5 *Cardinal Numbers*

1. Introduction

There are numerous mathematical generalizations of the natural numbers. On the one hand, there are the integers, the rational numbers, the real numbers, and the complex numbers. On the other hand, there are the cardinal numbers and the ordinal numbers. In the present chapter, we concentrate on cardinal numbers, leaving the other kinds of number to later chapters.

Natural numbers have both a cardinal use and an ordinal use. The former pertains to the quantitative notion of "how many". The latter pertains to the order of the numbers rather than their sizes. In ordinary language syntax, the cardinal *numerals* are '1', '2', '3', etc., whereas the ordinal *numerals* are '1st', '2nd', '3rd', etc.

The cardinal (i.e., chief) use of numbers pertains to measuring how big sets are. This yields the derivative concept of the *cardinality* of a set A, which is how big A is, or how many elements A has. This suggests introducing a function sign '#(_)', defined unofficially as follows.

(d) $\#(A) =_{df}$ the number of elements in A

We need to provide a formal version of the definiens. Whatever we choose, the definition should have the following consequences. [Recall the numerical predicates from the previous chapter.]

(t0) $\#(A) = 0 \leftrightarrow 0[A]$
(t1) $\#(A) = 1 \leftrightarrow 1[A]$
(t2) $\#(A) = 2 \leftrightarrow 2[A]$
etc.

This just says the intuitively obvious – that the cardinality (size) of A is n iff A has n elements. One might be tempted to write the above series more succinctly as follows.

(t?) $\forall n\,(\,\#(A) = n \leftrightarrow n[A]\,)$

But this is ungrammatical; in first order logic, the same variable cannot appear in both singular term position and predicate position, as 'n' does in (t?). We have used the numerals ambiguously, as quantifiers, as predicates, and as singular terms; but only numerals-as-singular-terms can be quantificationally generalized in first order logic.

However, we can simulate (t?), by defining the expression '$n[A]$', not to be the result of applying predicate variable 'n' to singular term 'A' (which cannot be accomplished in first order logic), but as applying a two-place predicate, written '_[_]', to singular terms 'n' and 'A'.

In the next section, we discuss how one can define '_[_]' as a two-place predicate expression in set theory.

2. Equipollence

We know how to say that A has two, three, four, etc., elements. How do we say that A has n elements, or m+n elements?

First of all, we know (intuitively at least) that every natural number has the appropriate number of elements – 0 has 0 elements, 1 has 1 element, and in general, m has m elements. Accordingly, we know (intuitively) that a set has m elements iff it *has the same size* as the number m.

How do we define sameness of size? Usually, to decide whether sets A and B have the same size, we count A, and we count B, and we compare the results. In particular, we deem A and B to be equal in size if they are both empty, or if they both have 1 element, or if they both have 2 elements, etc.

But this produces a circular definition! We define number of elements in terms of sameness of size, and we define sameness of size in terms of number of elements.

Fortunately, counting is not the only way of comparing the sizes of A and B. We can also compare them directly. For example, I don't have to count the fingers on my right hand, and on my left hand, to know that my two hands have equally many fingers. All I have to do is pair up the fingers of the two hands. More dramatically perhaps, I do not have to count the cars on the road, and the drivers on the road, to know there are equally many cars and drivers [let us presume there are no towed cars, teaching cars, fire trucks, etc.]

The reason is that, in each case, the objects in the two sets can be paired one-to-one.

This idea of pairing the elements of the two sets leads to the official definition for equality-of-size.

(D1) A and B are equal in size $=_{\text{df}}$ there is a bijection between A and B.

Recall that a bijection between A and B is a 1-1 function from A onto B. We use a special symbol for this predicate, and we give the corresponding concept a special name – *equipollence*, also *equipotence*. To say that A and B are equipollent is to say they have the same size. The word derives from 'pollence' which means power. The power of a set is its size. For example, the power set $\wp(A)$ of a set A is always bigger than the set, as we later prove.

The formal definition goes as follows.

(D1*) $A \approx B \;=_{\text{df}}\; \exists f\,[\,f{:}A \leftrightarrows B\,]$

First of all, let us observe that $\approx$ is an equivalence relation, in the sense that the following are theorems.

