Formal Preliminaries, Part 2: Cardinalities, Infinities, and Proof by Induction [1]

(1) **Some Key Players**

a. The Natural Numbers ($\mathbb{N}$)
- All the whole numbers greater than or equal to 0, {0, 1, 2, … }

b. The Integers ($\mathbb{Z}$)
- All the whole numbers (including those less than 0), { …, -2, -1, 0, 1, 2 … }

c. The Rational Numbers ($\mathbb{Q}$)
- All the numbers that can be written as a fraction, $\{ n/m : n, m \in \mathbb{Z} \ \& \ m \neq 0 \}$

d. The Real Numbers ($\mathbb{R}$)
- All the numbers that can be represented by an infinite decimal expansion
- All the rational numbers and all the irrational numbers (*e.g.*, π)

Note: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

1. Cardinalities and Infinities

(2) **Cardinality (Informal)** |A| = 'the cardinality of A'
= 'the number of elements in A'

(3) **Cardinality, Injection, and Bijection**

The following statements are intuitively true for finite sets. We'll therefore assume they are true for *all* sets (including infinite ones).

a. $|A| \leq |B|$ *if and only if* there is an **injection** f: A→ B

b. $|A| = |B|$ *if and only if* there is an **bijection** f: A→ B

Note:
- Recall that if f is a bijection, then f^{-1} is a bijection too.
- Thus, if there is a bijection f: A→B, then there is also a bijection f^{-1}: B→ A
  - Thus, by the definition in (3b), if $|A| = |B|$, then $|B| = |A|$ (as desired)
  - Also, as you can prove to yourself:
    If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$
    For any set A, $|A| = |A|$

[1] These notes are based upon the following required readings: Partee *et al.* (1993), Chapter 4, pp. 192-198.

(4) **Key Consequence: Infinite Sets Can Have Same Cardinality as Proper Subsets**

- Consider the following function: $f(x) = 2x$ / $f = \{ \langle x,y \rangle : y = 2x \}$

- This function f is a bijection from $\mathbb{N}$ to the set of even numbers!
    - It's an injection: every x is mapped to a different even number
    - It's a surjection: every even number is equal to 2x for some $x \in \mathbb{N}$

- Thus, even though $\{ n : n \in \mathbb{N} \text{ and n is even} \} \subset \mathbb{N}$,
  $|\{ n : n \in \mathbb{N} \text{ and n is even} \}| = |\mathbb{N}|$

- Intuitively, no finite set contains a proper subset of the same cardinality.
    - Thus, we can take this interesting property of $\mathbb{N}$ as characteristic of 'infinities'

(5) **Characterization of Non-Finite**
A set S is infinite *if and only if* there is a proper subset $S' \subset S$ such that $|S'| = |S|$

(6) **Transfinite Cardinals**

- Although it seems sensible to speak of $|\mathbb{N}|$, there is clearly no finite cardinal number $n \in \mathbb{N}$ such that $|\mathbb{N}| = n$.

- It will be useful to introduce new, *transfinite* cardinal numbers to allow us give a name to the cardinality of $\mathbb{N}$

- We introduce the special symbol '$\aleph_0$' (aleph null) below to refer to this first transfinite cardinal.

$$\aleph_0 = |\mathbb{N}|$$

(7) **Countable and Countably Infinite**

a. A set S is **countably** (**denumerably**) **infinite** *iff* $|S| = \aleph_0$
b. A set S is **countable** *iff* S is finite or S is countably infinite.

