Mathematical Logic I

Cardinality and the Uncountable

Johns Hopkins University, Fall 2019

The Concept of Cardinality

The idea of the **cardinality** of a set A amounts to being able to answer the question: how many members does A have?

The answer presupposes that there are **cardinal numbers**. For finite sets, this is not particularly problematic. We can use natural numbers. For larger sets it takes some finesse.

The answer also presupposes that we can make **cardinality comparisons**: do two sets have the same number of members or does one set have more than the other?

Cardinality comparisons can be defined even in the absence of cardinal numbers. They are a matter of whether certain **mappings** exist from one set to another.

Functions and Their Inverses

Mappings involve functions. So, recall that a **function** f is a relation such that for every $x \in \text{dom } f$ there exists a unique y s.t. $(x, y) \in f$ and this unique y is denoted '$f(x)$'.

Every function f has an inverse f^{-1}, *viz*.

$$f^{-1} = \{(y, x) \mid (x, y) \in f\},$$

which, although a relation to be sure, need not itself be a function.

Def 1.4.1. A function f is said to be **one-to-one (1-1)** iff f^{-1} is also a function, or, equivalently, for all $x_1, x_2 \in \text{dom } f$,

$$\text{if } f(x_1) = f(x_2), \text{ then } x_1 = x_2.$$

The notion of a 1-1 function is crucial for making cardinality comparisons.

Mappings

Def 1.4.2. f **maps** A to B iff (i) f is a function s.t. (ii) $A = \text{dom } f$ and (iii) $\text{ran } f \subseteq B$.

B is called the **codomain** of the mapping.

The notation '$f : A \to B$' means either

- 'f maps A to B', or, more commonly,
- 'the mapping f from A to B'.

Def 1.4.3.: If f is 1-1, then $f : A \to B$ is said to be an **injection**, or, simply, **1-1**.

Def 1.4.4. If $\text{ran } f = B$, then $f : A \to B$ is said to be a **surjection**, or, simply, **onto**.

If $f : A \to B$ is both injective and surjective, then $f : A \to B$ is said to be a **bijection**, or, a **1-1 correspondence** from A to B.

Mappings (cont.)

Recall that, for relations R and S,

$$S \circ R = \{(x, z) \mid \text{there exists a } y \text{ s.t. } (x, y) \in R \text{ and } (y, z) \in S\}.$$

Since functions are relations, we can use the same definition for the composition of functions, and hence the composition of mappings.

However, here is a more perspicuous definition:

Def 1.4.5. Suppose that $f : A \to B$ and $g : B \to C$. Then the **composition** of g with f is the mapping $g \circ f : A \to C$ s.t., for any $x \in A$, $(g \circ f)(x) = g(f(x))$.

Cardinality Comparisons

A cardinality comparison of one set with another involves the existence of certain mappings from the one set to the other.

Def 1.4.6. A **is equinumerous with** B, written $A \sim B$, iff there is a bijection $f : A \to B$.

Alternative terminology: A is **equipotent** with, **equipollent** with, or **similar** to B.

Example. $\{\text{Moe}, \text{Curly}, \text{Larry}\} \sim \{0, 1, 2\}$.

Sample bijection: $f(\text{Curly}) = 2$, $f(\text{Moe}) = 0$, $f(\text{Larry}) = 1$.

Cardinality Comparisons (cont.)

Def 1.4.7. A **is no more numerous than** B, written $A \preceq B$, iff there exists an injection $f : A \to B$.

An equivalent definition is that A is equinumerous with some subset of B.

Def 1.4.8. A **is less numerous than** B, written $A \prec B$, iff $A \preceq B$ but $B \not\preceq A$.

Example. $\{\text{Bonnie}, \text{Clyde}\} \preceq \{0, 1, 2\}$.

Sample injection: $f(\text{Bonnie}) = 0$, $f(\text{Clyde}) = 2$.

But $\{0, 1, 2\} \not\preceq \{\text{Bonnie}, \text{Clyde}\}$. No surjection is 1-1.

Hence $\{\text{Bonnie}, \text{Clyde}\} \prec \{0, 1, 2\}$.

Basic Properties of $\sim$

Lemma 1.4.1. For any sets A, B, and C,

1. $A \sim A$.
2. If $A \sim B$, then $B \sim A$.
3. If $A \sim B$ and $B \sim C$, then $A \sim C$.

