Logic, Computability and Incompleteness

Cardinality, Enumerability, Diagonalization

Cardinality

- The **cardinality** of a set is a measure of its ‘size’ in terms of numbers of elements. For example, the set $\Gamma = \{0,1,2\}$ contains 3 elements, and therefore Γ has a cardinality of 3.
- Two sets have the same cardinality iff they are ‘equinumeros’.
- Equinumerosity is defined in terms of a 1-1 correspondence between two sets, where a 1-1 correspondence is in turn defined in terms of certain types of ‘mappings’ or **functions**.
- In brief, a function is an assignment of *values* to *arguments*, where the domain of the function is the set to which its arguments or ‘inputs’ belong, and the range of the function is the set to which its values or ‘outputs’ belong.

Cardinality

- A function f with the set Γ as domain and the set Δ as range, written $f: \Gamma \bullet\!\!\rightarrow \Delta$, is a **bijection** (also called a 1-1 correspondence between Γ and Δ) iff

(1) $\forall x,z \in \Gamma$, if $x \neq z$, then $f(x) \neq f(z)$ (i.e. f is 1-1, or *injective*),

and

(2) $\forall y \in \Delta, \exists x \in \Gamma$: $y = f(x)$ (i.e. f is *onto* or *surjective*).

- Two sets Δ and Γ have the **same cardinality** iff there exists a bijection $f: \Gamma \bullet\!\!\rightarrow \Delta$.
- The **cardinal number** of Γ will be written as $|\,\Gamma\,|$.
- If Γ and Δ have the same cardinality, then $|\,\Gamma\,| = |\,\Delta\,|$.

$\subset$

Cardinality

- Γ has **greater cardinality** than Δ, written $|\,\Gamma\,| > |\,\Delta\,|$, iff

  (i) there is no bijection $g : \Delta \bullet\!\!\rightarrow \Gamma$ <u>and</u>

  (ii) for some <u>proper</u> subset $\Sigma \subset \Gamma$, there **is** a bijection $f : \Sigma \bullet\!\!\rightarrow \Delta$
- All sets have either <u>finite</u> or <u>infinite</u> cardinality.

  A simple characteristic which distinguishes the two is that a set Γ is **infinite** iff there exits a bijection $f : \Gamma \bullet\!\!\rightarrow \Sigma$ for some proper subset $\Sigma \subset \Gamma$.
- For example, the set **N** of natural numbers (= {0,1,2,3,…}) is **infinite**, since the set of squares of natural numbers is a proper subset of **N**, and the function $f(x) = x^2$ is a bijection between **N** and the set of squares of natural numbers.

Cardinality

- The smallest infinite cardinality is that of the natural numbers. Any set with this cardinality is called **denumerable**, and has cardinal number $\aleph_0$. A **countable** set is defined as either finite or denumerable and an **uncountable** set is neither.
- The **power set** of Γ, written $\mathscr{P}(\Gamma)$, is defined as the set of all subsets of Γ.
- Π is a subset of Γ, written $\Pi \subseteq \Gamma$, iff $\forall x(x \in \Pi \rightarrow x \in \Gamma)$.
- By failure of the antecedent condition in this definition, the empty set $\varnothing$ is a subset of every set,

  and obviously every set Γ is a subset of itself.

Cardinality

- Thus $\varnothing$ and Γ form the two endpoints of the spectrum for membership in $\mathscr{P}(\Gamma)$, and all other members of the power set fall between these two extremes.
- As a simple example, let $\Gamma = \{0,1,2\}$.
- Then $\mathscr{P}(\Gamma) = \boldsymbol{\{}\varnothing,\{0\},\{1\},\{2\},\{0,1\},\{0,2\},\{1,2\},\{0,1,2\}\boldsymbol{\}}$
- **Cantor's Theorem (**1891)**:** The power set of any set always has greater cardinality than the set itself. A brief proof of this theorem will be given in the section on diagonalization.
- If it is assumed that there is an infinite set, and that the power set of a set always exists, then an infinite hierarchy of ever increasing cardinality is induced.

Cardinality

- Power set cardinality is governed by the general equation that for any set Γ:

$$|\mathscr{P}(\Gamma)| = 2^{|\Gamma|}$$

This relation is easy to verify for finite sets.

- Cantor's Theorem, in combination with the fact that **N** is denumerable, immediately yields the result that

$$\mathscr{P}(\mathbf{N}) \text{ is } \underline{\text{uncountable}}$$

this will also be proved (independently) in the section on diagonalization.

- The present section will end by mentioning a few related mathematical facts and conjectures.

Cardinality

- Even though the natural numbers **N** are not dense, while the rational numbers **Q** are, the set of rational numbers **Q** is still denumerable. Thus |**Q**| = $\aleph_0$
- However, the set $\mathscr{R}$ of real numbers is uncountable, and furthermore it is provable that $|\mathscr{R}| = |\mathscr{P}(\mathbf{N})|$.
- The above relation, in combination with the exponential equation governing power set cardinality, yields the result that $|\mathscr{R}| = 2^{\aleph_0}$
- **Cantor's Continuum Hypothesis** (1878): there is no cardinal number greater than $\aleph_0$ and less than $2^{\aleph_0}$. If this conjecture is true, then there is no 'missing' level of infinity between | **N** | and $|\mathscr{P}(\mathbf{N})|$.

