Two Classical Surprises Concerning the Axiom of Choice and the Continuum Hypothesis

Leonard Gillman

1. INTRODUCTION. In this paper we introduce the reader to two remarkable results in the theory of sets. Both are more than fifty years old, but neither one appears to be well known among nonspecialists. Each one states that a certain proposition implies the *Axiom of Choice*. First we describe the results, then review definitions, then, finally, present the proofs, most of which are straightforward.

Our first surprise concerns *Trichotomy*, which states that any two (infinite) cardinals $\mathfrak{a}$ and $\mathfrak{b}$ are *comparable*—i.e., either $\mathfrak{a} < \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} > \mathfrak{b}$. In the absence of special assumptions, Trichotomy may not be taken for granted. In fact, Friedrich Hartogs proved in 1915 that Trichotomy implies the Axiom of Choice. (This is the surprise.) It is an astounding result, as Trichotomy appears to be an isolated proposition. In addition, the same paper of Hartogs makes a crucial contribution to the "continuum problem," which is to decide where $\mathfrak{c}$, the cardinal of the continuum (i.e., the cardinal of the set $\mathbf{R}$ of real numbers), lies in the hierarchy of the "alephs": $\aleph_1, \aleph_2, \ldots, \aleph_\alpha, \ldots$. (I exclude $\aleph_0$ from the list, as it had been ruled out by Cantor twenty-five years earlier [2].) The problem was unyielding, causing some mathematicians to wonder in desperation whether $\mathfrak{c}$ might actually be greater than *all* the alephs. But Hartogs showed that *no* cardinal can have this property. Remarkably, Hartogs's reputation is primarily as the best known among the early pioneers in the field of several complex variables.

Georg Cantor was the creator of the theory of sets. His most famous theorem states that every cardinal $\mathfrak{m}$ satisfies $\mathfrak{m} < 2^{\mathfrak{m}}$ [2]. The *Continuum Hypothesis* asserts that $2^{\aleph_0} = \aleph_1$, the latter being an immediate successor to $\aleph_0$—conceivably, there are more than one—and hence implies that there is no cardinal lying strictly between $\aleph_0$ and $2^{\aleph_0}$. The *General* (or *Generalized*) *Continuum Hypothesis* states that, for every cardinal $\mathfrak{m}$, no cardinal lies strictly between $\mathfrak{m}$ and $2^{\mathfrak{m}}$.

The second surprise, published by Wacław Sierpiński in 1947, is that the General Continuum Hypothesis implies the Axiom of Choice, whereas the two seem to have nothing to do with one another. As a bonus, the proof makes use of Sierpiński's sharpened version of Hartogs's theorem.

Kurt Gödel proved in 1938 that the General Continuum Hypothesis and the Axiom of Choice are consistent with the usual (Zermelo-Fraenkel) axioms of set theory [4]. Twenty-five years later, Paul Cohen established that the negations of the Continuum Hypothesis and the Axiom of Choice are also consistent with these axioms [3]. Taken together, these results tell us that the Continuum Hypothesis and the Axiom of Choice are *independent* of the Zermelo-Fraenkel axioms.

We shall work within the framework of classical "naive" set theory rather than modern axiomatic set theory. We assume that the reader is familiar with the elementary notions of *set, element, membership, subset, inclusion, union* and *intersection*, and the *empty set*. This last is denoted by the Norwegian and Danish letter $\varnothing$, sounded much like the "u" in "put" or the German "ö".

A (*total* or *linear*) *order* on a set S is a relation '$<$' that satisfies the following three conditions for all x, y, and z in S:

(i) either $x = y$ or $x < y$ or $y < x$;

(ii) $x \not< x$;

(iii) if $x < y$ and $y < z$, then $x < z$.

The set S, equipped with the order relation $<$, is called a (*totally* or *linearly*) *ordered* set. The set **R** of real numbers, with its natural ordering, is a familiar example of an ordered set, as are all its subsets (understood: in the order inherited from **R**).

