition involves a recursive construction. Two sets have the same cardinal number if a one-to-one correspondence between them exists[1]. For a finite set, the cardinality is simply the number of elements. The cardinalities of infinite sets are termed ”transfinite” numbers[2]. We will use the term ”cardinal number” to refer to the mathematical object which represents the size of a set and ”cardinality” to refer to the topic as well as the cardinal number associated with a given set. Their use will prove unambiguous.

Note that equal cardinality does not guarantee the existence of a bijection[3] which preserves any particular structure. For example, if two vector spaces have equal cardinality, there need not be a homomorphism between them. Cardinality is solely a property of the underlying sets.

As in other areas of mathematics, a few basic proof techniques suffice to address most questions of cardinality. Given a set S, we attempt to determine its cardinality relative to sets of known size. Typically this involves constructing a bijection to establish equal cardinality or an injection or surjection to exclude lesser or greater cardinalities. The most common sets used for such comparison are $\mathbb{R}$ and $\mathbb{N}$. For example we could try to show that every element of S can be codified as a real or that there exist elements which cannot be. Cantor's famous demonstration that $|\mathbb{Q}| = |\mathbb{N}|$ relied on such a construction, and a number of the proof sketches we provide have a similar flavor. In other cases, it is easy to demonstrate that S is an obvious subset or superset of a set of known cardinality. Because cardinality can be counter-intuitive, it is important to explicitly demonstrate any relationships rather than simply postulate them.

[1] It also is possible to view Cardinal Numbers as equivalence classes of sets.
[2] Along with the infinite ordinals, which we do not discuss here.
[3] For a review of this terminology, see Appendix A.

In the following, we assume the axiom of choice and the generalized continuum hypothesis (defined below)[4].

3. Notation

First a word on our notation:

(1) $|S|$ is the cardinality of a set S.
(2) $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are the sets of natural, rational, real, and complex numbers respectively.
(3) A^B denotes the set of maps $B \to A$ between two sets B and A. Equivalently, it is the set of partitions of B indexed by A.
(4) 2^B is a special case of A^B that corresponds[5] to the set of all subsets of B.
(5) S^n is a shorthand for $S \times S \times \cdots \times S$ (n-times) or, equivalently, $S^{\{1,\ldots,n\}}$.
(6) a, b are any cardinal numbers.
(7) n, m are any finite nonnegative integers.

4. Basic Operations

Let us define some basic operations of cardinal arithmetic.

(1) Addition: $|S_1| + |S_2| \equiv |S_1 \cup S_2|$ using a disjoint union[6].
(2) Multiplication: $|S_1| \cdot |S_2| \equiv |S_1 \otimes S_2|$ using a direct product.
(3) Exponentiation: $|S_1|^{|S_2|} \equiv |S_1^{S_2}| \equiv |f : S_2 \to S_1|$.
(4) Power set: $2^{|S_1|} \equiv |\{0,1\}^{S_1}|$. As mentioned earlier, this is a special case of exponentiation. It is the cardinality of the set of all subsets of S_1.
(5) Ordering: $|S_1| \leq |S_2|$ if an injection exists from $S_1 \to S_2$.
(6) Equality: $|S_1| = |S_2|$ iff there exists a bijection between S_1 and S_2. By the Cantor-Shroeder-Bernstein thm[7], this is equivalent to the condition that both $|S_1| \leq |S_2|$ and $|S_2| \leq |S_1|$.
(7) Strict Inequality: $|S_1| < |S_2|$ iff $|S_1| \leq |S_2|$ and $|S_2| \nleq |S_1|$.

5. Notation and definitions for classes of cardinal numbers

The following are the symbols and terms commonly used to represent cardinal numbers.

(1) The cardinality of the empty set is denoted $0 \equiv |\emptyset|$.
(2) Finite cardinals: For a set S_n bijective with $\{1 \ldots n\}$, the cardinality is denoted n. For the finite cardinals, the arithmetic operations defined above correspond exactly to those of the non-negative integers. There is no ambiguity in the use of n for both purposes.
(3) Transfinite cardinals: Any non-finite cardinals. The ones we consider here are denoted $\aleph_i$ and $\beth_i$ for $i \in \mathbb{N}$.

[4] We thank Alvin Halpern for his help in proofreading this work.

[5] We may view it as $\{0,1\}^B$, where each map assigns 1 to those elements of B that are members of the corresponding subset and 0 to all others.

[6] To be precise, it is $(S_1 \otimes (1)) \cup (S_2 \otimes (2))$.

[7] Obviously, the existence of a bijection implies the existence of injections in both directions. The Cantor-Schroeder-Bernstein thm says that the converse holds as well; the existence of injections in opposite directions implies the existence of a bijection. This may seem trivial, but it is not. The sets could be infinite and the two injections need not be inverses.

(4) $\aleph_0$: The cardinality[8] of the set $\mathbb{N}$. Any set with this cardinality is termed "Denumerable". Any set with either this or finite cardinality is termed "Countable"[9].
(5) $\aleph_i$: The i^{th} lowest transfinite cardinal number under the supposition that the lowest transfinites can be indexed by $\mathbb{N}$ (to be elaborated on below).
(6) $\beth_0$: The lowest transfinite cardinal number.
(7) $\beth_i$: Recursively defined as $\beth_i \equiv 2^{\beth_{i-1}}$ for $i > 0$.
(8) $\beth_1$ is termed the cardinality of the continuum[10] because $\beth_1 = |\mathbb{R}|$ as mentioned below.

There are some theorems and hypotheses that govern the relationships between the $\aleph$'s and $\beth$'s. We state them without proof here.

(1) Thm: There is a lowest transfinite cardinal number $\beth_0$. It is the cardinality of $\mathbb{N}$. Thus $\beth_0 = \aleph_0$.
(2) Thm: $2^a > a$. A set is always smaller than its power set. Thus, $\beth_i > \beth_{i-1}$.
(3) Thm: $\beth_1 = |\mathbb{R}|$. The proof of this is discussed in the Section 18.2.
(4) Continuum Hypothesis (CH): There is no cardinal number between $|\mathbb{N}|$ and $|\mathbb{R}|$. Equivalently, $\aleph_1 = \beth_1$.
(5) Generalized Continuum Hypothesis (GCH): There is no cardinal number between $\beth_i$ and $\beth_{i+1}$. Equivalently, $\aleph_i = \beth_i$ for $i > 1$.
(6) Thm (combined results of Godel, Cohen, and Sierpinski): Denote the axioms of Zermelo-Frankel set theory ZF and the axiom of choice AC[11]. We then have a set of results regarding their independence in combination with CH and the GCH (for clarification of what is meant by "independence", see Appendix B). These are as follows[12]:
   - AC and CH are independent given ZF. That is, ZF+AC+CH, ZF+$\sim$AC+CH, ZF+AC+$\sim$CH, and ZF+$\sim$CH+$\sim$AC each are consistent.
   - GCH is independent given ZF+AC. That is, ZF+AC+GCH, and ZF+AC+$\sim$GCH each are consistent.
   - AC and GCH are not independent given ZF. Specifically, ZF+GCH$\Rightarrow$AC (which means that ZF+GCH+$\sim$AC is inconsistent).
(7) Consequence of GCH: It is necessary (but not sufficient) for the GCH that the lowest transfinite numbers be indexed by $\mathbb{N}$. This is important because it means that if they are dense (even if only like $\mathbb{Q}$) the GCH would not hold.
(8) Thm: There are cardinals higher than any $\aleph_i$. The cardinals form a linearly ordered set, indexed by the ordinals.

Note that if we reject the AC (or to a lesser extent the GCH), most of the results discussed here no longer hold. From this point onward, we assume the GCH, drop the $\beth_i$, and simply use $\aleph_i$ to denote the (lowest) transfinite cardinal numbers (those indexed by $\mathbb{N}$). We do not consider transfinites higher than the $\aleph_i$, though many of the arithmetic results hold for those as well.

6. Basic properties of Cardinal Arithmetic

The following hold for all cardinal numbers a, b, and c:

(1) $a + b = b + a$

[8]The symbol ω is sometimes used for this as well.
[9]Occasionally, "countably infinite" is used in place of denumerable (as dictated by common usage); it is not to be confused with "countable" (which allows for finite values as well).
[10]It often is denoted c, but we do not use that convention here.
[11]ZF+AC typically is denoted ZFC, but we just use ZF+AC for clarity.
[12]Godel came up with the results involving our inability to disprove CH or GCH. Cohen came up with the results involving out inability to prove CH or GCH. Sierpinski proved that ZF+GCH+$\sim$AC is inconsistent.