Proof Sketch:

For (1), use the identity map $id_A : A \to A$.

For (2), show that the inverse of a bijection is a bijection.

For (3), show that the composition of bijections is a bijection.

Basic Properties of $\sim$ (cont.)

Scholium.

So $\sim$ behaves formally like an equivalence relation.

Only $\sim$ is not really a relation on a set because (i) there is no set of all sets, and (ii) $\sim$ is not a SET of ordered pairs, and hence not a RELATION, but a PROPER CLASS of ordered pairs.

However, equinumerosity does partition V, the class of all sets, into equivalence classes, which also are not sets, but proper classes.

To illustrate, recall that $V = \{x \mid x \text{ is a set}\}$. If $\sim$ were a set, then (dom $\sim$) would be a set, and hence so would V, since

$$(\text{dom } \sim) = \{x \mid x \in V\}.$$

Basic Properties of $\preceq$

Lemma 1.4.2. For any sets A, B, and C,

1. $A \preceq A$
2. If $A \preceq B$ and $B \preceq C$, then $A \preceq C$.
3. If $A \preceq B$ and $B \preceq A$, then $A \sim B$.

Proof Comments: The proofs of (1) and (2) are rather immediate. For (1), the identity map $id_A : A \to A$ again suffices, and for (2), it suffices to show that the composition of injections is an injection.

Part (3), however, is highly non-trivial, and is known in the literature as the **Schröder-Bernstein Theorem**. One is given the existence of two injections, $f : A \to B$ and $g : B \to A$, neither of which can be assumed to be surjective, and then one must somehow construct a bijection $h : A \to B$.

Are All Sets Comparable in Cardinality?

Scholium: The preceding lemma suggests that $\preceq$ behaves like a partial ordering if one thinks of $\sim$ as replacing identity. So, without begging too much confusion, it says that V, the class of all sets, is partially ordered in cardinality (numerosity). This motivates the following question:

Query: Does it also follow that, for any sets A and B, $A \preceq B$ or $B \preceq A$, i.e., are any two sets comparable in cardinality (numerosity)?

It would seem strange if there were sets A and B without the same number of members, but neither of which has *more* members than the other.

Answer: No, not unless one assumes the axiom of choice (**AC**), which is equivalent to the proposition that all sets can be well-ordered.

(This, then, is strong motivation for adopting **AC**. That **AC** is non-trivial is evident from the following challenge: construct a well-ordering of $\mathcal{P}(\mathbb{N})$ with assuming **AC**.)

Finite, Infinite, and Uncountable Sets

Def 1.4.9. A set A is **finite** iff $A \sim n$ for some $n \in \mathbb{N}$, in which case it is said to have n members.

Otherwise, A is **infinite**.

Def 1.4.10. A is **countable** iff $A \preceq \mathbb{N}$.

Otherwise, A is **uncountable**.

N.B. Two important points deserve emphasis here:

1. One needs to distinguish between infinity in **number** and infinity in **magnitude** (for example, infinite distance, or infinite mass).
2. As for infinity in number, if there are uncountable sets, then some infinities in number are greater than others.

Countably Infinite Sets

Are there any uncountable sets?

To try to answer this, let us start going through our methods of constructing sets from other sets and see if, when applied to countably infinity sets, they do or do not yield a set that is countably infinite...

Lemma 1.4.3. The union of countable sets is countable.

The proof is left as an exercise.

Corollary. The set $\mathbb{Z}$ of integers is countable. [Defn. of $\mathbb{Z}$? Next slide.]

Proof. $\mathbb{Z}$ is the union of two sets, the set of all non-zero integers $\{0, 1, 2, \ldots\}$ and the set of all negative integers $\{-1, -2, -3, \ldots\}$. The enumerations given suggest how to show that each is countable.

Lemma 1.4.4. Any finite union of countable sets is countable.

Proof Hint: Use Lemma 1.4.3 and argue by mathematical induction on the number of unions.

Construction of $\mathbb{Z}$ from $\mathbb{N}$

Def. Recursive definition of addition on $\mathbb{N}$:

$$\begin{aligned} n + 0 &= n \\ n + S(m) &= S(n + m) \end{aligned}$$

Let $m, n, p, q \in \mathbb{N}$.

Def. $(m, n) \equiv_Z (p, q)$ iff $m + q = p + n$.

Example: $(2, 5) \equiv_Z (9, 12)$.