Two ordered sets are said to be *similar* (or *order-isomorphic*) if there is an order-preserving, one-to-one correspondence between them. Similar sets are said to have the same *order type* (and dissimilar sets to have different order types). It is clear that similarity is an equivalence relation. A finite set of n elements can be ordered in $n!$ ways, but all the ordered sets thus obtained are similar: each has a first element, a second, ..., and, finally, an nth. The order type in this instance is (happily) symbolized by n.

Conditions (ii) and (iii) by themselves define $<$ as a *partial order* (and the set with this ordering as a *partially ordered* set). The standard example of a partially ordered set that is not totally ordered is the set of all subsets of a given set (of more than one element) ordered by inclusion. An example for the nonmathematician is a couple with two children, with $x < y$ meaning that person x is a direct ancestor of person y.

2. CARDINAL NUMBERS.

The "cardinal (number)" of a set is a generalization to all sets, nonfinite as well as finite, of the concept of "number of elements." The cardinal of a finite set of n elements is denoted by n (the same symbol used for its order type). In particular, the cardinal of the empty set is 0. The terms *finite set* (or *cardinal*) and *infinite set* (or *cardinal*) should be obvious. (But see the "crucial distinction" a few paragraphs hence.) Fundamental in this discussion is the relation of 'equipotency': two sets are said to be *equipotent* provided a one-to-one correspondence exists between them. It is clear that equipotency is an equivalence relation on the class of all sets. [*Technical note*: One does not speak of "the *set* of all sets," as this concept leads to serious logical difficulties.]

In the absence of the Axiom of Choice, the definition of cardinal number is complicated. In our informal setting, we shall accept the principle that with every set there is associated an object called its *cardinal number* (or *cardinal* or *cardinality* or *power*) in such a way that two sets are associated with (or "have") the same cardinal if and only if they are equipotent. We do not go into how this association is achieved, but just assume that somehow or other it is. This is probably the attitude of many if not most mathematicians, who are likely to be more interested in their own fields than in learning about axioms in someone else's. We will often refer to a set as a *representative* of its cardinal. The cardinal of a set S is denoted by $|S|$.

The number $\aleph_0$. The character $\aleph$ is "aleph," the first letter of the Hebrew alphabet. The symbol $\aleph_0$ denotes the cardinal of the set **N** of natural numbers $0, 1, \ldots, n, \ldots$, i.e., $|\mathbf{N}| = \aleph_0$. A set that is either finite or of cardinal $\aleph_0$ is said to be *countable*. (A set of cardinal $\aleph_0$ itself is conveniently referred to as *countably infinite*.) One of Cantor's earliest triumphs was to prove that **Q**, the set of rational numbers, is countable (and hence countably infinite) [1].

Comparability of cardinals. Let $\mathfrak{a}$ and $\mathfrak{b}$ be cardinals, with representative sets A and B, respectively. We define $\mathfrak{a} < \mathfrak{b}$ (or, equivalently, $\mathfrak{b} > \mathfrak{a}$) to mean that A is equipotent with some subset of B, but B is not equipotent with any subset of A. (As usual, A and B may be replaced by any other representative sets.) The relation $<$ just defined

is irreflexive and transitive; it therefore defines a partial ordering relation on the class of all cardinals. The notation $\mathfrak{a} \leq \mathfrak{b}$ ($\mathfrak{b} \geq \mathfrak{a}$) signifies that A is equipotent with some subset of B. [*A crucial distinction*: In the absence of the Axiom of Choice (in fact, in the absence of the weaker axiom of "countable choice"), we do not know that an arbitrary infinite set necessarily has a countably infinite subset—in other words, we do not know that an arbitrary infinite cardinal is greater than or equal to $\aleph_0$.]