(8) **Demonstrating that an Infinite Set is Countable, Part 1**

- To show that an infinite set S is countable, show that there is a bijection from S to $\mathbb{N}$
- After all, this would entail $|S| = |\mathbb{N}| = \aleph_0$

(9) **The Natural Numbers Without Zero ($\mathbb{N} - \{0\}$) are Countable**

Consider the following function: $f(n) = n - 1$

a. The function f is clearly an injection from $\mathbb{N}-\{0\}$ to $\mathbb{N}$
(each number in $\mathbb{N}-\{0\}$ is mapped to a different member of $\mathbb{N}$)

b. The function f is clearly a surjection from $\mathbb{N}-\{0\}$ to $\mathbb{N}$
(every member of $\mathbb{N}$ is equal to (n-1) for some element in $\mathbb{N}-\{0\}$)

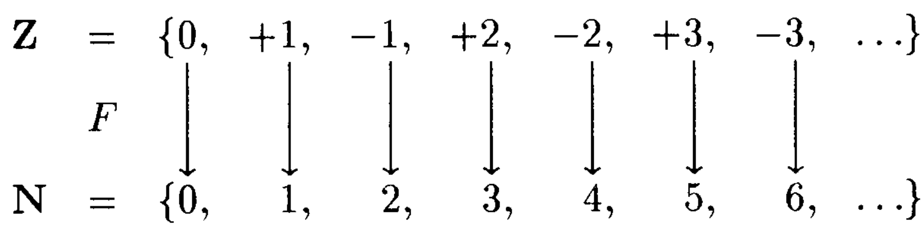
Thus, $|\mathbb{N} - \{0\}| = |\mathbb{N}| = \aleph_0$

(10) **The Integers $\mathbb{Z}$ are Countable**

Consider the function f defined below:

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ 2x-1 & \text{if } x \text{ is positive} \\ -2x & \text{if } x \text{ is negative} \end{cases}$$

Picture of f(x), from Partee et al. (1993):



a. f(x) is clearly a function from $\mathbb{Z}$ to $\mathbb{N}$
b. f(x) is an injection from $\mathbb{Z}$ to $\mathbb{N}$
- Each positive number is mapped to an odd number
- Each negative number is mapped to an even number (greater than 0)
- Only 0 is mapped to 0

c. f(x) is a surjection from $\mathbb{Z}$ to $\mathbb{N}$
- 0 is mapped to 0
- Every positive even number is equal to -2x for some negative integer
- Every positive odd number is equal to 2x-1 for some positive integer

Therefore, f(x) is a bijection, and so $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$

(Note, this is despite the fact that $\mathbb{N} \subset \mathbb{Z}$)

(11) **Demonstrating that an Infinite Set is Countable, Part 2**

Now that we know that $\mathbb{Z}$ and $\mathbb{N}-\{0\}$ are countable, we can show that S is countable by showing that there is a bijection from S to $\mathbb{Z}$ or from S to $\mathbb{N}-\{0\}$

- After all, this would entail $|S| = |\mathbb{Z}| = \aleph_0$ or $|S| = |\mathbb{N}-\{0\}| = \aleph_0$

(12) **The Positive Rationals are Countable**

Usually, the following 'intuitive' (or 'visual') proof is used to show that there is a bijection from $\{ n : n \in \mathbb{Q} \text{ and } n > 0 \}$ to $\mathbb{N}-\{0\}$

a. Step One:
We can arrange the set $\{ n : n \in \mathbb{Q} \text{ and } n > 0 \}$ into the following infinite table:

1/1	1/2	1/3	1/4	1/5	1/6	1/7	…
2/1	2/2	2/3	2/4	2/5	2/6	2/7	…
3/1	3/2	3/3	3/4	3/5	3/6	3/7	…
4/1	4/2	4/3	4/4	4/5	4/6	4/7	…
…	…	…	…	…	…	…	

b. Step Two:
Some rationals appear more than once in this table (e.g., 1/1 = 2/2). We can fix this by snaking around the grid (infinitely) in the way sketched below. Every time we hit a number that we've already passed, we cross it out.

1/1 →	1/2	1/3 →	1/4	1/5 →	1/6	1/7	…
2/1	~~2/2~~	2/3	~~2/4~~	2/5	2/6	2/7	…
3/1	3/2	~~3/3~~	3/4	3/5	3/6	3/7	…
4/1	~~4/2~~	4/3	4/4	4/5	4/6	4/7	…
5/1	5/2	5/3	5/4	5/5	5/6	5/7	…
…	…	…	…	…	…	…	

c. <u>Step Three:</u>
We take the augmented grid resulting from Step 2 (where repeated rationals are crossed out), and we snake through it again just as before, mapping the rationals in the grid to ℕ−{0} in the following way:

(i) We map 1/1 to 1
(ii) We then proceed as follows:

- Suppose that at step m in the 'snaking' we've just mapped the rational p/q to the natural number n.