(T1) $A \approx A$
(T2) $A \approx B \;\rightarrow\; B \approx A$
(T3) $A \approx B \;\&\; B \approx C \;.\!\rightarrow\; A \approx C$

The proofs are quite simple. (T1) is shown by showing that the identity function on A is a bijection from A onto itself. (T2) is shown by showing that if f maps A onto B 1-1, then the inverse function f^{-1} maps B onto A 1-1. (T3) is shown by showing that if f maps A onto B 1-1, and g maps B onto C 1-1, then the composite function $g \circ f$ maps A onto C 1-1.

We are now in a position, finally, to define '$n[A]$', at least in the finite case.

(d) $n[A] =_{df} n \in \omega \ \& \ n \approx A$

In other words, A has n elements iff there is a bijection from the number n onto A. Notice that, $t_1[t_2]$ is well-formed for any singular terms t_1, t_2, even if t_1 does not refer to a natural number. However, given the definition, $t_1[t_2]$ cannot be true unless t_1 denotes a natural number.

Notice the following natural consequences of our definitions.

(T4) $\forall n(n \in \omega \rightarrow n[n])$
(T5) $\forall n(n \in \omega \rightarrow \forall yz(n[y] \ \& \ n[z] \ .\!\rightarrow y \approx z))$

In other words, every natural number n has n elements, and if A and B both have n elements (for any n), then A and B are equal in size.

We are now in a position to go back and define the function sign '#(_)'.

(d) $\#(A) = n \ =_{df} \ n[A]$

This has the following consequence, in conjunction with the earlier theorem.

(t) $\#(A) = \#(B) \rightarrow A \approx B$

This says that if the number of A-elements is the same as the number of B-elements, then A and B are equipollent.

What we would like is the corresponding biconditional.

(??) $\#(A) = \#(B) \leftrightarrow A \approx B$

But this is not true, at least the way we have defined '#(_)' so far. The problem is that our definition of '#(_)' applies only to *finite* sets.

Finitude and infinitude are the topics of the next section.

3. Finite and Infinite Sets

At this point, we are in a position, finally, to define the term 'finite' and the complementary term 'infinite'.

(D2) $\text{fin}[A]) =_{df} \exists n(n \in \omega \ \& \ n[A])$

In other words, A is finite iff it has n elements for some natural number n, which is to say that it is equipollent to some natural number.

To say that a set is infinite is simply to say that it is not finite:

(D3) $\text{infin}[A]) =_{df} \sim\text{fin}[A]$

Clearly, there are finite sets; for example, every natural number is finite, since every natural number is equipollent to a natural number – itself. Also, the singleton of any natural number is finite, having exactly one element.

The following are expected (if not easily proved) theorems about finite sets.

(T6) $\forall x \forall y$ (fin[x] & $y \subseteq x$.→ fin[y])
(Any subset of a finite set is finite.)

(T7) $\forall x$ (fin[x] → fin[$\wp(x)$])
(The power set of any finite set is finite.)

(T8) $\forall x \forall y$ (fin[x] & fin[y] .→ fin[$x \cup y$])
(The union of two finite sets is finite.)

(T9) $\forall x \forall y$ (fin[x] & fin[y] .→ fin[$x \times y$])
(The Cartesian product of two finite sets is finite.)

(T10) $\forall x$ (fin[x] & $\forall y(y \in x$ → fin[y]) .→ fin[$\bigcup x$])
(The union of a finite collection of finite sets is finite.)

The existence of finite sets is obvious. The existence of infinite sets is less obvious. However, the Axiom of Infinity (appropriately so called) does yield the existence of at least one infinite set. In particular, we have the following theorem.

(T11) ω is infinite

Proof: we proceed by induction, proving that no natural number is equipollent to ω. Base case: ω is not equipollent to 0; this is because only 0 is equipollent to 0, and ω is not 0. Inductive hypothesis: ω is not equipollent to m, to show: ω is not equipollent to m^+. Suppose otherwise, to show a contradiction. Then there is a function that maps ω 1-1 onto m^+, call it f. There is a unique element x in ω such that $f(x)=m$, call it b. Claim: f restricted to ω-$\{b\}$ maps $\omega-\{b\}$ 1-1 onto m. Define function g from ω to $\omega-\{b\}$ as follows. For all $x \leqslant b$, $g(x)=x$; for all $x>b$, $f(x)=x^+$. Claim: g maps ω 1-1 onto $\omega-\{b\}$. Claim: $f \circ g$ maps ω 1-1 onto m, which means that ω is equipollent to m, which contradicts the inductive hypothesis.