(2) $a + 0 = a$
(3) $(a + b) + c = a + (b + c)$
(4) $a \cdot b = b \cdot a$
(5) $a \cdot 1 = a$
(6) $a \cdot 0 = 0$
(7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(8) $a \cdot (b + c) = a \cdot b + a \cdot c$
(9) $a^b \cdot a^c = a^{b+c}$
(10) $a^c \cdot b^c = (a \cdot b)^c$
(11) $(a^b)^c = a^{b \cdot c}$
(12) $a \geq 0$
(13) $a + b \geq a$
(14) $a \cdot b \geq a$ if $b > 0$
(15) $a^b \geq a$ if $b > 0$
(16) $a > b$ implies $c^a \geq c^b$ for $c > 0$
(17) $a > b$ implies $a^c \geq b^c$ for $c > 0$
(18) $a > b$ implies $c + a \geq c + b$
(19) $a > b$ implies $c \cdot a \geq c \cdot b$ for $c > 0$

Note that neither the existence nor uniqueness of a multiplicative or additive inverse is guaranteed. Also note that the last few inequalities are not strict, as they would be for ordinary numbers.

As mentioned, for the finite cardinals the operations above are those on $\mathbb{N}$. They act like ordinary numbers.

7. General Arithmetic Properties Of Transfinite Cardinals

In the following, all cardinals are nonzero and n is finite.

7.1. **Useful Special Cases.** First some useful special cases:

(1) $n < \aleph_0$. *Definition of* $\aleph_0$.
(2) $\aleph_i < \aleph_{i+1}$. *Follows from* $|X| < |2^X|$.
(3) $\aleph_i + \aleph_i = \aleph_i$. *Consider a mapping in which we alternately select elements. Alternatively, we can show that this set has strictly smaller cardinality than* $2^{\aleph_i}$*, which is the next higher* $\aleph$*, and thus must equal* $\aleph_i$.
(4) $n \cdot \aleph_i = \aleph_i$ for $n > 0$. *Repeat the additive operation* n *times.*
(5) $\aleph_0 \cdot \aleph_0 = \aleph_0$. *We use Cantor's argument for why* $|\mathbb{Q}| = \aleph_0$. *See section 18.1.*
(6) $\aleph_i \cdot \aleph_i = \aleph_i$ for $i > 0$. *Write as* $2^{\aleph_{i-1}} \cdot 2^{\aleph_{i-1}} = 2^{(\aleph_{i-1}+\aleph_{i-1})} = 2^{\aleph_{i-1}} = \aleph_i$.
(7) $\aleph_0 \cdot \aleph_i = \aleph_i$. *We note that* $\aleph_i \leq (\aleph_0 \cdot \aleph_i) \leq (\aleph_i \cdot \aleph_i) = \aleph_i$.
(8) $\aleph_i^n = \aleph_i$ for $n > 0$. *Just multiply a finite number of times.*
(9) $\aleph_0^{\aleph_0} = \aleph_1$. *See section 18.2.*

7.2. **General Cases.** Now for some more general results:

(1) $a + \aleph_i = \aleph_i$ for $a \leq \aleph_i$. *Clearly,* $a + \aleph_i \geq \aleph_i$ *because there is a surjection. But also* $a + \aleph_i \leq \aleph_i + \aleph_i = \aleph_i$.
(2) $a \cdot \aleph_i = \aleph_i$ for $0 < a \leq \aleph_i$. *Just note that* $\aleph_i = (1 \cdot \aleph_i) \leq (a \cdot \aleph_i) \leq (\aleph_i \cdot \aleph_i) = \aleph_i$.
(3) $a^b = max(a, 2^b)$ if either a or b (or both) is transfinite and $a > 1$ and $b > 0$. *See Section 18.4*[13].

[13] As a side note, for higher cardinal numbers (larger than those we consider here), the condition $a > 1$ is replaced with a more general one involving a concept called cofinality.

8. Specific Arithmetic Relations

We now list specific cases involving the first few $\aleph$'s, as these are of common use.

8.1. Cases involving $\aleph_0$.

(1) $n + \aleph_0 = \aleph_0$
(2) $\aleph_0 + \aleph_0 = \aleph_0$
(3) $n \cdot \aleph_0 = \aleph_0$ for $n > 0$
(4) $\aleph_0 \cdot \aleph_0 = \aleph_0$
(5) $n^{\aleph_0} = \aleph_1$ for $n > 1$
(6) $\aleph_0^n = \aleph_0$ for $n > 0$
(7) $\aleph_0^{\aleph_0} = \aleph_1$
(8) $\aleph_0^{\aleph_i} = \aleph_{i+1}$
(9) $\aleph_i^{\aleph_0} = \aleph_i$ for $i > 0$

8.2. Cases involving $\aleph_1$.

(1) $n + \aleph_1 = \aleph_1$
(2) $\aleph_0 + \aleph_1 = \aleph_1$
(3) $\aleph_1 + \aleph_1 = \aleph_1$
(4) $n \cdot \aleph_1 = \aleph_1$ for $n > 0$
(5) $\aleph_0 \cdot \aleph_1 = \aleph_1$
(6) $\aleph_1 \cdot \aleph_1 = \aleph_1$
(7) $n^{\aleph_1} = \aleph_2$ for $n > 1$
(8) $\aleph_0^{\aleph_1} = \aleph_2$
(9) $\aleph_1^n = \aleph_1$ for $n > 0$
(10) $\aleph_1^{\aleph_0} = \aleph_1$
(11) $\aleph_1^{\aleph_1} = \aleph_2$
(12) $\aleph_2^{\aleph_1} = \aleph_2$

9. Tables of common results

The above results, along with their extension to $\aleph_i$ for $i > 1$, may be summarized in three tables corresponding to the operations of addition, multiplication, and exponentiation. In the following, a and b refer to any nonzero cardinals and n and m refer to finite nonzero cardinals. Note that the exponentiation table is not symmetric: a is the row and b the column.

TABLE 1. Addition Between Cardinals

$a+b$	n	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_i$
m	$m+n$	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_i$
$\aleph_0$	$\aleph_0$	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_i$
$\aleph_1$	$\aleph_1$	$\aleph_1$	$\aleph_1$	$\aleph_2$	$\aleph_{\max(i,1)}$
$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_{\max(i,2)}$
$\aleph_j$	$\aleph_j$	$\aleph_j$	$\aleph_{\max(j,1)}$	$\aleph_{\max(j,2)}$	$\aleph_{\max(i,j)}$

TABLE 2. Multiplication Between Cardinals

$a \cdot b$	n	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_i$
m	$m \cdot n$	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_i$
$\aleph_0$	$\aleph_0$	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_i$
$\aleph_1$	$\aleph_1$	$\aleph_1$	$\aleph_1$	$\aleph_2$	$\aleph_{\max(i,1)}$
$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_{\max(i,2)}$
$\aleph_j$	$\aleph_j$	$\aleph_j$	$\aleph_{\max(j,1)}$	$\aleph_{\max(j,2)}$	$\aleph_{\max(i,j)}$

10. Counting Subsets, Sequences, Permutations, and Partitions

Many of the sets typically encountered are derived from other sets. Some common examples of these are subsets, sequences, partitions, permutations, and automaps.

TABLE 3. Cardinal Exponentiation

a^b	n	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_i$
m	m^n	$\aleph_1$	$\aleph_2$	$\aleph_3$	$\aleph_{i+1}$
$\aleph_0$	$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_3$	$\aleph_{i+1}$
$\aleph_1$	$\aleph_1$	$\aleph_1$	$\aleph_2$	$\aleph_3$	$\aleph_{\max(i+1,1)}$
$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_2$	$\aleph_3$	$\aleph_{\max(i+1,2)}$
$\aleph_j$	$\aleph_j$	$\aleph_{\max(j,1)}$	$\aleph_{\max(j,2)}$	$\aleph_{\max(j,3)}$	$\aleph_{\max(i+1,j)}$

10.1. **Definitions.** Given a set S, the difference between counting subsets and sequences is whether we draw elements with or without replacement. An automap is any map from S to itself. A permutation is a bijection from S to itself[14]. An injective automap doesn't map any two elements of S to the same element[15]. A partition is a unique separation of S into disjoint subsets. An ordered partition is such a separation in which the ordering of the subsets matters[16].

10.2. **Examples.** A simple illustration should suffice. Consider the set $S = (1, 2, 3)$. We use $()$ to denote unordered sets and $[]$ to denote ordered sequences. For maps (such as permutations and automaps), we use $[a, b, c]$ to denote the values of $[m(1), m(2), m(3)]$ (the ordering matters).