Of major importance in connection with the comparability of cardinals is:

Bernstein's Equivalence Theorem. *Two sets each equipotent with a subset of the other are equipotent.*

This result justifies the notation '$\leq$', as it can be paraphrased as:

$$\text{If } \mathfrak{a} \leq \mathfrak{b} \text{ and } \mathfrak{a} \geq \mathfrak{b}, \text{ then } \mathfrak{a} = \mathfrak{b}.$$

The theorem was conjectured by Cantor, who assigned it to his doctoral student Felix Bernstein, who eventually proved it. The names "Cantor" or "Schröder" are often included along with Bernstein's in the title of the theorem, Schröder having been the first person to give a proof. Proofs were subsequently given by several others, notably Peano [**7**] and Zermelo [**11**], whose proofs are essentially identical. Their argument is sufficiently elegant that I cannot resist the temptation to repeat it here.

Let A and B be the two sets under consideration in Bernstein's theorem. We are given that there exist a one-to-one mapping of A onto a subset B' of B and a one-to-one mapping of B onto a subset A' of A. The latter takes B' onto a subset A'' of A', so $A \supset A' \supset A''$. Decompose A into the disjoint sets

$$P = A'', \quad Q = A' \setminus A'', \quad R = A \setminus A',$$

and note that $P \cup Q = A'$. We have $P \cup Q \cup R = A \equiv A'' = P$ ('$\equiv$' denoting equipotency). Because $B \equiv A'$, it will suffice to show that $P \cup Q \equiv P$. (All this is in Bernstein's proof.)

Now let f denote the composite one-to-one mapping $A \rightarrow B' \rightarrow A''$, and for each subset X of A define $X^* = f(X) \cup Q$. Let us say that a subset X of A is "normal" if $X \supset X^*$. (For example, A is normal.) It is readily seen that all sets X^* are normal and that arbitrary intersections of normal subsets are normal. In particular, the set N that is the intersection of *all* normal subsets is normal. Obviously, N is the smallest of all the normal subsets. Since $N \supset N^*$ and N^* is normal, we must have $N = N^*$. Thus, $N = f(N) \cup Q$. Noting that the sets $f(X)$ are subsets of P, we may introduce a set Y, the complement of $f(N)$ in P. Then $P = Y \cup f(N)$ and we have

$$P \cup Q = Y \cup f(N) \cup Q = Y \cup N \equiv Y \cup f(N) = P,$$

which completes the proof.

Suppose that for every pair of cardinals $\mathfrak{a}$ and $\mathfrak{b}$ either $\mathfrak{a} \leq \mathfrak{b}$ or $\mathfrak{a} \geq \mathfrak{b}$—that is to say, either $\mathfrak{a} < \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} > \mathfrak{b}$. Then Trichotomy holds and the partial ordering relation on the class of all cardinals is a total ordering. On the other hand, as was pointed out earlier, we may not assume without further evidence that this is the case: conceivably for some pair of cardinals $\mathfrak{a}$ and $\mathfrak{b}$ the relations $\mathfrak{a} \leq \mathfrak{b}$ and $\mathfrak{a} \geq \mathfrak{b}$ both fail.

3. THE ARITHMETIC OF CARDINALS. In the definitions that follow, $\mathfrak{a}$ and $\mathfrak{b}$ will denote arbitrary cardinals, and A and B will be corresponding representative sets.

It will be true in each case that the defining equation is independent of the choice of representatives. Note that from arbitrary representatives A and B of $\mathfrak{a}$ and $\mathfrak{b}$ we can always create *disjoint* representatives—for example, the set of all pairs $(a, 0)$ for a in A and the set of all pairs $(b, 1)$ for b in B.