4. Denumerable Sets

A set is finite iff it is equipollent to some element of ω; otherwise, it is infinite. On the other hand, a set is said to be *denumerable* (or denumerably infinite) if it is equipollent to the set ω of all natural numbers. Formally speaking,

(D4) $den[A] =_{\mathrm{df}} A \approx \omega$

Notice the following immediate theorem.

(T12) $\forall X$ ($den[X]$ → $infin[X]$)

I.e., every denumerable set is infinite. Reason: if X is denumerable, it is equipollent to ω; if X is finite, it is equipollent to some natural number. So if X is both denumerable and finite, then ω is equipollent to some natural number, and hence is finite, which we have already proved is not true.

Examples of denumerable sets abound. For example, the set

$$\{x : x \in \omega \ \& \ x>m\},$$

where m is any natural number, is denumerable. To show a set is denumerable, it is sufficient to produce a bijection from ω onto A. In the above case, the function is defined so that $f(x) = m+x$.

Another example, the set of multiples of m,

$$\{x : \exists y(y \in \omega \ \& \ x=my)\},$$

where m is any natural number, is also denumerable. The bijection is defined so that $f(x)=mx$.

Similarly, the set of powers of m,

$$\{x : \exists y(y \in \omega \ \& \ x=m\uparrow y) \},$$

where m is any natural number, is also denumerable. The bijection is defined so that $f(x)=m\uparrow x$.

The sets in question are all subsets of ω; indeed, they are all infinite subsets. The upshot of this is that, although it would seem that there are twice as many numbers as even numbers (multiples of 2), there are in fact equally many. The two sets can be paired up one-to-one.

The sets in question are all infinite subsets of ω. One can actually prove that every infinite subset of ω is denumerable.

(T13) $\forall X\ (\ X \subseteq \omega \ \& \ \text{infin}[X] \ .\!\rightarrow \ \text{den}[X]\ )$

Intuitive proof sketch: suppose $A \subseteq \omega$, and infin[A]. Then A is well-ordered by $\leqslant$. That means every subset X of A has a first element, denoted first(X). Define f as follows (using strong induction).

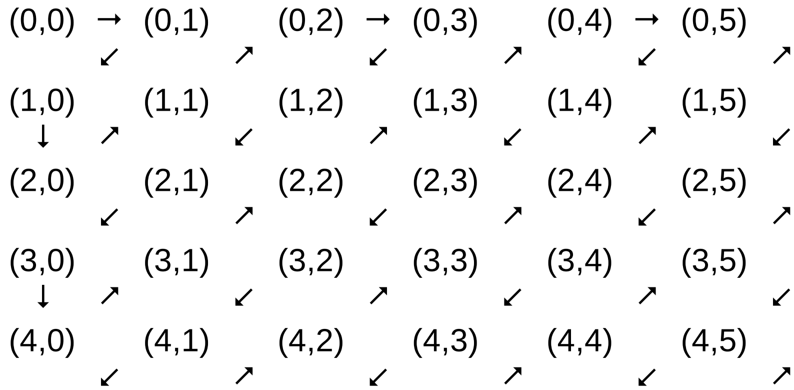
$$f(n) = \ \text{first}(A - \cup\{\{f(m)\} : m \leqslant n\})$$

Intuition: $f(0)$ is first element of A, $f(1)$ is the next element of A after $f(0)$, $f(2)$ is the next element of A after $f(1)$, etc.

Claim: f is a 1-1 function from ω onto A. Hence, A is denumerable.

So far, we have concentrated on subsets of ω. We can also look at selected supersets of ω. For example, ω^+, ω^{++}, ω^{+++}, etc. [which are the first few transfinite *ordinals*]. Recall the definition of successor: $A^+ = A \cup \{A\}$. So $\omega^+ = \omega \cup \{\omega\}$. These sets are also denumerable. For example, define $f{:}\omega^+ \rightarrow \omega$ as follows: $f(x)=0$, if $x=\omega$, otherwise $f(x)=x^+$.

The Cartesian product $\omega\times\omega$ of ω with itself seems like a candidate for a set that is considerably bigger than ω, but it too is denumerable. The function (ω-sequence) may be pictured as follows, using a technique that traces to Cantor.