(1) Subsets: There are 8 subsets: $()$, (1), (2), (3), $(1, 2)$, $(1, 3)$, $(2, 3)$, $(1, 2, 3)$.
(2) Sequences: There are an infinite number of sequences: $[]$, $[1]$, $[1, 2]$, $[1, 2, 1]$, $[3, 1, 2, 3, 1, 2, 2, 2, 1, 3, \ldots]$, etc. Some are infinite in length.
(3) Partitions: There are 5 partitions: $((1, 2, 3))$, $((1),(2, 3))$, $((2),(1, 3))$, $((3),(1, 2))$, $((1),(2),(3))$.
(4) Ordered Partitions: There are 13 ordered partitions: $[(1, 2, 3)]$, $[(1),(2, 3)]$, $[(2, 3),(1)]$, $[(2),(1, 3)]$, $[(1, 3),(2)]$, $[(3),(1, 2)]$, $[(1, 2),(3)]$, $[(1),(2),(3)]$, $[(1),(3),(2)]$, $[(2),(1),(3)]$, $[(2),(3),(1)]$, $[(3),(1),(2)]$, $[(3),(2),(1)]$
(5) Permutations: There are 6 permutations: $[1, 2, 3]$, $[1, 3, 2]$, $[2, 1, 3]$, $[2, 3, 1]$, $[3, 1, 2]$, $[3, 2, 1]$.
(6) Automaps: There are 27 automaps: $[1, 1, 1]$, $[1, 1, 2]$, $[1, 1, 3]$, $[1, 2, 1]$, $[1, 2, 2]$, $[1, 2, 3]$, $[1, 3, 1]$, $[1, 3, 2]$, $[1, 3, 3]$, $[2, 1, 1]$, $[2, 1, 2]$, $[2, 1, 3]$, $[2, 2, 1]$, $[2, 2, 2]$, $[2, 2, 3]$, $[2, 3, 1]$, $[2, 3, 2]$, $[2, 3, 3]$, $[3, 1, 1]$, $[3, 1, 2]$, $[3, 1, 3]$, $[3, 2, 1]$, $[3, 2, 2]$, $[3, 2, 3]$, $[3, 3, 1]$, $[3, 3, 2]$, $[3, 3, 3]$.
(7) Injective Automaps: There are 6 injective automaps (as mentioned, for finite sets they are the same as permutations): $[1, 2, 3]$, $[1, 3, 2]$, $[2, 1, 3]$, $[2, 3, 1]$, $[3, 1, 2]$, $[3, 2, 1]$.

10.3. **Table of Results.** In the following table, the column is the cardinality of the underlying set and the row is the derivative set being counted. The symbol B_n refers to the n^{th} Bell number and OB_n refers to the n^{th} Ordered Bell Number[17]. We separate the cases $\aleph_0$ and $\aleph_1$, and refer to $\aleph_i$ with the implicit assumption that $i > 1$. Proof sketches for the entries in the table are provided in section 19.

From this, we observe that there are three classes of derivative sets:

(1) Finite, Countable, or Denumerable subsets or sequences – other than the countable or denumerable subsets or sequences of an $\aleph_0$ set. These all have the same cardinality as the underlying set.
(2) The countable or denumerable subsets or sequences of an $\aleph_0$ set are bumped up to $\aleph_1$ cardinality.

[14] The intuition for finite sets is that we rearrange elements. For infinite sets, we think of a permutation as a bijective automap.
[15] An ordinary automap could map many elements of S to the same element. For finite sets, every injective automap is a permutation; however, for infinite sets this need not be the case (consider $n \to 2n$ for $\mathbb{N}$).
[16] Of course, the elements within each subset remain unordered.
[17] This is our notation and is not standard.

TABLE 4. Cardinalities of Derivative Sets

Cardinality of Underlying Set→	$n > 0$	$\aleph_0$	$\aleph_1$	$\aleph_i$ $(i > 1)$
Finite Subsets	2^n	$\aleph_0$	$\aleph_1$	$\aleph_i$
Countable Subsets	2^n	$\aleph_1$	$\aleph_1$	$\aleph_i$
Denumerable Subsets	0	$\aleph_1$	$\aleph_1$	$\aleph_i$
All Subsets	2^n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Finite Sequences	$\aleph_0$	$\aleph_0$	$\aleph_1$	$\aleph_i$
Countable Sequences	$\aleph_1$	$\aleph_1$	$\aleph_1$	$\aleph_i$
Denumerable Sequences	$\aleph_1$	$\aleph_1$	$\aleph_1$	$\aleph_i$
Finite Partitions	B_n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Countable Partitions	B_n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Denumerable Partitions	0	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
All Partitions	B_n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Finite Ordered Partitions	OB_n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Countable Ordered Partitions	OB_n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Denumerable Ordered Partitions	0	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
All Ordered Partitions	OB_n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Permutations	$n!$	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Injective Automaps	$n!$	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$
Automaps	n^n	$\aleph_1$	$\aleph_2$	$\aleph_{i+1}$

(3) Everything else – all subsets; finite, countable, denumerable, or all partitions; permutations; and automaps – gets bumped up a cardinal number.

11. CARDINALITY OF SPECIFIC SETS

Let us enumerate the cardinalities of some common sets. There are several surprising cases. Note that all results which hold for $\mathbb{R}$ also hold for the complex numbers $\mathbb{C}$, which are of the same cardinality. Likewise, all results that hold for $\mathbb{Z}$ hold for $\mathbb{N}$ or any other infinite subset of $\mathbb{Z}$. In the following, we list different names for the same set separately to provide easy reference. Note that strings are just sequences of characters, but we mention them separately because of their use in computer science.

11.1. Sets with Cardinality $\aleph_0$.

(1) $\mathbb{N}$: The natural numbers. *This is the definition of* $\aleph_0$.
(2) $\mathbb{Z}$: The integers. $2\aleph_0 + 1 = \aleph_0$.
(3) $\mathbb{Z}^n$: n-tuples of integers. $\aleph_0^n = \aleph_0$.
(4) $\mathbb{Q}$: The rational numbers. *Cantor's famous "diagonal argument" for this is provided in section 18.1.*
(5) $\mathbb{Q}^n$: n-tuples of rationals. *Given that* $|\mathbb{Q}| = \aleph_0$, *we take* $\aleph_0^n = \aleph_0$.
(6) Finite strings over a finite alphabet. *Strings are just sequences of characters, and this was demonstrated in section 19.2 - item 7.*
(7) Finite sequences drawn from a finite set. *See section 19.2 - item 7.*
(8) Finite subsets of a denumerable set. *See section 19.2 - item 9.*
(9) Finite subsets of the integers or rationals. *See section 19.2 - item 9.*
(10) Finite strings over a denumerable alphabet. *These are the same as finite sequences drawn from an* $\aleph_0$ *set. See section 19.2 - item 8.*
(11) Finite sequences drawn from a denumerable set. *See section 19.2 - item 8.*
(12) Finite sequences of integers or rationals. *See section 19.2 - item 8.*

(13) The (Schauder) Fourier basis for the square integrable functions on $\mathbb{R}$. *This is just the set* $\{cos(n\pi x), sin(n\pi x)\}\forall n \in \mathbb{N}$*, and is denumerable.*
(14) The Hamel basis for $\mathbb{R}^{\mathbb{N}}$. *See section 16.1.*
(15) Any orthogonal basis for the set of continuous functions on $\mathbb{R}$. *See section 20.1. Alternately, we could use the Stone-Weierstrass thm.*
(16) Any Schauder or orthogonal bases for the sets of continuous, j-differentiable, smooth, periodic, or square integrable functions on $\mathbb{R}^n$ or $\mathbb{C}^n$. *See section 20.1.*
(17) Any Schauder or orthogonal basis for the set of analytic functions. *See section 20.1.*

11.2. Sets with Cardinality $\aleph_1$.

(1) $\mathbb{R}$: The reals. *This involves a cute Cantor-like argument. See section 18.2 and section 18.3 for two proofs.*
(2) $\mathbb{R}^n$: n-dimensional real space. $\aleph_1^n = \aleph_1$.
(3) $\mathbb{C}$: The complex numbers. *This may be written as* $\mathbb{R}^2$ *from a set theory standpoint, and* $\aleph_1^2 = \aleph_1$.
(4) $\mathbb{R}^{\mathbb{N}}$: A countably-infinite-dimensional real space. $\aleph_1^{\aleph_0} = \aleph_1$.
(5) Countable, Denumerable, or All subsets of $\mathbb{Z}$. *See section 19.2 - items 1, 4, and 14.*
(6) Finite, Countable, or Denumerable subsets of $\mathbb{R}$. *See section 19.2 - items 9, 12, and 13.*
(7) Countable or Denumerable sequences of integers. *See section 19.2 - items 5 and 10.*
(8) Countable or Denumerable sequences over a finite set. *See section 19.2 - items 5 and 10.*
(9) Finite, Countable or Denumerable sequences of reals. *See section 19.2 - items 5, 6, and 11.*
(10) Permutations of the integers. *See section 19.2 - item 16.*
(11) All maps between integers. *See section 19.2 - item 15.*
(12) Countable or Denumerable strings over a countable alphabet. *See section 19.2 - items 5 and 10.*
(13) Finite strings over an $\aleph_1$ alphabet. *See section 19.2 - item 6.*
(14) Finite, Countable, Denumerable, or All partitions (ordered or unordered) of a countable set. *See section 19.2 - items 20-25.*
(15) Continuous functions on $\mathbb{R}$. *See section 20.1 where the expansion functions could be any of the standard sets of orthogonal polynomials such as the Legendre, Laguerre, or Hilbert Polynomials. Alternately, we could use the Stone-Weierstrass thm. Yet another alternative would be to argue that since* $\mathbb{R}$ *is a separable space, every continuous function is determined by its values on any dense subset – of which* $\mathbb{Q}$ *is one. Hence the cardinality is at most* $\aleph_1^{\aleph_0} = \aleph_1$ *and is at least* $\aleph_1$ *because there is at least one continuous function per real number.*
(16) Differentiable functions on $\mathbb{R}$. *See section 20.1.*
(17) Smooth functions on $\mathbb{R}$. *See section 20.1.*
(18) Analytic functions on $\mathbb{C}$. *See section 20.1.*
(19) j-Differentiable, Smooth, Periodic, or Square integrable functions on $\mathbb{R}^n$ or $\mathbb{C}^n$. *See section 20.1.*
(20) $L^2(0,1)$: Square integrable functions on $\mathbb{R}$. *See section 20.1 using as expansion functions* $cos(n\pi x)$ *and* $sin(n\pi x)$.
(21) The Hamel basis of any of the function spaces listed above.