Def. $\mathbb{Z} =_{df} (\mathbb{N} \times \mathbb{N}) / \equiv_Z$.

Example: $-3 = [(0, 3)]_{\equiv_Z}$.

Def. $[(m, n)]_{\equiv_Z} + [(p, q)]_{\equiv_Z} = [(m + p, n + q)]_{\equiv_Z}$.

Countably Infinite Sets (cont.)

Lemma 1.4.5. The Cartesian product of countable sets is countable.

Proof. It suffices to show that $\mathbb{N} \times \mathbb{N} \preceq \mathbb{N}$. Consider the mapping $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by

$$f(n, m) = 2^{n+1} \cdot 3^{m+1}.$$

Since each natural number greater than 2 has a unique prime decomposition, f is 1-1. ■

Corollary. The set $\mathbb{Q}$ of rational numbers is countable.

Proof. By the lemma and the corollary to Lemma 1.4.3, $\mathbb{Z} \times \mathbb{Z}$ is countable. Each rational number has a unique representation as the ratio of two integers p/q with no common divisors. The mapping $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ given by $f(p/q) = (p, q)$ is obviously 1-1. So, $\mathbb{Q} \preceq \mathbb{Z} \times \mathbb{Z} \preceq \mathbb{N}$. ■

The Set of All Finite Sequences on a Countable Set

A case of considerable importance for studying languages is the set of finite sequences over a countable vocabulary.

This is formally the same as determining the cardinality of the set of n-tuples, for arbitrary n, of elements from a countable set.

Lemma 1.4.6. If A is countable, then

$$A^{<\omega} =_{df} \{\langle x_1, \ldots, x_i, \ldots, x_n\rangle \mid n \in \mathbb{N} \text{ and } x_i \in A \text{ for all } i \text{ s.t. } 1 \leq i \leq n\}$$

is countable.

The proof is left as an exercise.

The Set of All Infinite Sequences of 0's and 1's

Lemma 1.4.7. The set of all infinite sequences of 0s and 1s is uncountable.

Proof. Call this set $\mathcal{S}$. What we want to show is that $\mathcal{S} \not\preceq \mathbb{N}$.

We argue by *reductio ad absurdum*, i.e., by assuming, contrary to what we want to show, that $\mathcal{S} \preceq \mathbb{N}$ and then deriving a contradiction.

So let's assume that $\mathcal{S} \preceq \mathbb{N}$.

Since obviously $\mathbb{N} \preceq \mathcal{S}$, this is equivalent, by the Schröder-Bernstein theorem, to assuming that $\mathbb{N} \sim \mathcal{S}$; in other words, that there exists a bijection $s : \mathbb{N} \to \mathcal{S}$.

An Uncountable Set (cont.)

We choose 's' as a pneumonic aid. For, if we write s_n for $s(n)$, then the sequence $s_0, s_1, \ldots$ allegedly enumerates all the members of $\mathcal{S}$.

Now list this infinite sequence of 0s and 1s running down the page. It will look something like this:

$$\begin{array}{lcccccc}
s_0: & 1 & 0 & 0 & 1 & 0 & \cdots \\
s_1: & 1 & 1 & 1 & 1 & 0 & \cdots \\
s_2: & 0 & 0 & 0 & 1 & 1 & \cdots \\
s_3: & 0 & 1 & 0 & 0 & 1 & \cdots \\
s_4: & 0 & 0 & 1 & 0 & 1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

Now scan down the diagonal of this infinite matrix starting from the upper left and running toward the lower right.

An Uncountable Set (cont.)

There you see the sequence beginning:

$$1 \quad 1 \quad 0 \quad 0 \quad 1 \quad \cdots$$

If you "flip" each member of the sequence by replacing 1s with 0s and 0s with 1s, then you get the sequence beginning:

$$0 \quad 0 \quad 1 \quad 1 \quad 0 \quad \cdots$$

This sequence cannot be any of the sequences listed going down. For it must disagree with each on the diagonal. Therefore, there is an infinite sequence of 0's and 1's that has been left off the list, contrary to the assumption that we had listed all of them.

N.B. See the supplemental slides for a rigorous formulation.

Corollary. $\mathcal{P}(\mathbb{N})$ is uncountable.

The proof is left as an exercise.

More Uncountable Sets

A similar kind of 'diagonalization' argument establishes the following:

Lem 1.4.8. The open set $\mathbb{R}(0, 1)$ of real numbers between 0 and 1 is uncountable.