An alternative picture might be visually helpful.

(0,0)

(1,0) (0,1)

(2,0) (2,1) (2,2)

(3,0) (3,1) (3,2) (3,3)

(4,0) (4,1) (4,2) (4,3) (4,4)

… … … … … …

In this diagram, we simply count the first row, the second row, etc. It is evident that every ordered pair is on some row, and each row can be counted.

The same technique can be used to prove that the rational numbers are denumerable, which means that there are just as many natural numbers as there are rational numbers!

The above technique can also be used to prove the following.

(T14) If C is denumerable, and every element of C is denumerable, then $\cup C$ is denumerable. I.e., the union of any denumerable collection of denumerable sets is itself denumerable.

(T15) If C is a finite family of denumerable sets, then $\times C$ is denumerable. I.e., the Cartesian product of any finite family of denumerable sets is denumerable.

From what has transpired so far, one would naturally draw the conclusion that all infinite sets are denumerable, which implies in particular that all infinite sets have the same size. This is quite definitely not true, as we see in the next section.

5. Uncountable Sets

So far, we have discussed finite sets and denumerable sets, which are a species of infinite sets. It was suggested at the end of the last section that there are infinite sets that are not denumerable. Such sets are called *uncountable* (also, uncountably infinite, also *nondenumerable*). The traditional usage is actually somewhat confusing, so let us chart the relationships.

(D2) A set is finite iff it is equipollent to some natural number.

(D3) A set is infinite iff it is not finite.

(D4) A set is denumerable iff it is equipollent to ω.

(D5) A set is countable iff it is finite or denumerable.

(D6) A set is uncountable (non-denumerable) iff it is infinite but not denumerable.

Notice in particular that there is overlap of the concepts; in particular, Infinite + Countable = Denumerable. Also notice the mildly illogical fact that 'nondenumerable' does not mean 'not denumerable'. A set that is not denumerable (versus nondenumerable) may be either uncountable or finite, whereas a nondenumerable set cannot be finite.

Are there any uncountable sets? The affirmative answer was first proved by Cantor, who proved two examples, namely

(c1) the set of real numbers (rationals $\cup$ irrationals) is uncountable.

(c2) the power set of ω is uncountable.

We have not discussed, nor even defined, the real numbers so far, so we must postpone the proof of (c1) until later. However, we already have the machinery to prove (c2).

(T16) $\wp(\omega)$ is uncountable.

Proof: Let f be *any* function from ω *into* $\wp(\omega)$. We wish to prove that f is not *onto*. For each number n, there is a unique subset $f(n)$; n may or may not be an element of $f(n)$. Call a number n *normal* if it is *not* an element of $f(n)$. Consider the subset of normal numbers, call it N: $N = \{n : n \notin f(n)\}$. Claim: $N \notin \text{ran}(f)$, and hence f is not onto $\wp(\omega)$. Proof: Suppose $N \in \text{ran}(f)$. Then $N = f(m)$, where $m \in \omega$. I.e., $f(m) = \{n : n \notin f(n)\}$. It follows that $m \in f(m) \leftrightarrow m \notin f(m)$, which is a contradiction. This proves that $\wp(\omega)$ is not denumerable; to prove that $\wp(\omega)$ is uncountable (nondenumerable; recall distinction from above), we must further prove that ω is infinite. This is left as an exercise.

6. Infrapollence

The theorem that $\wp(\omega)$ is uncountable is actually a special case of a more general theorem, which says that no set is equal in size to its power set, that every set is smaller in size than its power set. In order to state this theorem, we need to develop some additional notation and terminology.

Just as the identity of two sets, A and B, can be decomposed into two inclusions, $A \subseteq B$ and $B \subseteq A$, the equipollence (equality of size) of two sets can be similarly decomposed. The relevant notion is what I propose to call *infrapollence*, which means "of *lower* (or equal) *power*". It is officially defined as follows.

(D7) $A \preceq B =_{\text{df}} \exists f\,[\, f{:}A \rightarrow B(1\text{-}1)\,]$

The definiendum is read: A is smaller than or equal in size to B. The definition says this means that there is a 1-1 function from A *into* B. Recall that such a function is sometimes called an *injection*. Thus, A is smaller than or equal in size to B iff there is an injection from A into B.