11.3. Sets with Cardinality $\aleph_2$.

(1) All subsets of the reals.*See section 19.2 - item 1.*
(2) All automaps on the reals. *See section 19.2 - item 15.*
(3) All permutations of the reals. *See section 19.2 - item 16.*
(4) Finite, Countable, Denumerable, or All partitions (ordered or unordered) of the reals. *See section 19.2 - items 20-25.*
(5) The Hamel basis for the maps between reals. *This was demonstrated in section 16.1.*

Part 2. Cardinality of Bases

12. Reasons to consider the Cardinality of Bases

Physics traffics extensively in vectors spaces and their bases. This hardly is surprising given its heavy reliance on calculus, a linear approximation, and the tractability of linear calculations in general. That the theories of modern physics rely on vector spaces in a fundamental rather than merely pragmatic way is a cause for both relief that they proved successful in so doing and concern that they rely on a possibly unjustified simplification. That discussion is beyond our present scope, however, and we merely mention it to motivate the present topic.

Almost all vector spaces that arise in physics have transfinite cardinality when regarded as sets. Many are infinite-dimensional as well, most notably the Hilbert spaces of quantum mechanics. An understanding of the bases of such spaces can be of great importance. In particular the ”size” of the basis plays an important role. For example, the eigenvectors of a mutually commuting set of observables in quantum mechanics constitute a basis for the Hilbert space of possible states. Their corresponding eigenvalues form the spectrum of possible measured values for those observables. The properties of this set – including its cardinality – strongly affect our analysis of the system.

The concept of dimension is purely an algebraic property of a vector space[18]. As shall be explained, the mathematical definition of dimension may not correspond to what we intuitively wish to describe when dealing with large spaces. Moreover, the formally defined basis often turns out to be of little interest. Alternate definitions prove far closer to our desired meaning, but require additional structure. Fortunately, this structure is present in many cases where the need arises.

A good example is the space of square integrable functions on $[-1, 1]$, a common Hilbert space that arises in quantum mechanics. As every physicist knows, this space has a Fourier basis in the functions $\cos(n\pi x)$ and $\sin(n\pi x)$ for integral n. These are orthogonal and can be made orthonormal through appropriate scaling. However the use of such a basis presumes a norm on the space, and the sums over vectors are infinite rather than finite ones.

Another closely related question is how many degrees of freedom an integral has. Loosely speaking, how big is the set of functions that can be described as an integral with given measure or an infinite sum over a specified set of ”basis” functions?

Once infinite sums (or integrals) are involved, constraints such as boundedness and convergence are implicitly imposed. Most vector spaces encountered in normal applications are product spaces, and their cardinalities are relatively straightforward to compute. However, in the presence of constraints they may no longer be regarded as simple product spaces. We must be more careful when analyzing them.

13. A Quick Review of Vector Spaces

(1) A vector space V is a set with addition and scalar multiplication defined, where ”scalar” means an element of some field[19] F.
(2) Like all algebraic objects, the vectors themselves are abstract. We generally work in terms of concrete representations, such as n-tuples of real numbers, that have the same structure as the space under consideration. The abstract space may be defined from a specific concrete

[18] Other definitions, such as ”topological dimension”, arise elsewhere in mathematics but are not of interest here.

[19] A ”field” in mathematics is an algebraic object that conforms to our ordinary notion of arithmetic: addition which is commutative, associative, and invertible, multiplication which is commutative, associative and invertible – other than division by 0 – and a distributive property that connects the two. Common fields are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$. There also are fields of functions that are larger than these.

representation that arises through need[20], implicitly as a set of conditions, or constructively through a choice of basis or other structural specification.

(3) We either may define the vector space from a basis or construct a basis for an existing space. This basis is a set of vectors $B \subseteq V$ with the following two properties:
   (a) The vectors within any finite subset $S \subseteq B$ are linearly independent. Formally, $\sum_{i=1}^{|S|} c_i s_i = 0$ iff $c_i = 0, \forall i$ where $c_i \in F$ (the underlying field), and $s_i \in S$. Stated simply, no element of S can be written as a linear combination of other elements of S.
   (b) Every $v \in V$ is a linear combination[21] of a finite set of vectors in B.

(4) It is possible to show that there always exists a basis for a vector space.

(5) The basis so defined is called a ”Hamel” basis. Its cardinality is the ”dimension” of the vector space.

(6) For spaces with $|V| \leq \aleph_1$ the Hamel basis and dimension behave as expected. However for larger spaces (such as $\mathbb{R}^{\mathbb{R}}$), it turns out that $|B| = |V|$. That is $dim(V) = |V|$ and is not a particularly useful concept.

14. Product Spaces

Many of the vector spaces that arise in practice are product spaces of the form X^Y. Moreover the space X often is the same as the underlying field F, for example $\mathbb{R}^3$ or $\mathbb{C}^4$. Even the function spaces $f : \mathbb{R} \to \mathbb{R}$ are product spaces of the form $\mathbb{R}^{\mathbb{R}}$ or subspaces of such products. Consequently, we are accustomed to thinking of $|Y|$ as the dimension of the space. As discussed, the latter is a vector space property; from the standpoint of cardinality it is meaningless. Nonetheless, cardinal theory can give us some important insights into its behavior for large $|Y|$. This is important when we ask questions such as how large the basis for a given function space is.

First, let us clarify what is meant by X^Y. From the standpoint of set theory, the meaning is clear; it is the set of maps $Y \to X$. In the case of $\mathbb{R}^3$ for instance, it would be the set of maps $f : \{1, 2, 3\} \to \mathbb{R}$, which corresponds to 3-tuples of reals.

However when X is a vector space, X^Y inherits an algebraic structure over the same underlying field F. Given two maps $f : Y \to X$ and $g : Y \to X$, the linear operation on X^Y is $(f + \eta g)$ defined by $(f + \eta g)(y) \equiv f(y) + \eta g(y)$ with $\eta \in F$ an element of the underlying field.

For finite-dimensional spaces, it may seem that $|Y|$ corresponds to our notion of dimension as well as yielding the size of the Hamel basis. However, this isn't quite the case. Specifically, the underlying vector space X may be multi-dimensional. Our overall dimension is $dim(X^Y) = |Y| dim(X)$. We should note one possible point of confusion. Suppose we encounter something like $(\mathbb{R}^3)^4$. It may seem that this could look structurally different from $\mathbb{R}^{12}$. However, $\mathbb{R}^3$ is not a field so there is no ambiguity in choosing $\mathbb{R}$ as the underlying field. That is, the dimensions remain independent. In general, when X itself can be expressed as a product space A^B we have $(A^B)^Y = A^{(B \times Y)}$.

15. Example of a Pitfall

Before proceeding, let's illustrate a potential pitfall in using Cardinality to understand vector spaces. As mentioned earlier, when considering the properties of vector spaces (or any other objects with structure), we must be careful not to confuse the properties of the underlying set with those of the

[20] This isn't circular. It is common practice to define an algebraic object from a concrete instance. That instance remains one of many representations of the abstract object. Theoretical results may be derived in terms of the abstract object and applied to all the representations without getting bogged down in the specifics on any individual choice.

[21] Note that this implies that this linear combination is unique. If two such combinations existed using subsets S_1 and S_2, then $S_1 \cup S_2$ would violate the first requirement.

space itself. For example, we could be tempted to count elements to determine the number of basis vectors needed to span the space. A set of a basis vectors should yield $|F|^a$ independent vectors. So shouldn't the number of basis vectors needed to span X^Y be the smallest a such that $|F|^a = |X|^{|Y|}$? In some sense, we expect $log_{|F|}(|X|^{|Y|})$ basis vectors.