- We next examine the rational r/s we come to at step (m+1).
  - If r/s is *not* crossed off in the grid, we map it to (n+1).
  - If r/s is crossed off, then we proceed to the next step in the snaking…

1/1	1/2	1/3	1/4	1/5	1/6	1/7	…
2/1	~~2/2~~	2/3	~~2/4~~	2/5	~~2/6~~	2/7	…
3/1	3/2	~~3/3~~	3/4	3/5	~~3/6~~	3/7	…
4/1	~~4/2~~	4/3	~~4/4~~	4/5	~~4/6~~	4/7	…
5/1	5/2	5/3	5/4	~~5/5~~	5/6	5/7	…
6/1	~~6/2~~	~~6/3~~	~~6/4~~	6/5	~~6/6~~	6/7	…
…	…	…	…	…	…	…	

f(1/1)	=	1	f(2/3)	=	7	
f(1/2)	=	2	f(3/2)	=	8	
f(2/1)	=	3	f(4/1)	=	9	
f(3/1)	=	4	f(5/1)	=	10	
f(1/3)	=	5	f(1/5)	=	11	
f(1/4)	=	6	f(1/6)	=	12	…

d. <u>Step Four:</u>
The function f defined above is a bijection from { n : n ∈ ℚ and n > 0 } to ℕ−{0}

(i) It is an injection:
No two rationals will end up mapped to the same number in ℕ−{0}

(ii) It is a surjection:
Since there are infinite number of positive rationals, every number in ℕ−{0} will be equal to f(x) for some rational x.

(13) **The Rationals are Countable**

- We can use the result in (12) to show that the entire set of rationals $\mathbb{Q}$ is countable.
- Consider the function h defined below (where f is the function in (12))

For all n ∈ $\mathbb{Q}$, h(n)	=	0	if n = 0
		f(n)	if n > 0
		–f(–n)	if n < 1

<u>The function h above is a bijection from $\mathbb{Q}$ to $\mathbb{Z}$</u>

a. The function h is clearly an injection
   - Because f is an injection to $\mathbb{N}$–{0} every positive rational will be mapped to a different positive integer, and every negative rational will be mapped to a different negative integer.

b. The function is clearly a surjection
   - Because f is an surjection to $\mathbb{N}$–{0} every positive integer n will be equal to h(x) (=f(x)) for some positive rational.
   - Because f is an surjection to $\mathbb{N}$–{0} every negative integer n will be equal to h(x) (= -f(-x)) for some negative rational).

Therefore, $|\mathbb{Q}| = |\mathbb{Z}| = \aleph_0$

---

2. Uncountable (Non-denumerable) Sets

So far, we've seen that $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$, even though $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

- This might lead one to wonder whether, in addition, $|\mathbb{R}| = \aleph_0$
- In this section, we'll see that this is *not* the case, $|\mathbb{R}| \neq \aleph_0$
   - That is, there are some infinities that are *uncountable (non-denumerable)*

(14) **Powersets and Cardinalities**

For every set S, | S | < | ℘(S) |

- Suppose that | S | = | ℘(S) |. There must then be a bijection f: S → ℘(S)
- Now, for any element x ∈ S, it is clear that either x ∈ f(x) or x ∉ f(x)
- Thus, we can define the set R = { x : x ∉ f(x) }
- Now, R is a subset of S, and so there must be some y ∈ S such that f(y) = R
- Finally, it must be that either y ∈ f(y) or y ∉ f(y)
   - Suppose y ∈ f(y). But then y ∉ R, and so y ∉ f(y). Contradiction.
   - Suppose y ∉ f(y). But then y ∈ R, and so y ∈ f(y). Contradiction.