The definition seems intuitively correct. It basically says that for every A-element, a, there is a unique B-element, $f(a)$, and maybe there are some B-elements left over; in other words, there are enough B's to "go around".

The following theorems are obvious consequences of the definition.

(T17) $A \preceq A$
(T18) $A \preceq B\ \&\ B \preceq C\ .\!\rightarrow\ A \preceq C$
(T19) $A \subseteq B\ \rightarrow\ A \preceq B$
(T20) $A \approx B\ \rightarrow\ A \preceq B$

In (T17), the identity function injects A into itself. In (T18), if f injects A into B, and g injects C into D, then the composite function $g\circ f$ injects A into C. In (T19), the identity map on A injects A into any superset of A. In (T20), if f maps A 1-1 *onto* B, then it automatically maps A 1-1 *into* B.

(T17) and (T18) say that $\preceq$ is a quasi-order relation, so there is an associated strict order relation, called strict infrapollence, defined as follows.

(D8) $A \prec B\ =_{\text{df}}\ A \preceq B\ \&\ \sim[B \preceq A]$

It is easy to show that $\prec$ satisfies the following conditions.

(T21) $A \prec B\ \&\ B \prec C\ .\!\rightarrow\ A \prec C$
(T22) $A \prec B\ \rightarrow\ \sim[B \prec A]$
(T23) $\sim[A \prec A]$

In other words, strict infrapollence is transitive, asymmetric, and irreflexive.

7. The Schroeder-Bernstein Theorem

As we saw in the previous section, infrapollence is a quasi-order relation, which is to say that the following obtains.

(T17) $A \preceq A$
(T18) $A \preceq B\ \&\ B \preceq C\ .\!\rightarrow\ A \preceq C$

As with every quasi-order relation, there is an affiliated equivalence relation, defined in the usual way.

(d) $A \simeq B\ =_{\text{df}}\ A \preceq B\ \&\ B \preceq A$

Recall that a quasi-order is a partial order iff the affiliated equivalence relation is the identity relation. Needless to say, $\preceq$ is not a partial order relation; the following is *not* true.

(false) $A \preceq B\ \&\ B \preceq A\ .\!\rightarrow\ A = B$

For example, consider $\{a\}$, $\{b\}$, where $a \neq b$. Then $\{a\} \preceq \{b\}$ and $\{b\} \preceq \{a\}$, but $\{a\} \neq \{b\}$. On a more esoteric level, the set $\omega+$ of positive natural numbers can be injected into ω, by the identity function, and ω can be injected into $\omega+$, by the successor function. But $\omega \neq \omega+$.

But what is the equivalence relation $\simeq$? The answer is exactly what one might expect – equipollence. In other words, we have the following theorem, which is usually called the Schroeder-Bernstein Theorem

(T24) $A \preceq B \ \& \ B \preceq A \ .\!\rightarrow\ A \approx B$

It is also called the Cantor-Schroeder-Bernstein Theorem; Cantor conjectured it, and Schroeder and Bernstein independently proved it in the 1890's.

In order to prove The Schroeder-Bernstein Theorem, (T24), we first prove another important theorem, the Fixed Point Theorem (or rather, a special case).

Fixed Point Theorem (special case):

(T25) Let A be any set, and let f be any function from $\wp(A)$ into $\wp(A)$ satisfying the following condition, called monotonicity.

(m) $\forall XY[X \subseteq Y \ \rightarrow\ f(X) \subseteq f(Y)]$

Then there is a "fixed point", i.e., a set Z such that $f(Z)=Z$.

Proof: Suppose f is such a function on $\wp(A)$. Consider the collection $\{X\colon X \subseteq f(X)\}$, call it C. Consider the union, $\cup C$. We wish to show that $\cup C = f(\cup C)$.
Claim: $\forall X[X \in C \ \rightarrow\ X \subseteq f(\cup C)]$. For suppose $D \in C$; then $D \subseteq f(D)$; also $D \subseteq \cup C$, so by (m), $f(D) \subseteq f(\cup C)$. So, $D \subseteq f(\cup C)$. So, by a previous theorem, $\cup C \subseteq f(\cup C)$. We are half done. Now, $\cup C \subseteq f(\cup C)$, so by (m), $f(\cup C) \subseteq f(f(\cup C)$. But the latter means that $f(\cup C) \in C$, from which we obtain the converse inclusion, $f(\cup C) \subseteq \cup C$. Thus, $f(\cup C) = \cup C$.