But consider $\mathbb{R}^n$ (which implicitly has $F = \mathbb{R}$ as its field). We know that $|\mathbb{R}^n| = |\mathbb{R}|$. By this token we should require only a single basis vector, independent of n. In fact, this even would be true of $\mathbb{R}^{\mathbb{N}}$. The problem is that counting is not sufficient. The cardinality of the set is not enough to determine its linear structure. Equal cardinality guarantees that a bijection exists between $\mathbb{R}^n$ and $\mathbb{R}$. However, it does not preserve the algebraic structure. The structure-preserving maps are homomorphisms[22]. If such a map existed between $\mathbb{R}^n$ and $\mathbb{R}$, then they would indeed have the same dimension, and cardinality would be the least of our worries[23].

16. Useful Bases for Large Spaces

16.1. **Problem with the Hamel Basis.** The problem with the Hamel basis, is that it can prove unusably large for infinite-dimensional vector spaces. It is not difficult to see why. We must be able to write every vector as a finite linear combination of basis elements.

Let B be a set of basis vectors with which we intend to span a space V. Although the example in section 15 amply illustrates that cardinality alone cannot determine the basis size, it nonetheless may be used to place a lower bound on it. Structure or no structure, we cannot produce more than a certain number of vectors through linear combinations. We may require more basis vectors than this because of the structure, but we certainly cannot make do with fewer. Given a vector space V over field F, any finite subset $S \subset V$ can span at most $|F|^{|S|}$ vectors. But for $|F|$ transfinite, $|F|^{|S|} = |F|$. Let us suppose $|B|$ to be transfinite as well. As shown in section 19.2 - item 9, it has $|B|$ finite subsets. The maximum number of vectors spanned through finite linear combinations of elements in B is $|F| \cdot |B| = \max(|F|, |B|)$. We thus require that $\max(|F|, |B|) \geq |V|$.

Let us consider $|F| = \aleph_1$, as in the case of $\mathbb{R}$ or $\mathbb{C}$ (which almost invariably are the fields under consideration). As mentioned, for $V = \mathbb{R}^n$ or $V = \mathbb{R}^{\mathbb{N}}$, we get $|B| = 1$. We need only one basis vector from a cardinality standpoint, which isn't particularly helpful as a lower bound. However for larger spaces, things get interesting. For example, consider the space of maps $f : \mathbb{R} \to \mathbb{R}$. It has cardinality $|\mathbb{R}^{\mathbb{R}}| = \aleph_2$. For any $|V| > \aleph_1$, we require that $|B| = |V|$. Suddenly, $|B| = \aleph_2$. Obviously, this is an upper bound as well because we could choose $B = V$ as a trivial basis. Thus the Hamel basis is the same size as V itself and is not particularly useful.

16.2. **Alternate Infinite Bases.** For spaces in which infinite sums have meaning, we may define a more useful basis. This is termed a "Schauder" or "Orthogonal" basis depending on the context.

Though the Hamel basis may be too large to be useful, its definition is unambiguous and reliable. Finite sums always are defined. However, when we turn to infinite sums things get more difficult. We must demand some sort of convergence or other constraint that guarantees that our vectors will be meaningful. Pure product spaces also are out of the question, for any such constraint necessarily reduces us to a non-product subspace. Moreover, the mechanism for defining the sum involves the imposition of additional structure.

There are many such spaces and means of doing so, and we won't attempt a comprehensive discussion. Instead, let us restrict ourselves to the example of function spaces on $\mathbb{R}$ (the same results hold

[22] See appendix A for a review of this terminology.

[23] As an aside, we note that there is only one vector space of each dimension for a given underlying field F. That is, all vector spaces over F of the same dimension are isomorphic to one another.

for $\mathbb{C}$). Ideally, a basis would consist of a "manageable" set of functions with pleasant properties from which we could construct the entire desired function space. What is the "desired" function space? That depends on the context, but it rarely is the entirety of $\mathbb{R}^{\mathbb{R}}$. Rather, it likely is defined through some property. For example, the space of square integrable functions (using some measure) or periodic functions or bounded functions. Such definitions are meaningful only if the property is preserved under finite linear combinations. Stated differently, the property must be compatible with the vector space structure.

However instead of using a Hamel basis (which we know is possible but pointless), we attempt to construct the vectors as infinite sums or integrals of functions drawn from a different type of basis. In the case of square-integrable functions these would be the aforementioned sines and cosines. In the case of continuous functions they could be any of the standard orthonormal bases of special functions (Legendre polynomials, etc).

The same issue arises in considering dimension. The Hamel dimension may not be particularly enlightening, but it is well defined. It is not obvious what we mean by the dimension of a non-product space using a non-Hamel basis. In the case of a Fourier expansion, the closest to our intuitive ideal is the cardinality of the set of Fourier functions ($\aleph_0$ in the example given). While the cardinality of a Schauder basis may be informative, we must keep in mind that it may not have any real meaning as a "dimension" – especially for constrained subsets of product spaces.

The situation grows even less intuitive when we attempt to move to larger spaces. What does it mean to take an uncountable sum[24]? A non-Hamel basis may still be far smaller and more useful than a Hamel basis, but the definition needs to be made carefully and with appropriate attention to the exact space we are attempting to span. To discuss the various means of doing so is beyond our scope, but we emphasize the dangers inherent in attempting an intuitive definition of dimension or basis for such spaces.

17. Integrals and Sums

Integrals and sums are directly related to infinite-dimensional vector spaces. Specifically, an integral with a given measure can be thought of as a way to define infinite sums on such a space.

Consider a denumerable sum of the form $\sum_{i=0}^{\infty} f_i(x)a_i$ where the $f_i(x)$ constitute a fixed set of real functions and the a_i are real. If we view the f_i as some sort of basis spanning a subset of the function space $\mathbb{R}^{\mathbb{R}}$, then how many such functions can it describe?

The answer is quite simple: $\aleph_1^{\aleph_0} = \aleph_1$. This is the total number of maps $f : \mathbb{R} \to \mathbb{R}$ that may formally be written as a denumerable sum over the f_i. By "formally" we mean that these are maps from a set theory standpoint. We have said nothing about analytic properties such as boundedness or convergence. Nor need the a_i behave in any constrained manner.

It can be shown that $\aleph_1$ is the size of almost all of the commonly encountered function spaces over the real or complex numbers (or finite-dimensional or denumerable-dimensional versions of these). Section 20.1 provides a simple justification for why this is the case.

[24] To illustrate one of the issues, consider the question of linear ordering. Ordinary concepts of calculus such as limits and integrals presume denumerable sequences and sums with an implicit ordering of terms. The Well-Ordering theorem, equivalent to the Axiom of Choice, tells us that a strict linear ordering exists for any set. However, for summation (or limits) we need a natural choice of such ordering or some sort of proof that the sum is independent of ordering. Natural linear orderings exist on $\mathbb{N}$ and $\mathbb{R}$ because of their algebraic structures. But for other sets, there may be no natural choice.

Next let us ask the same question for integrals. Here we speak of indefinite integrals[25] $\int_0^x a(x')dx'$ where $a(x')$ is a function $\mathbb{R} \to \mathbb{R}$. On the surface, integrals may appear to have a finer granularity than series. The upper bound is real, not discrete, and the integral is a limit of series so we may expect it to contain more information. It doesn't.

To understand why integration does not surpass summation in content, consider the two apparent differences mentioned above. It may seem like the choice of sample points depends on the upper limit x, and hence can be any real number. For example, $\int_0^x a(x')dx'$ is a limit of sums where the n^{th} sum samples the points $\frac{x \cdot j}{n}$ with $j = 0 \ldots n$. Obviously, one could cheat by noting that the space of continuous functions is $\aleph_1$ in size, and hence the space of differentiable functions must be $\aleph_1$ as well. But let us consider a more direct approach. Although x may be any real number, we aren't really considering *any* real number. The Reimann integral can be defined more generally in terms of a mesh in which we sample one point from each interval. These need not be the points $\frac{j \cdot x}{n}$. If the Reimann integral exists then it doesn't matter which points we sample as long as we refine the mesh to contain n intervals as $n \to \infty$. We could choose a rational number in any of our intervals as our sample point. This is true regardless of x. So, we need only the rational values of $a(x)$ to determine the integral. The space is at most $\aleph_1^{\aleph_0} = \aleph_1$ in size.

So far, we only considered the set of differentiable functions (those that are integrals of other functions). The proper analog of the series (with fixed $f_i(x)$) is an integral of the form $\int_{-\infty}^{\infty} k(t,x)a(t)dt$. The $a(t)$ correspond to the a_i and the $k(t,x)$ correspond to the functions $f_i(x)$ where the index i has become the variable t. How many functions can be so described? This is a slightly different question because two variables are involved. However, once again we sample only a countable number of points in t (and hence a countable set of points from k). Thus, we can't get past a countable representation[26] for k.