Corollary. The set $\mathbb{R}$ of all real numbers is uncountable.

Lem 1.4.9. $\mathbb{R} \sim \mathbb{R}(0, 1)$.

The proof is left as an exercise.

Cantor's Theorem

Figure: Georg Cantor (1845–1918)

Cantor's Theorem

We have seen that $\mathbb{N} \prec \mathcal{P}(\mathbb{N})$. Here is a more general result:

Theorem 1.4.1. For any set X, $X \prec \mathcal{P}(X)$.

Proof. That $X \preceq \mathcal{P}(X)$ is pretty obvious: just map each $a \in X$ to $\{a\}$.

Slightly harder is to show that $\mathcal{P}(X) \npreceq X$. We argue again by *reductio ad absurdum*.

Suppose that $\mathcal{P}(X) \preceq X$. Then by the Schröder-Bernstein Theorem, $X \sim \mathcal{P}(X)$, and hence, there is a bijection $f : X \to \mathcal{P}(X)$. We show this is impossible. Let

$$Y =_{df} \{a \in X \mid a \notin f(a)\}.$$

Since $Y \in \mathcal{P}(X)$ and f by hypothesis is surjective, there exists a $b \in X$ s.t. $Y = f(b)$. Now ask whether or not $b \in Y$.

Cantor's Theorem (cont.)

For sake of reference, we redisplay the set Y.

$$Y =_{df} \{a \in X \mid a \notin f(a)\}.$$

Suppose that $b \in Y$. Then, by the definition of Y, $b \notin f(b)$.

But, by hypothesis, $f(b) = Y$. So, it follows that $b \notin Y$.

Alternatively, suppose that $b \notin Y$. Then, by the definition of Y, $b \in f(b)$.

But, again, since by hypothesis $f(b) = Y$, it follows that $b \in Y$.

So, $b \in Y$ iff $b \notin Y$, which is a classical inconsistency. ■

Endlessly Large Cardinalities

Since for *any* set X, $X \prec \mathcal{P}(X)$, we can continue to iterate the power set operator on $\mathbb{N}$:

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \cdots .$$

Let

$$\begin{aligned} \mathcal{P}^0(X) &=_{df} X \\ \mathcal{P}^{n+1}(X) &=_{df} \mathcal{P}(\mathcal{P}^n(X)). \end{aligned}$$

Then, if $\{\mathcal{P}^n(\mathbb{N}) \mid n \in \mathbb{N}\}$ is a set,

$$\bigcup \{\mathcal{P}^n(\mathbb{N}) \mid n \in \mathbb{N}\}$$

gives us an even bigger set. Cantor was so smart, he showed that for any uncountable cardinality, we can get that many more even larger cardinalities. David Hilbert referred to this as *Cantor's Paradise*.

Figure: David Hilbert (1862-1943)

The Power of the Continuum

So, we have seen that $\mathbb{N}$ is the smallest infinite set in cardinality.

And we have seen that $\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \sim \mathbb{R}$.

Is there a set A such that $\mathbb{N} \prec A \prec \mathbb{R}$? Cantor couldn't find one, so he conjectured:

Cantor's Continuum Hypothesis (CH). There is no set A such that $\mathbb{N} \prec A \prec \mathbb{R}$.

But Cantor could not prove **CH**. Nor could Gödel. Nor could Gödel prove $\neg$**CH**.

But Gödel could show

- if **Z** is consistent, then **Z + AC** is consistent,
- and if **Z + AC** is consistent, then **Z + AC + CH** is consistent.

Figure: Kurt Gödel (1906-1978)

The Status of **CH**

- It seems, once all the definitions are given, there ought to be a brute fact of the matter as to whether or not there is an uncountable subset of the reals strictly smaller in cardinality than the reals.
- Paul Cohen (1963): If **Z** + **AC** is consistent, then **Z** + **AC** + ¬**CH** is consistent. I.e., **CH** is independent of **Z** + **AC**.
- Not only is **CH** independent, it is WILDLY independent: there could be one, five, a dozen, infinitely many, even uncountably many sets of intermediate cardinality.
- Attitudes:
    - *Platonism*: There really is a fact of the matter. We just need to discover more axioms.
    - *Conventionalism*: It's like the parallel postulate in metric geometry.
    - *Fictionalism*: It's all a game, anyway.
    - *Your View Here*: ...