Next, we state a few relevant lemmas, whose proofs are left as exercises.

Lemma 1:

Let A and B be sets. Let A_1 and A_2 be disjoint subsets of A such that $A_1 \cup A_2 = A$. Similarly, let B_1 and B_2 be disjoint subsets of B such that $B_1 \cup B_2 = B$. Then:

$A_1 \approx B_1 \ \& \ A_2 \approx B_2 \ \rightarrow .\ A \approx B$

Lemma 2:

Let A be any set, let X,Y be any subsets of A, and let f be any function on A. Then:

(1) $X \subseteq Y \ \rightarrow\ A - Y \subseteq A - X$
(2) $X \subseteq Y \ \rightarrow\ f^{\rightarrow}(X) \subseteq f^{\rightarrow}(Y)$

Lemma 3 (a corollary to Lemma 2):

Let A,B be any sets, let f be any function from A to B, let g be any function from B into A, let X,Y be any subsets of A. Then:

$$X \subseteq Y \;\rightarrow\; g^{\rightarrow}(B{-}f^{\rightarrow}(A{-}X)) \subseteq g^{\rightarrow}(B{-}f^{\rightarrow}(A{-}Y))$$

Lemma 4:

if f is a 1-1 function, and $A \subseteq \text{dom}(f)$, then $A \approx f^{\rightarrow}(A)$

Having proven the fixed point theorem, and the relevant lemmas, we now prove

The Schroeder-Bernstein Theorem.

(T24) $A \preceq B \;\&\; B \preceq A \;.\!\rightarrow\; A \approx B$

Proof: Suppose $A \preceq B$ & $B \preceq A$, to show $A \approx B$. Then there is an injection, f, from A into B. And there is an injection, g, from B into A. We use Lemma 1 to show $A \approx B$; in particular, we divide A into disjoint parts A_1, A_2, and B into disjoint parts B_1, B_2, and we show the respective parts are equipollent. We divide A into parts by appealing to the Fixed Point Theorem. Specifically, by Lemma 3, the function that maps each subset X of A to the set $g^{\rightarrow}(B{-}f^{\rightarrow}(A{-}X))$ satisfies the requirements of (FTP), so there is fixed point, namely a set, call it K, such that $g^{\rightarrow}(B{-}f^{\rightarrow}(A{-}K)) = K$. Since $A{-}K \subseteq \text{dom}(f)$, $A{-}K \approx f^{\rightarrow}(A{-}K)$, by Lemma 4. Also, $B{-}f^{\rightarrow}(A{-}K) \subseteq \text{dom}(g)$, and $K = g^{\rightarrow}(B{-}f^{\rightarrow}(A{-}K))$, so $K \approx B{-}f^{\rightarrow}(A{-}K)$, by Lemma 4. Furthermore, the sets in question divide A and B respectively, so applying Lemma 1, we have $A \approx B$.

8. Hyper-Uncountable Sets; The Continuum Hypothesis

We proved earlier that the power set of ω is uncountable. In the present section, we use the same technique, in conjunction with the Schroeder-Bernstein theorem, to show that every set is strictly smaller than its power set. This is sometimes called Cantor's Theorem.

(T25) $A \prec \wp(A)$

Proof: Given the definition, we have to show $A \preceq \wp(A)$, and we have to show $\sim[\wp(A) \preceq A]$. The former is shown by noting that the function f, defined so that $f(x)=\{x\}$ is an injection from A into $\wp(A)$. The latter is shown by showing $\sim[\wp(A) \approx A]$, and appealing to the Schroeder-Bernstein Theorem. So suppose that $\wp(A) \approx A$. Then there is a 1-1 function from A onto $\wp(A)$. We prove that, in fact, there is no function from A onto $\wp(A)$. Once again, we construct the set of normal elements of A. $N = \{x\colon x \notin f(x)\}$. Claim: $N \notin \text{ran}(f)$. For suppose otherwise. Then $N = f(a)$, where $a \in A$. So $f(a) = \{x\colon x \notin f(x)$, from which it follows that $a \in f(a) \leftrightarrow a \notin f(a)$, a contradiction.