(15) **Key Consequence:** $|\wp(\mathbb{N})| > |\mathbb{N}| = \aleph_0$

If a set S is such that $|S| > \aleph_0$, then we say that S is *uncountable (non-denumerable).*

(16) **Key Result: The Real Numbers Between 0 and 1 are Uncountable**

a. Key Background Fact:
Every real number between 0 and 1 can be uniquely represented as a sequence consisting of '0.', followed by an infinitely long number of decimals:

0.13456789890989999….
0.57682838494827789…

- Thus, every real number between 0 and 1 uniquely corresponds to a sequence of the form '$0.a_1a_2a_3a_4a_5a_6 \ldots$ ', where each a_i is a decimal numer.

b. The Proof;

- Suppose that $|\{ n : n \in \mathbb{R} \text{ and } 0 < n < 1 \}| = |\mathbb{N}|$. Then there is a bijection f from $\{ n : n \in \mathbb{R} \text{ and } 0 < n < 1 \}$ to $\mathbb{N}$.

- Given this bijection f, it is possible to write an (infinitely long) list of all the members of $\{ n : n \in \mathbb{R} \text{ and } 0 < n < 1 \}$. Given the key background fact in (16a), this list will look as follows, where a_{nm} is the m^{th} decimal in the nth real number in the ordering:

1	$0.\ a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15} \ldots$
2	$0.\ a_{21}\ a_{22}\ a_{23}\ a_{24}\ a_{25} \ldots$
3	$0.\ a_{31}\ a_{32}\ a_{33}\ a_{34}\ a_{35} \ldots$
4	$0.\ a_{41}\ a_{42}\ a_{43}\ a_{44}\ a_{45} \ldots$
…	

- Now, we can use this list to define a real number *r* between 0 and 1 that is *not* on this list:
  - The integer component of *r* is 0
  - The first decimal in *r* after 0 is different from a_{11}
  - The second decimal in *r* after 0 is different from a_{22}
  - The third decimal in *r* after 0 is different from a_{33}
  - (and so on…)

- The real number *r* is guaranteed not to appear anywhere on this list.
  - After all, for any natural number n, *r* will differ from f(n) in the n^{th} decimal after 0.

- Therefore, this list *doesn't* contain all the real numbers between 0 and 1. Consequently, there is no bijection from $\{ n : n \in \mathbb{R} \text{ and } 0 < n < 1 \}$ to $\mathbb{N}$.

  Thus, $|\{ n : n \in \mathbb{R} \text{ and } 0 < n < 1 \}| \neq |\mathbb{N}|$. Thus, $|\mathbb{R}| > |\mathbb{N}| = \aleph_0$

(17) **Additional Transfinite Cardinals**

- For various reasons, it will be helpful to have a name for $|\wp(\mathbb{N})|$:

$$2^{\aleph_0}$$

'the cardinality of $\wp(\mathbb{N})$'

- It is known that $|\mathbb{R}| = |\wp(\mathbb{N})|$

---

3. Proof by Mathematical Induction

(18) **Key Axiom of Number Theory**

Suppose that for some property *P*, we can show (i) and (ii):
(i) 0 has property *P*
(ii) For any $n \in \mathbb{N}$, if n has property *P*, then (n+1) has property *P*.
Then we can conclude that *every* $n \in \mathbb{N}$ has property *P*

(19) **Key Consequence of (18)**

Suppose that for some property *P*, we can show (i) and (ii):
(i) 0 has property *P*
(ii) For any $n \in \mathbb{N}$, if *every* number $m < n$ has property *P*, then n has *P*
Then we can conclude that *every* $n \in \mathbb{N}$ has property *P*

(20) **Some Terminology**

a. An argument making use of the axiom in (18) is typically referred to as a *proof by (weak) induction*

b. An argument making use of the consequence in (19) is typically referred to as *proof by strong induction.*

c. In a proof by (weak/strong) induction,

(i) Proving that 0 has property *P* is called the 'base step' ('base case')
(ii) Proving either (18ii) or (19ii) is called the 'induction step'.