Figure: Paul Cohen (1934-2007)

The Consistency of Set Theory Redux

- Russell showed that naive set theory is inconsistent.
- As we asked awhile ago, is **Z** consistent?
- Gödel (1931): Arithmetic cannot be shown to be consistent unless more than arithmetic is assumed (e.g., the existence of an infinite set). Moreover, this holds for any stronger mathematical system. (More on this much later in the course . . .)
- **Z** is a stronger mathematical system. (We showed how to construct all the natural numbers, and could show how to add them, multiply them and so on.)
- **Z** can be shown to be consistent if one postulates in addition there are certain very large cardinalities, called *inaccessible cardinals*.

The Consistency of Set Theory (cont.)

- Is **Z** + 'There exist inaccessible cardinals' consistent?
- It cannot be shown that if **Z** is consistent, then **Z** + 'There exist inaccessible cardinals' is consistent.
- By Gödel's theorem, the latter could be shown only by ascending to an even stronger system, adding greater risk of inconsistency.
- And this can be shown to be consistent only by moving to a yet stronger system, and so on.
- So, <u>*is*</u> **Z** consistent?

Supplementary Material

A Countable Union of Countable Sets

Lemma. Assuming **AC**, a countable union of countable sets is countable.

Proof. This is much the same as showing that $\mathbb{N} \times \mathbb{N}$ is countable, only **AC** must be used to select a bijection for each of the countable sets entering into the union. Let's suppose it's an infinite union, else it degenerates to the case of a finite union of countable sets. So, it has the form

$$\bigcup_{n \in \mathbb{N}} A_n.$$

Using **AC**, we select for each $n \in \mathbb{N}$ an injection $f_n : A_n \to \mathbb{N}$. Then for each $x \in A_n$, $(f_n(x), n)$ is an ordered pair of natural numbers. Considering all n, we have a subset of $\mathbb{N} \times \mathbb{N}$, and thus a countable set. ■

Formal Proof of Lemma 1.4.7

More formally, the argument goes like this.

Each infinite sequence s_j of 0s and 1s is itself really a mapping $s_j : \mathbb{N} \to \{0, 1\}$ telling us whether we get a 0 or a 1 in the kth place.

So, in general, let $\delta_{jk} = s_j(k)$. Then we get the fancier picture:

	0	1	2	$\cdots$	n	$\cdots$
s_0	δ_{00}	δ_{01}	δ_{02}	$\cdots$	δ_{0n}	$\cdots$
s_1	δ_{10}	δ_{11}	δ_{12}	$\cdots$	δ_{1n}	$\cdots$
s_2	δ_{20}	δ_{21}	δ_{22}	$\cdots$	δ_{2n}	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
s_n	δ_{n0}	δ_{n1}	δ_{n2}	$\cdots$	δ_{nn}	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Formal Proof of Lemma 1.4.7 (cont.)

The diagonal is the sequence consisting of δ's which have equal indices, i.e., $\delta_{00}, \delta_{11}, \delta_{22}, \ldots, \delta_{nn}, \ldots$.

We now define a sequence, call it s^*, as follows. For all $n \in \mathbb{N}$,

$$s^*(n) = \begin{cases} 1 & \text{if } \delta_{nn} = 0 \\ 0 & \text{if } \delta_{nn} = 1. \end{cases}$$

The claim is that s^* cannot be any of the rows going across, i.e., that $s^* \neq s_n$ for any $n \in \mathbb{N}$.

For suppose otherwise, i.e., that for some $n \in \mathbb{N}$, $s^* = s_n$.

Then, for each $k \in \mathbb{N}$ we must have $s^*(k) = s_n(k)$.

Formal Proof of Lemma 1.4.7 (cont.)

This must hold for n in particular. But, since $s_n(n) = \delta_{nn}$, we have

$$s^*(n) = \begin{cases} 1 & \text{if } s_n(n) = 0 \\ 0 & \text{if } s_n(n) = 1. \end{cases}$$

Thus, $s^* \neq s_n$ for any $n \in \mathbb{N}$.

Recall that for each $n \in \mathbb{N}$, $s_n = s(n)$, where $s : \mathbb{N} \to \mathcal{S}$.

Thus, s cannot be surjective, and hence $\mathbb{N} \not\sim \mathcal{S}$. Thus $\mathcal{S} \not\preceq \mathbb{N}$, i.e., $\mathcal{S}$ is uncountable. ■