Since every set is smaller than its power set, we have the following infinite chain.

$$A \prec \wp(A) \prec \wp\wp(A) \prec \wp\wp\wp(A) \prec \text{etc.}$$

In the case that A is infinite, we obtain the result that there are infinitely many degrees of infinity. $\wp(\omega)$ is bigger than ω, $\wp\wp(\omega)$ is bigger than $\wp(\omega)$, $\wp\wp\wp(\omega)$ is bigger than $\wp\wp(\omega)$, etc. One might describe this by saying that $\wp(\omega)$ is uncountable, $\wp\wp(\omega)$ is hyper-uncountable, $\wp\wp\wp(\omega)$ is hyper-hyper-uncountable, etc.

[What is worse, there is a set bigger than all of these – an infinitely-hyper-uncountable set! However, we do not prove that just yet.]

Before moving on, it is useful to consider the following questions.

(q1) $\exists X[\omega \prec X \;\&\; X \prec \wp(\omega)]$??
(q2) $\exists X[\wp(\omega) \prec X \;\&\; X \prec \wp\wp(\omega)]$??
(q3) $\exists X[\wp\wp(\omega) \prec X \;\&\; X \prec \wp\wp\wp(\omega)]$??
etc.

The *negative* answer to (q1) is known as the **Continuum Hypothesis** (CH), and the *negative* answer to the entire series is known as the **Generalized Continuum Hypothesis** (GCH).

To prove the Continuum Hypothesis was the first problem posed by Hilbert in his famous list of outstanding problems in mathematics (1900). In the 30's, Gödel proved CH could be consistently added to set theory. In the 60's, Paul Cohen proved that CH cannot be derived from the usual axioms of set theory.

9. The Cardinal Numbers

Finally, we return to our original problem – to identity (or postulate) the cardinal numbers in such a way that we can deduce the following theorem, which might be called the Fundamental Principle of Cardinal Numbers.

(t) $\#(A) = \#(B) \leftrightarrow A \approx B$

Perhaps it is useful to consider the solution proposed by Russell and Whitehead in *Principia Mathematica*, where #(_) is defined as follows.

(RW1) $\#(A) =_{\text{df}} \{X : X \approx A\}$

(RW2) $\text{card}[A] =_{\text{df}} \exists X\,[\, A = \#(X)\,]$

In other words, the cardinality of a set A is simply the collection of all sets equipollent to A, and cardinal numbers are equivalence classes, where the equivalence relation is equipollence. For example, the cardinality of the empty set is $\{\varnothing\}$, which is Russell's definition of the cardinal number zero, and the cardinality of the singleton $\{\varnothing\}$ is the set of all singletons, which is Russell's definition of the cardinal number one. Infinite cardinal numbers are just equivalence classes whose members are infinitely large sets.

It is easy to see that, *provided* $\#(A)$ is always a proper set (i.e., non empty), then (t) is an immediate consequence of the Russell-Whitehead definition. It is just like factoring out an equivalence relation on a set. The equivalence classes are identical iff the objects are equivalent.

Unfortunately, as we have already seen, there is a serious difficulty with the Russell-Whitehead definition of the natural numbers, let alone their definition of general cardinal numbers. Within our framework, the equivalence classes in question do not exist (except the first one); they are too big.

As seen in an earlier chapter, in the case of the natural numbers (the finite cardinal numbers), we circumvent this problem by a special selection method. We select a representative singleton, and decree it to be the number 1, we select a representative doubleton, and decree it to be the number 2, etc.

It appears that we have to do the same thing for the transfinite cardinals. For each “cardinality class”, we have to select a representative set of that cardinality. This includes picking a representative of each of the following.

(c1) an X such that $X \approx \omega$
(c2) an X such that $X \approx \wp(\omega)$
(c3) an X such that $X \approx \wp\wp(\omega)$
etc.

More generally, for each set A, we must select a representative set equipollent to A.

The official definition we adopt goes as follows.

(D9) $\#(A) =_{df}$ the first ordinal number α such that $\alpha \approx A$

[Ordinals are discussed in detail in the next chapter.] Observe that this definition does not work properly unless we assume the Axiom of Choice. The ordinals are well-ordered by $\preceq$, where $a \preceq b$ iff $a \in b$ or $a = b$. So if there are any ordinals equipollent to a set A, there is a smallest such ordinal. The question, then, is whether every set is equipollent to at least one ordinal number. Here, we appeal to the Well-Ordering Theorem, which is a well-known equivalent of the Axiom of Choice. In particular, we well-order the set A (using AC), and then we appeal to a further theorem that every well-ordered set is isomorphic (and hence equipollent) to at least one ordinal.