Cardinality

- Establishing the truth or falsity of the Continuum Hypothesis (CH) is the first of Hilbert's 23 outstanding problems for 20^{th} century mathematics.
- In 1938 Kurt Gödel proved that CH is consistent with the axioms of standard (ZFC) set theory

  and in 1963 Paul Cohen proved that the *negation* of CH is also consistent with ZFC.
- Hence CH is **logically independent** of standard set theory:

  it cannot be proved or disproved on the basis of these axioms.

Enumerability

- Intuitively, an enumerable set is one whose members can all be ‘arranged’ in a single list.
- Clearly every finite set is enumerable.
- For infinite sets, an acceptable list must be such that each item eventually appears as the *n*th entry, for some finite *n*.
- Thus for the set **P** of positive integers (= **N** – {0}),

  1,2,3,4,5, … is an acceptable list, while

  1,3,5, …, 2,4,6, … is *not*

  because in the latter case, it takes infinitely many entries to get to the first even number.

Enumerability

- In more precise terms, an enumeration of a set Γ is equivalent to an *onto* function $f : \mathbf{P} \bullet\!\!\rightarrow \Gamma$. The function f must be *onto* so that every member of Γ appears at least once in the list.
- It is not required that f be 1-1, and hence an enumeration can be **redundant** (since if f is not 1-1, then at least one item $b \in \Gamma$ will occur at least twice on the list).
- In principle this is not a problem, because redundancies can be systematically eliminated by reviewing the (finitely many) entries preceding any given item on the list and deleting it if it has already appeared.

Enumerability

- It is also permissible to have ***gaps*** in the list, since in principle it is always possible to close these gaps.
- A gap in the list means that f is <u>undefined</u> on the respective argument $n \in \mathbf{P}$, in which case f is a *partial function* on **P**.
- For example, the set **E** of even positive integers is very naturally enumerated by the function
- h: $\mathbf{P} \bullet\!\!\rightarrow \mathbf{E}$ such that $h(n) = 2n$,

  which defines the non-gappy list 2,4,6,8, …
- However, **E** is also enumerated by the partial function j

  such that $j(n) = n$, if n is even, and undefined otherwise.
- The function j defines the gappy list -,2,- ,4,-,6,-,8, …

Enumerability

- The positive rational numbers can be enumerated through use of a 2-dimensional array, with (+)integer numerators comprising one axis and (+)integer denominators the other.
- A path through this array can be defined by taking all fractions whose numerators and denominators sum to 2, then 3,

  then 4, …,

  listing the fractions in order of lowest numerator.

  There will be $k - 1$ entries for each sum k. This gives the (redundant) list 1/1, 1/2, 2/1, 1/3, 2/2, 3/1, 1/4, 2/3, …
- Since every positive rational will appear at least once on this list, it follows that the set of positive rationals is <u>d</u>enumerable.

Enumerability

- The enumerability of a set is simply a result of its cardinality. Any countable set Γ is necessarily enumerable (and vice versa), because to be enumerable is just to be the range of an onto function of positive integers.
- So *if* Γ is countable, then it follows that there must be a bijection between Γ and some subset of **P**, and this bijection is sufficient to serve as an enumeration.
- Similarly, if Γ is uncountable, then it *cannot* be enumerable, because any attempted list would have to omit (an uncountable infinity of) elements of Γ.

Enumerability

- An enumeration is <u>effective</u> iff the enumerated set is finite, or else there is an explicit, ‘mechanical’ procedure for determining the value $f(n) \in \Gamma$ in a finite number of steps, for every $n \in \mathbf{P}$.
- It is important to make <u>two</u> immediate points about effective enumerability:
- (i) it is a claim about the *abstract existence* of a mechanical procedure, and as such carries no <u>epistemological</u> baggage; a set may be effectively enumerable, even though no human being ever knows of an effective procedure for enumerating it

Enumerability

- (ii) it makes no claim about the practicability of the procedure, which means that it may not be humanly possible, due to various resource limitations, to actually compute the value $f(n)$ for even a single n.
- The only requirement for the enumeration to be effective is that it will yield the correct output value after a finite number of steps.
- Thus a procedure could be effective even though no computation took less than, say, 10^{50} steps.

Enumerability

- This definition of *effective* may seem overly idealized, but it is the natural limiting case mathematically, and the fact that is so strong in principle will lend significant conceptual bite to the negative results.
- Not all enumerable sets are effectively enumerable, even under this very idealized notion of what it is to be effective.
- Thus **effective enumerability** is *not* just the result of brute cardinality.

Diagonalization

- In this section, Cantor's elegant and versatile **diagonal method** will be employed, first in a *specific* instance to show that $\mathscr{P}(\mathbf{P})$ is uncountable, and then in the *general* case to prove that the cardinality of the power set is always greater than that of the original set.
- **Proof** that $|\,\mathscr{P}(\mathbf{P})\,| > |\,\mathbf{P}\,|$:

$\mathscr{P}(\mathbf{P})$ is by definition the set of all subsets of $\mathbf{P}$.