Note: If the base case is some numeral $n > 0$, then a proof by induction demonstrates that *P* holds for all m such that $n \leq m$

(21) **Key Application**
If S is a countable set – that is, if there is a bijection f: $\mathbb{N} \rightarrow S$ – then we can use proofs by induction to prove things about S!

(22) **Illustration: Generalized Distributive Law**

Claim:
For all $n \in \mathbb{N}$ such that $2 \leq n$, $A \cup (B_1 \cap \ldots \cap B_n) = (A \cup B_1) \cap \ldots \cap (A \cup B_n)$

Proof by Induction:

a. *Base Step: n = 2*
$A \cup (B_1 \cap B_2) = (A \cup B_1) \cap (A \cup B_2)$

This follows from the simple set-theoretic equivalences proven in Chapter 1 of Partee *et al.* (1993).

b. *Induction Step*
Let $n \in \mathbb{N}$ be such that: $A \cup (B_1 \cap \ldots \cap B_n) = (A \cup B_1) \cap \ldots \cap (A \cup B_n)$

- By the associativity of intersection:
  $A \cup (B_1 \cap \ldots \cap B_n \cap B_{n+1}) \quad = \quad A \cup ((B_1 \cap \ldots \cap B_n) \cap B_{n+1})$

- Next, by the base step in (22a):
  $A \cup ((B_1 \cap \ldots \cap B_n) \cap B_{n+1}) = (A \cup (B_1 \cap \ldots \cap B_n)) \cap (A \cup B_{n+1})$

- Next, by the induction assumption for n:
  $(A \cup (B_1 \cap \ldots \cap B_n)) \cap (A \cup B_{n+1}) =$
  $((A \cup B_1) \cap \ldots \cap (A \cup B_n)) \cap (A \cup B_{n+1})$

- Finally, by the associativity of intersection again:
  $((A \cup B_1) \cap \ldots \cap (A \cup B_n)) \cap (A \cup B_{n+1}) =$
  $(A \cup B_1) \cap \ldots \cap (A \cup B_n) \cap (A \cup B_{n+1})$

- **Thus, $A \cup (B_1 \cap \ldots \cap B_n \cap B_{n+1}) =$**
  $(A \cup B_1) \cap \ldots \cap (A \cup B_n) \cap (A \cup B_{n+1})$

Therefore, by (weak) induction, it follows that for all $n \in \mathbb{N}$ such that $2 \leq n$:
$A \cup (B_1 \cap \ldots \cap B_n) = (A \cup B_1) \cap \ldots \cap (A \cup B_n)$

(23) **Illustration of Strong Induction: Well Ordering Principle**

Claim: If $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then there is an $a \in S$ such that for all $s \in S$, $a \leq s$.

Proof by Strong Induction:

- Suppose that there is an $S \subseteq \mathbb{N}$ and $S \neq \emptyset$. For a contradiction, suppose that there is *no* $a \in S$ such that for all $s \in S$, $a \leq s$.

- By strong induction, we'll show that for all $n \in \mathbb{N}$, $n \notin S$, and so $S = \emptyset$, contrary to assumption.

a. *Base Step: n = 0*
Clearly, $0 \notin S$. (After all, for all $s \in S$, $0 \leq s$)

b. *Induction Step*
Let $n \in \mathbb{N}$ be such that for all $m < n$, $m \notin S$. We will show that $n \notin S$.

  - Suppose that $s \in S$. Now, clearly $(n-1) < s$. (After all, if $s \leq (n-1)$, then $s < n$, and so by the induction assumption $s \notin S$, contrary to assumption.)

  - Next, since $(n-1) < s$, it follows that $n \leq s$. Since s was arbitrary, it follows that for all $s \in S$, $n \leq s$.

  - **Consequently, $n \notin S$** (After all, by assumption there is no $a \in S$ such that for all $s \in S$, $a \leq s$.)

- **Thus, by strong induction, for all $n \in \mathbb{N}$, $n \notin S$, and so $S = \emptyset$, contrary to assumption.**

- **Therefore, for any $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, there is $a \in S$ such that for all $s \in S$, $a \leq s$.**