One counterintuitive example is a comparison between a Fourier Series and a Fourier Integral[27]. Consider two sets of functions:

(1) The set of functions that can be written as Fourier Sums: $f(x) = \sum_{n=0}^{\infty}(a_i cos(n\pi x) + b_i sin(n\pi y)$.
(2) The set of functions that can be written as Fourier Integrals: $f(x) = \int_{-\infty}^{\infty}(a(t)cos(t \cdot x) + b(t)sin(t \cdot x)dt$.

It may seem unfathomable that the second doesn't describe a larger set of functions than the first. The Fourier integrals describe the set of square-integrable functions on $\mathbb{R}$ (denoted $L^2(\mathbb{R})$) while the Fourier series describe the square-integrable functions on a finite interval (usually taken to be $[-\pi, \pi]$) – or equivalently the functions on $\mathbb{R}$ with fixed periodicity. Given that there are $\aleph_1$ of the latter and at most an $\aleph_0$ product of such intervals to produce the former[28], we note that $\aleph_1^{\aleph_0} = \aleph_0$. The sets of functions differ but are the same size.

One familiar with Fourier Analysis may raise an objection regarding the Dirac δ function. A Dirac δ function may be constructed from a Fourier integral, yet represents the most precise refinement possible – specification of a single point. So why can we not construct an arbitrary map from such

[25] We could use any lower limit.

[26] What about general integrals on measure spaces? It certainly is possible for an integral to surpass a mere denumerable series, but this involves uncountable summation. This must carefully be defined, and the question of ordering dealt with. In such circumstances, it is not denumerable sums that we must compare the integral with. In fact, integration never is more than the associated summation. Conceivably integration could be defined through other means. Differential geometry relies on a reference space, usually $\mathbb{R}^n$, for charts, but more abstract definitions could be employed.

[27] Strictly speaking, the theory of Fourier Series and Integrals is rather involved. A Fourier series (or transform) is an approximation. The series converges at almost every point, and measure theory must be invoked to properly discuss the topic. In fact, measure theory largely arose from this need.

[28] There are fewer because of redundancy and the global constraint of square-integrability.

δ functions? There are two problems. First, we may get arbitrarily close to a δ function through a Fourier integral, but "arbitrarily" close in this case means a denumerable limit as distance goes to 0. We always can find a rational number arbitrarily close to the point. Second, we can only sample a denumerable number of δ functions at different points without moving to a non-denumerable summation. The integral is not equipped for this. Were we to attempt it, the integral would continue to sample a denumerable set of points and we would fool ourselves into thinking we have more information than we do. In truth, the Dirac δ function is not really a function and only has meaning under an integral. It is a dual to a function (also called a distribution) and cannot be used as a basis vector of a function space[29].

We employed a Riemann measure in our discussion. For other types of integrals the size of the sample space must be examined more carefully[30].

Part 3. Proof Sketches

18. Outlines of Some Basic Important Proofs

18.1. Cantor's proof that $\aleph_0 \cdot \aleph_0 = \aleph_0$. Cantor provided a famous argument for why $|\mathbb{Q}| = |\mathbb{N}|$, which we briefly sketch here. Create a 2-dimensional grid with the x axis and y axis labelled with integers from the lower left corner to the right and up starting with 0. Then, diagonally zig zag starting from the lower left corner and lay a successive integer in each square traversed. The entire grid will be covered. We have shown that $\aleph_0 \cdot \aleph_0 = \aleph_0$. As an important aside, note that equal cardinality does not guarantee equivalence of other properties. For example, $\mathbb{Q}$ is dense, while $\mathbb{N}$ is not. We cannot construct a bijection which preserves their respective linear orderings.

18.2. Proof that $\aleph_0^{\aleph_0} = \aleph_1$. Let $\mathbb{N}$ be our set of size $\aleph_0$ and $[0, 1] \subset \mathbb{R}$ be our set of size $\aleph_1$. The set $\mathbb{N}^{\mathbb{N}}$ corresponds to all denumerable sequences of non-negative integers. Given any such sequence (indexed by $n_i \in \mathbb{N}$), we construct a real from $[0, 1]$ as follows: Write a decimal point followed by n_1 ones followed by a zero then n_2 ones followed by a 0 and so on. This yields a unique binary encoding as a real. Likewise, any real in $[0, 1]$ can be written as a unique sequence of non-negative integers (adjacent 0's become 0 integers).

18.3. An Alternate Proof that $|\mathbb{R}| > \aleph_0$. Cantor provided an elegant proof that $|\mathbb{R}| > |\mathbb{N}|$. It is easy to construct an isomorphism from $\mathbb{R}$ to $[0, 1)$, so let's work with the unit interval. Represent each real by a sequence of digits following a decimal point. Suppose we could index them with the integers. Write the reals below one another so we have an array of digits. Now construct a new real in the following manner. For the first digit, choose anything but the first digit of the first real. For the second, choose anything but the second digit of the second real. Following this regimen, we end up with a real number that differs from each existing real in at least one digit. Thus the reals cannot be counted.

18.4. Proof that $a^b = max(a, 2^b)$. To prove that $a^b = max(a, 2^b)$ when at least one of a and b is transfinite and $a > 1$, there are several cases to consider:

(1) $\aleph_i^b$ ($b > 0$ and $i > 0$): Write this as $(2^{\aleph_{i-1}})^b = 2^{b \cdot \aleph_{i-1}} = 2^{\max(b, \aleph_{i-1})} = \max(2^b, \aleph_i)$.
(2) $n^{\aleph_0}$ ($n > 1$): $\aleph_1 = 2^{\aleph_0} \leq n^{\aleph_0} \leq \aleph_0^{\aleph_0} = \aleph_1$.

[29] This is a vast oversimplification but addresses the question.

[30] It seems unlikely that any integral defined as a countable limit of some sort will yield a space of cardinality $\aleph_2$, but we do not claim to know of a proof to this effect.

(3) $\aleph_0^{\aleph_0}$: We saw that this is $\aleph_1$.
(4) $\aleph_0^n$: We saw that this is $\aleph_0$.
(5) $\aleph_0^{\aleph_i}$ $(i > 0)$: $\aleph_{i+1} = 2^{\aleph_i} \leq \aleph_0^{\aleph_i} \leq \aleph_i^{\aleph_i} = \max(2^{\aleph_i}, \aleph_i) = \aleph_{i+1}$.

19. Proof Sketches for the Sets in Table 4

19.1. **General Observations.** To justify the entries in table, we begin with some simple observations:

(1) "X" subsets $\subseteq$ "X" sequences, where "X" is Finite, Denumerable, or Countable. Each such subset is a sequence of the same type.
(2) Permutations $\subseteq$ injective-automaps $\subseteq$ automaps. Each permutation is an injective-automap and each injective-automap is an automap.
(3) Partitions $\subseteq$ automaps. Each partition is a map from S to a set which indexes the groupings in that partition. The largest such set is of size $|S|$, corresponding to a partition into individual elements. Using S as the index set, each partition thus corresponds to an automap.
(4) "X" Partitions $\subseteq$ "X" Ordered Partitions, where "X" is Finite, Denumerable, Countable, or All. Each partition corresponds to at least one ordered partition.
(5) The automaps of S are given by S^S.
(6) The set of all subsets of S is given by 2^S.
(7) The Denumerable sequences over S are given by $S^{\mathbb{N}}$.

19.2. **Specific Proof Sketches.** Now for the details. The following are comments and derivation outlines for the elements in the table.

(1) All Subsets (any): As mentioned, there are $2^{|S|}$ subsets of a set. For infinite sets, $2^{\aleph_i} = \aleph_{i+1}$ (for $i \geq 0$).
(2) Finite or Countable Subsets (n): The number of subsets – finite, countable, or all – of a finite set is just 2^n.
(3) Denumerable Subsets (n): There trivially are no denumerable subsets of a finite set.
(4) Countable Subsets $(\aleph_0)$: The number of countable subsets of $\aleph_0$ is $\aleph_1$. *All subsets of $\aleph_0$ are countable, and there are $2^{\aleph_0}$ subsets.*
(5) Denumerable Sequences (any): The number of denumerable sequences is $\aleph_1$ drawn from sets of size n or $\aleph_0$, and $\aleph_i$ drawn from a set of size $\aleph_i$ (for $i > 0$). *The number of denumerable sequences drawn from a set S is just $|S|^{\aleph_0}$. For n or $\aleph_0$, this is $\aleph_1$. For $\aleph_i$ (where $i > 0$), it is $\aleph_i$.*

Uses item 5.