For those who don’t accept the Axiom of Choice, other routes are available. One approach is to treat the expression ‘$\#(A)$’ as syncategorimatic, as a pseudo-term, by which I mean that it only appears in formulas of the form ‘$\#(A)=\#(B)$’, and these formulas are defined as follows.

(d) $\#(A) = \#(B) =_{df} A \approx B$

A more common alternative approach is to introduce ‘#(_)’ as a further *primitive* item of set theory, and postulate the following further axiom.

(a1) $\forall x \forall y\, [\, \#(x)=\#(y) \leftrightarrow x \approx y\,]$

If this is all we postulate, then we cannot prove that the natural numbers, as defined earlier, are cardinal numbers. In this case, we have both the finite cardinals and the natural numbers. If this is undesirable, then we probably would add the following further postulates.

(a2) $\forall x\, [\, \exists n(n \in \omega\ \&\ x \approx n\ . \leftrightarrow \#(x)=n\,]$

This has the desirable consequence that the finite cardinals are coextensive with the natural numbers. It does not say what the infinite cardinal numbers are, however. For example, the infinite cardinal numbers may be finite sets, for all we know. This is ok, so long as they are not natural numbers. The following might be true (for all we know).

$\#(\omega) = \{\{\varnothing\}\}$
$\#(\wp(\omega)) = \{\{\{\varnothing\}\}\}$
$\#(\wp\wp(\omega)) = \{\{\{\{\varnothing\}\}\}\}$

If we want the infinite cardinal numbers to be like the finite cardinal numbers, in the sense that they all have the “appropriate” size, then the following is a further plausible axiom.

(a3) $\forall X[\#(X) \approx X]$

This just says that the cardinal number of a set is the same size as the set. This rules out the above identifications.

Still another approach is to treat cardinal numbers as points (first elements), rather than as sets, in which case no cardinal number is identified with any set. This requires redoing the theory of natural numbers.

So long as we have the Fundamental Principle of Cardinal Numbers, either as a theorem deduced from the definition of cardinal number, or as an axiom within a theory that regards '#(_)' as a primitive expression, we can deduce many properties of cardinal numbers.

For example, we can define addition, multiplication, and less-than-or-equal, as follows.

(D10) $m+n=k =_{df} \exists XY(\, X\perp Y \;\&\; \#(X)=m \;\&\; \#(Y)=n \;\&\; \#(X\cup Y)=k \,)$
(D11) $mn=k =_{df} \exists XY(\, \#(X)=m \;\&\; \#(Y)=n \;\&\; \#(X\times Y)=k \,)$
(D12) $m \leq n =_{df} \exists XY(\, \#(X)=m \;\&\; \#(Y)=n \;\&\; X \preceq Y \,)$

For example, one can prove that addition and multiplication are both associative and commutative, that multiplication distributes over addition, that ≤ is reflexive, transitive, and anti-symmetric. Curiously, one cannot prove that ≤ is connected; that is, one cannot prove

(C) $m \leq n \vee m \leq n$,

without appealing to the Axiom of Choice; (C) is in fact equivalent to the Axiom of Choice. So, if one believes that infinite cardinal numbers are (or should be) arranged in a linear order just like the finite cardinal numbers, then one must further postulate (C), but this is tantamount to postulating the Axiom of Choice, in which case one might as well define the cardinal numbers to be first ordinal numbers, as originally suggested.

Mathematicians routinely employ the Axiom of Choice in their reasoning, because of its great power, although many use it apologetically. As shown by Cohen, AC is not a logical consequence of Zermelo-Fraenkel set theory, and hence is not an essential feature of the *iterative conception of sets*.

The latter is the idea that sets are generated from first elements by repeated (iterated) application of a few set-forming processes, including – pairs, unions, power sets, and replacement. These seem a necessary part of our conception of sets. By contrast, the epistemological status of the other axioms, including the Axiom of Choice, and the Continuum Hypothesis, remains unclear. This suggests the existence of alternative set theories on a par with alternative (non-Euclidean) geometries.