If $\mathscr{P}(\mathbf{P})$ were enumerable, then there would exist some function

$f : \mathbf{P} \rightarrowtail \mathscr{P}(\mathbf{P})$ which would define a list of all subsets of $\mathbf{P}$.

Suppose there were some such list L, and suppose that the sequence $S_1, S_2, S_3, \ldots$ is the resulting enumeration of the sets S_i of positive integers.

Diagonalization

- Let the **antidiagonal set**, with respect to the list L, written $\underline{D}_L$, be specified as follows.

  (i) $\forall n \in \mathbf{P}\ [n \in \underline{D}_L \text{ iff } \neg(n \in S_n)]$.

- The set $\underline{D}_L$ is perfectly well defined given a well defined list L, and clearly $\underline{D}_L \subseteq \mathbf{P}$ and hence $\underline{D}_L \in |\mathscr{P}(\mathbf{P})|$.
- But $\underline{D}_L$ has been constructed in such away that it <u>cannot</u> <u>appear</u> anywhere in the given list of subsets.
- For suppose that $\underline{D}_L$ did appear somewhere in L.

  Then it must be the case that $\underline{D}_L = S_k$ for some $k \in \mathbf{P}$.

Diagonalization

But if $\underline{D}_L$ and S_k were indeed the same set, then the extensional identity condition on sets requires that

$$\text{(ii) } \forall n \in \mathbf{P}\ [n \in \underline{D}_L \text{ iff } n \in S_k)].$$

- Now take the particular positive integer k which specifies the place of S_k in the list L. Formula (ii) above requires that

  $k \in \underline{D}_L$ iff $k \in S_k$, while formula (i) above requires that

  $k \in \underline{D}_L$ iff $\neg(k \in S_k)$.

- Since by hypothesis $\underline{D}_L = S_k$, this leads to the contradiction

  $$\text{(iii)} \quad k \in \underline{D}_L \text{ iff } \neg(k \in \underline{D}_L).$$

- And since the choice of k was arbitrary, formula (iii) establishes by *reductio ad absurdum* that the set of positive integers $\underline{D}_L$ cannot occur <u>anywhere</u> on the list L.

Diagonalization

- And since an antidiagonal set can be defined for *any* purported list L, it follows that there can be no enumeration of $\mathscr{P}(\mathbf{P})$.
- Accordingly there is no bijection $f : \mathbf{P} \rightarrowtail\!\!\!\!\rightarrow \mathscr{P}(\mathbf{P})$.
- But for each $n \in \mathbf{P}$, $\{n\} \in \mathscr{P}(\mathbf{P})$. Let $\mathbf{S}$ be the set of all such singletons $\{n\}$ for $n \in \mathbf{P}$.
- Then clearly $\mathbf{S} \subset \mathscr{P}(\mathbf{P})$ and the function $g : \mathbf{S} \rightarrowtail\!\!\!\!\rightarrow \mathbf{P}$, such that $g(\{n\}) = n$ is a bijection.
- Therefore the cardinality of $\mathscr{P}(\mathbf{P})$ is strictly greater than that of $\mathbf{P}$, which means that $\mathscr{P}(\mathbf{P})$ is uncountable. □

Diagonalization

- **Proof of Cantor's Theorem** that the power set of <u>any</u> set always has greater cardinality than the set itself.
- Let Γ be any set (countable or otherwise), and consider any 1-1 function $f : \Gamma \bullet\!\!\rightarrow \mathscr{P}(\Gamma)$.
- Since f is 1-1, it follows that for each distinct $x \in \Gamma$, $f(x)$ is a distinct set $\Sigma \subseteq \Gamma$.
- Let the antidiagonal set $\underline{\Delta}$ be defined as the set of all $x \in \Gamma$ such that $x \in \underline{\Delta} \leftrightarrow \neg(x \in f(x))$.

Then $\underline{\Delta} \subseteq \Gamma$, and so $\underline{\Delta} \in \mathscr{P}(\Gamma)$. But $\neg\exists x \in \Gamma$ such that $f(x) = \underline{\Delta}$.

For suppose there were such an x. Then, by the definition of $\underline{\Delta}$, it must be the case that $x \in \underline{\Delta} \leftrightarrow \neg(x \in \underline{\Delta})$.

Diagonalization

- Hence for any set Γ and any 1-1 function $f : \Gamma \bullet\!\!\rightarrow \mathscr{P}(\Gamma)$

  it is impossible for f to be *onto*,

  from which it follows that there can be

  no bijection between Γ and $\mathscr{P}(\Gamma)$.
- And by taking the set **S** of singletons of elements of Γ, as in the proof above, it can be established that there is a bijection

  $g : \mathbf{S} \bullet\!\!\rightarrow \Gamma$, where $\mathbf{S} \subset \mathscr{P}(\Gamma)$ and $g(\{n\}) = n$
- Thus for *any* set Γ, the cardinality of the power set of Γ

  is strictly **greater than** the cardinality of Γ. □