(6) Finite Sequences ($\aleph_1$ or $\aleph_i$): There are $\aleph_i$ finite sequences drawn from a set of size $\aleph_i$ with $i > 0$. *As discussed in item 5, there are $\aleph_i$ denumerable sequences (for $i > 0$). The number of finite sequences is bounded above by this (we can map each finite sequence to a denumerable sequence by adding a denumerable number of copies of a fixed element after it). It is bounded below by the number of single element sequences, which also is $\aleph_i$.*
(7) Finite Sequences (n): There are $\aleph_0$ finite sequences drawn from a finite set with $n > 0$ elements. *View each sequence as a base $(n+1)$ representation of a natural number with only nonzero digits. There are at least $\aleph_0$ sequences (using one element repeated) and so the result is bounded by $\aleph_0$ on both sides.*
(8) Finite Sequences $(\aleph_0)$: There are $\aleph_0$ finite sequences drawn from a set with $\aleph_0$ elements. *Let $\mathbb{N}$ be our $\aleph_0$ set. Consider a binary code for each natural number consisting of a zero followed by n ones. Any finite sequence of natural numbers generates a finite binary string, thus a natural number. Any natural number can uniquely be decomposed into a sequence by using the zeros as break points. Thus the number of finite sequences is just $\aleph_0$.*

Uses items 6 and 8.

(9) Finite Subsets ($\aleph_0$, $\aleph_1$, or $\aleph_i$): The number of finite subsets of $\aleph_i$ is $\aleph_i$ (where $i \geq 0$). *There are at least $\aleph_i$ single-element subsets, so this is a lower bound. The number of finite sequences forms an upper bound, and as shown in items 6 and 8, this is $\aleph_i$.*

Uses items 5, 7, and 8.

(10) Countable Sequences ($\aleph_0$ or n): There are $\aleph_1$ countable sequences drawn from $\aleph_0$ or n. *From items 5, 7, and 8 there are $\aleph_0$ finite and $\aleph_1$ denumerable sequences, so the sum is $\aleph_1$.*

Uses items 5 and 6.

(11) Countable Sequences ($\aleph_1$ or $\aleph_i$): There are $\aleph_i$ countable sequences drawn from $\aleph_i$ (where $i > 0$). *items 5 and 6, there are $\aleph_i$ finite and $\aleph_i$ denumerable sequences, so the sum is $\aleph_i$.*

Uses item 5.

(12) Denumerable Subsets ($\aleph_1$ or $\aleph_i$): The number of denumerable subsets of $\aleph_i$ is $\aleph_i$ (where $i \geq 1$). *It clearly cannot be greater than the number of denumerable sequences, shown in item 5 to be $\aleph_i$. It also is bounded below by $\aleph_i$. To see this, select any denumerable subset $A \subset S$ of our set S. The remaining elements $(S - A)$ must be $\aleph_i$ in number because $a + \aleph_0 = \aleph_i \Rightarrow a = \aleph_i$. We construct $\aleph_i$ denumerable subsets as $\{x\} \cup A$ for each $x \in S - A$.*

Uses items 9 and 12.

(13) Countable Subsets ($\aleph_1$ or $\aleph_i$): The number of countable subsets of $\aleph_i$ is $\aleph_i$ (where $i \geq 1$). *As shown in items 9 and 12, there are $\aleph_i$ denumerable subsets and $\aleph_i$ finite subsets.*

Uses item 4.

(14) Denumerable Subsets ($\aleph_0$): There are $\aleph_1$ denumerable subsets of $\aleph_0$. *We are bounded above by the number of countable subsets, shown in item 4 to be $\aleph_1$. We also are bounded below by $\aleph_1$. To see this, we use a similar trick as in item 12. In the present case, we divide our set S into two disjoint denumerable subsets A and B by sorting alternating elements into them (the ordering we choose is irrelevant). We then construct a denumerable number of subsets by pairing $\{x\} \cup B$ for each element in A.*

(15) Automaps ($\aleph_0$, $\aleph_1$, or $\aleph_i$): There are $\aleph_{i+1}$ automaps of a set with cardinality $\aleph_i$ (where $i \geq 0$). *The number of automaps is directly computable as $\aleph_i^{\aleph_i} = \aleph_{i+1}$.*

Uses items 1 and 15.

(16) Permutations ($\aleph_0$, $\aleph_1$, or $\aleph_i$): There are $\aleph_{i+1}$ permutations (auto-bijections) of a set with cardinality $\aleph_i$ (where $i \geq 0$). *Each permutation is an automap, so the number of permutations is bounded above by the number of automaps – shown in item 15 to be $\aleph_{i+1}$. It is bounded below by the set of all subsets, shown in item 1 to also be $\aleph_{i+1}$. To see this, consider that associated with any subset with more than one element there is at least one permutation that solely involves all elements in the subset. It is not hard to see that the number of non-single-element subsets is $\aleph_{i+1}$. Both bounds are $\aleph_{i+1}$ and this must be the cardinality of the set.*

(17) Injective automaps (n): The number of injective automaps is $(n!)$. *The set of injective automaps is the set of permutations for a finite set, which has size $(n!)$.*

Uses items 15 and 16.

(18) Injective automaps($\aleph_0$, $\aleph_1$, or $\aleph_i$): There are $\aleph_{i+1}$ injective automaps of a set of size $\aleph_i$ with $i \geq 0$. *Every permutation is an injective automap and every injective automap is an automap. So we are bounded by the cardinalities of these sets. From items 15 and 16 we know that these both are $\aleph_{i+1}$.*

(19) All, Finite, Countable, and Denumerable Partitions (n): Obviously, there are no denumerable partitions of a finite set. All partitions are finite. The number of partitions of a finite set is given by the n^{th} Bell Number[31] B_n.

Uses items 1 and 15.

(20) All Partitions ($\aleph_0$, $\aleph_1$, or $\aleph_i$): The total number of partitions of a set of size $\aleph_i$ (for $i \geq 0$) is $\aleph_{i+1}$. *Given a subset, there is at least one partition corresponding to it and its complement. So we have a $2 \rightarrow 1$ map from subsets into partitions. The cardinality of an infinite set modulo 2 is the same as that of the set so we are bounded below by $\aleph_{i+1}$, seen in item 1 to be the number of subsets. We also are bounded above by the number of automaps, shown in item 15 to be $\aleph_{i+1}$. To see this, note that each partition is such a map. The largest partition has one element per group and requires an index of size $\aleph_i$. All other partitions could be indexed by a subset of this. So every partition corresponds to an automap. There may be many such automaps per partition, but that doesn't matter because we are establishing an upper bound.*

Uses item 20.

(21) Finite Partitions ($\aleph_0$, $\aleph_1$, or $\aleph_i$): The number of finite partitions of a set of cardinality $\aleph_i$ (with $i \geq 0$) is $\aleph_{i+1}$. *There cannot be more finite partitions than all partitions, and in item 20 we showed there are $\aleph_{i+1}$ of these. Every subset of the set constitutes a 2-partition (actually this is a $2 \rightarrow 1$ map as discussed in item 20, but the cardinality of the set remains the same). So the number of finite partitions is at least as great as $\aleph_{i+1}$.*

Uses items 20 and 21.

(22) Denumerable Partitions ($\aleph_0$, $\aleph_1$, or $\aleph_i$): The number of denumerable partitions of a set of cardinality $\aleph_i$ (with $i \geq 0$) is $\aleph_{i+1}$. *There cannot be more denumerable partitions than all partitions, shown in item 20 to be $\aleph_{i+1}$ in number. To get a lower bound, we select a denumerable subset A of our set S (in the case of a set of size $\aleph_0$, this can be done by choosing alternate elements). We construct a single denumerable partition P of A where each element is in a separate group. The set $S - A$ still has cardinality $\aleph_i$, so as seen in item 21 it has $\aleph_{i+1}$ finite partitions. For each of these, we construct a denumerable partition of S by joining it with P as a single addition grouping. The resulting partition has a denumerable number of elements. There are $\aleph_{i+1}$ of these partitions, and this is our lower bound.*

Uses items 21 and 22.

(23) Countable Partitions ($\aleph_0$, $\aleph_1$, or $\aleph_i$): The number of denumerable partitions of an infinite set of cardinality $\aleph_i$ (with $i \geq 0$) is $\aleph_{i+1}$. *We add the numbers of finite and denumerable partitions, shown in items 21 and 22 to both be $\aleph_{i+1}$, to get $\aleph_{i+1}$.*

Uses items 21, 22 and 23.

(24) Finite, Countable, and Denumerable Ordered Partitions ($\aleph_0$, $\aleph_1$, and $\aleph_i$): There are $\aleph_{i+1}$ finite, countable, or denumerable ordered partitions of a set of size $\aleph_i$. *Every partition of type "X"*

[31] In fact, the Bell Number is defined this way. It is computed recursively and is beyond the scope of our discussion.

(where "X" is finite, countable, or denumerable), corresponds to at least one ordered partition of type X. So we are bounded below by the number of partitions of type X, which is $\aleph_{i+1}$ independent of X as shown in items 21, 22 and 23. Likewise, every countable ordered partition corresponds to at least one map from our set S to a subset of $\mathbb{N}$. There are at most $\aleph_0^{\aleph_i} = \aleph_{i+1}$ of these. So we are bounded above by this as well.

Uses item 24.

(25) All Ordered Partitions ($\aleph_0$, $\aleph_1$, and $\aleph_i$): There are $\aleph_{i+1}$ ordered partitions of a set of size $\aleph_i$. Though the argument is the same as for finite, countable, and denumerable ordered partitions, we discuss this case separately for an important reason. To speak of "all" ordered partitions of a large set requires that it be possible to linearly order a set of that size[32]. The cases of $\aleph_0$ and $\aleph_1$ are not a problem; we may use $\mathbb{N}$ and $\mathbb{R}$ as examples. However, the same must be true for a set of size $\aleph_i$ in order for the definition to be meaningful. The well-ordering theorem, equivalent to the axiom of choice, guarantees the existence of such an ordering. *We use a similar argument to that of item 24, but the index set is of size $\aleph_i$ instead of $\mathbb{N}$. This is because the largest partition has $\aleph_i$ groups. As a result there are at most $\aleph_i^{\aleph_i} = \aleph_{i+1}$ ordered partitions, and the same upper bound holds.*

(26) All, Finite, Countable, and Denumerable Ordered Partitions (n): The result is similar to the finite unordered partitions, but the resulting quantity is known as the "Ordered Bell Number"[33].

20. Proof Sketches Regarding Specific Sets in Section 11

20.1. **Almost all common sets of functions are $\aleph_1$.** It is not difficult to see that almost all common sets of functions on $\mathbb{R}$ or $\mathbb{C}$ are $\aleph_1$ in size. First, we note that if such a set contains any subset that is parametrizable by a single $\mathbb{R}$ or $\mathbb{C}$ number[34] then it has size at least $\aleph_1$. For example, the periodic functions have a phase or frequency parameter, the continuous functions contain a 1-parameter set corresponding to constant functions, and so on.

Next, we note that any set of functions whose elements can be expressed as denumerable sums over a fixed set of functions can have cardinality at most $\aleph_1^{\aleph_0} = \aleph_1$.

Thus, any set of functions that have series expansions and contain at least a one-parameter subset must be $\aleph_1$ in size.

This extends to any functions whose domain and range are $\mathbb{R}^n$, $\mathbb{C}^n$ or even $\mathbb{R}^{\mathbb{N}}$ and $\mathbb{C}^{\mathbb{N}}$. As long as the total series expansion is denumerable[35] , the size of the function space is $\aleph_1$.

Appendix A. Review of Maps

We include here a brief review of some basic terminology regarding maps. Let A and B be sets.

(1) A "map" $f : A \to B$ takes every element of A to some element of B. For element $x \in B$, we denote this $f(x) \in B$.
(2) The "domain" of the map is A and the "image" is $f(A) \subseteq B$. For $A_0 \subseteq A$, we denote by $f(A_0)$ the union of the images of the points in A_0.
(3) For a point y in B, the "inverse image" $f^{-1}(y)$ is the set of points x in A such that $f(x) = y$. The inverse image of $B_0 \subseteq B$ is defined similarly as the union of the inverse images of its points. Note that the inverse image of a point or set can be empty.

[32] The ordering need not have any utility or purpose; we simply require the existence of such an ordering.
[33] Like the Bell Number, it is defined recursively and is beyond the scope of our discussion.
[34] It need only be parametrizable on some finite interval.
[35] In fact, a denumerable product of such spaces works too because $\aleph_1^{\aleph_0} = \aleph_1$ is the overall cardinality – even though the product of series may have a nondenumerable number of terms.

(4) An "injection" or "one-to-one map" takes every element of A to a unique element of B. That is $f(x) = f(y)$ iff $x = y$.
(5) A "surjection" or "onto map" has B as its image. I.e. $\forall y \in B$, $\exists x \in A$ s.t. $f(x) = y$. Equivalently, the inverse image of every point in B is nonempty.
(6) A "bijection" or "one-to-one correspondence" (not to be confused with "one-to-one *map*" as in item 4 above) between sets is a map that is both an injection and a surjection. It uniquely identifies each element of A with an element of B.
(7) Given two injections, one from $A \to B$ and one from $B \to A$, it may seem obvious that a bijection exists. Though this turns out to be true, it is not trivial. Those injections need not be inverses of one another, and for infinite sets this can complicate things. That a bijection exists follows from the "Cantor-Schroeder-Bernstein" theorem as discussed earlier. See [4] for a detailed discussion.
(8) When we speak of algebraic objects, a "homomorphism" is a structure-preserving map between two objects. For example, for groups, $f(a \cdot b) = f(a) \cdot f(b)$. More generally, in Category theory a "morphism" is a structure preserving map between any two objects (they need not be algebraic).
(9) An "isomorphism" between algebraic objects is a bijective map which is a homomorphism in each direction. Objects between which an isomorphism exists are considered "isomorphic"[36] and are "the same" from an abstract standpoint.

Appendix B. Independence of Axioms

The meaning of "independence" of axioms may be a point of confusion, so we provide some clarification.

(1) An axiom is a statement that is taken to be true.
(2) By ∼x we mean that the statement "x is false" is taken to be true.
(3) When we refer to the truth of a set of statements (or treat such a set as an axiom) we mean that every statement in the set is true (that is, the logical "and" or "conjunction" of those statements). For such a set to be false, it suffices for any one member to be false.
(4) Note that our use of sets of statements as opposed to single compound conjunctive statements is not fundamental; we choose whichever lends clarity to the discussion.
(5) An axiom A is self-consistent if it is logically possible for it to be true. If it is a conjunctive statement then this requires that no part imply the falsity of any other part. If it is a set of statements then we require that no subset of them imply the falsity of any other subset. Similarly ∼A is consistent if it is logically possible. This means that some choice of truth values – other than all true – is consistent. Note that it is possible for each of A and ∼A to be self-consistent.
(6) By A+B (where A and B are statements or sets of statements), we mean the the statement "A and B are true" (or as sets, their union).
(7) From now on, any axioms we consider are assumed to be self-consistent.
(8) We say that axioms $x_1 \cdots x_n$ are independent of one another if all 2^n possible combinations $a_1 + \cdots a_n$ (where each a_i can take the values x_i or $\sim x_i$) are consistent. For example, the axioms "The grass is green" (denoted x) and "The sky is blue" (denoted y) are independent because all four statements "The grass is green and the sky is blue" (x+y), "The grass is green and the sky is not blue" (x+∼y), "The grass is not green and the sky is blue" (∼x+y), and "The grass is not green and the sky is not blue" (∼x+∼y) are consistent. However, if we add a third axiom: "The grass is the color of the sky" (denoted z), then there are 8 combinations to consider. The combination x+y+z is inconsistent and, though all other

[36] It is important to note that the property of two objects being isomorphic depends only on the existence of a map, rather than any specific map. It is an equivalence relation on the set of algebraic objects of a given type.

combos are consistent, we must conclude that the axioms (x,y,z) are not independent of one another.

(9) We say that axioms $x_1 \cdots x_n$ are independent given another axiom z (perhaps compound) if the 2^n combinations z+$a_1 + \cdots a_n$ (where a_i takes the values x_i or $\sim x_i$) all are consistent. In our example above, x and y are independent given ∼z but are not independent given z. This makes sense because if we take z as true, then x⇒∼y (and hence y⇒∼x).

(10) As illustrated above, if $x_1 \cdots x_n$ are independent given z it does not imply that they are independent given ∼z. If they are, then all the axioms z,$x_1 \cdots x_n$ are independent of one another.

(11) Conversely, if $x_1 \cdots x_n$ are not independent of one another then obviously they cannot be independent both given z and given ∼z.

(12) Note that it is perfectly plausible that assuming z would restrict the possible combinations of $x_1 \cdots x_n$. For example, suppose that $x_2 \cdots x_n$ are independent given x_1 but not given $\sim x_1$. If z⇒ x_1, then $x_2 \cdots x_n$ are independent. However, that just means that we say $x_2 \cdots x_n$ are independent given z (or perhaps given z+x_1 if the case were more complex).

References

Seminal works

[1] G. Cantor, "Contributions to the Founding of the Theory of Transfinite Numbers," Dover Publications, 1915

[2] W. Sierpinski, "Cardinal And Ordinal Numbers," Second Edition Revised, PNW-Polish Scientific Publishers, 1965

Good texts

[3] A. G. Hamilton, "Numbers, sets and axioms: the apparatus of mathematics," Cambridge University Press, 1982

[4] R. M. Smullyan and M. Fitting "Set Theory and the Continuum Problem," Dover Publications, 2010

[5] T. Jech "The Axiom of Choice," Dover Publications, Inc., 1973

Key Papers regarding the Continuum Hypothesis

[6] P. J. Cohen "The Independence of the Continuum Hypothesis," Proceedings of the National Academy of Sciences 50 (6), 1963 p. 1143-1148

[7] P. J. Cohen "The Independence of the Continuum Hypothesis, II," Proceedings of the National Academy of Sciences 50 (1), 1964 p. 105-110

[8] K. Godel "Consistency of the Continuum Hypothesis," Princeton University Press, 1940

[9] W. Sierpinski "L'hypothese generalisee du continu et l'axiome du choix," Fund. Math. 34, 1-5