Addition.

$$\textit{Definition:} \quad \mathfrak{a} + \mathfrak{b} = |A \cup B|,$$

where in this one case we require A and B to be disjoint. Addition, thus defined, is associative and commutative, and $\mathfrak{a} + 0 = \mathfrak{a}$. (Infinite sums are also defined, typically with the help of the Axiom of Choice.) It is easy to show that

$$1 + \aleph_0 = \aleph_0,$$

and in fact that

$$\aleph_0 + \aleph_0 = \aleph_0.$$

For important use later, we establish the following fact:

$$\textit{If } \mathfrak{m} \geq \aleph_0, \textit{ then } 1 + \mathfrak{m} = \mathfrak{m}. \tag{1}$$

The hypothesis implies that a representative set M of power $\mathfrak{m}$ has a subset N of power $\aleph_0$. Define $\mathfrak{a} = |M \setminus N|$. Since M is the union of the disjoint sets N and $M \setminus N$, we have

$$\mathfrak{m} = \aleph_0 + \mathfrak{a} = 1 + \aleph_0 + \mathfrak{a} = 1 + \mathfrak{m}.$$

Multiplication.

$$\textit{Definition:} \quad \mathfrak{a}\mathfrak{b} = |A \times B|,$$

where $A \times B = \{(a, b) : a \in A, \ b \in B\}$, the usual Cartesian product of A and B. Multiplication, defined in this way, is associative and commutative, is distributive over addition, and satisfies $\mathfrak{a} \times 1 = \mathfrak{a}$ and $\mathfrak{a} \times 0 = 0$. Cantor's "First Diagonal Process" shows that $\aleph_0 \times \aleph_0 = \aleph_0$. Multiplication is also representable as repeated addition (usually requiring the Axiom of Choice when infinite sums are involved).

Exponentiation.

$$\textit{Definition:} \quad \mathfrak{a}^{\mathfrak{b}} = |A^B|,$$

where A^B denotes the set of all mappings from B into A. The familiar laws of exponents hold, plus the equation $0^0 = 1$. (Don't let your calculus students see this one!) Exponentiation is also representable as repeated multiplication (infinite products typically requiring the Axiom of Choice).

The most important exponentials are those with base 2, where 2 represents the set $\{0, 1\}$. (For clarification of this usage of the numeral 2, see the material on ordinal numbers in Section 5.) Observe that we may regard $\{0, 1\}^S$ as the set of all subsets of S: to do this we merely identify each subset T of S with its "characteristic function" χ_T, defined on S by

$$\chi_T(s) = \begin{cases} 1 & \text{if } s \in T, \\ 0 & \text{if } s \notin T. \end{cases}$$

The most famous example is $2^{\aleph_0}$, which we are free to interpret as either the set of all subsets of $\mathbf{N}$ or the set of all mappings of $\mathbf{N}$ into $\{0, 1\}$, i.e., the set of all sequences of 0s and 1s. Its cardinal is of course $2^{\aleph_0}$ (where now 2 is the cardinal of the set $\{0, 1\}$). This set of sequences represents the binary expansions of all real numbers in the interval $[0, 1]$—with the help of some tweaking to avert duplications of the sort $.0111\ldots = .1000\ldots$ that arise from the dyadic rationals. The interval $[0, 1]$, like all other intervals of $\mathbf{R}$, is equipotent with $\mathbf{R}$ itself. Therefore $\mathfrak{c} = 2^{\aleph_0}$.

If $\mathfrak{a} \leq \mathfrak{a}'$ and $\mathfrak{b} \leq \mathfrak{b}'$, then assuredly $\mathfrak{a}^{\mathfrak{b}} \leq \mathfrak{a}'^{\mathfrak{b}'}$. On the other hand, one should be wary of concluding the strict inequality, even when both the given inequalities are strict: Tarski long ago cooked up a counterexample [**10**, p. 10].

4. THE AXIOM OF CHOICE.
This is the assertion that for any collection of nonempty sets there exists a set containing an element from each set of the collection. Despite its innocuous sound, this principle has been a source of wide controversy among mathematicians and logicians, with many insisting that they don't know what its statement *means*: in the absence of a rule specifying which elements are to be chosen, what does it mean to say that the set in question *exists*? Others are content to interpret the axiom as simply postulating a set without identifying the elements it comprises. It is a safe bet that most mathematicians who make use of the axiom in their work as a matter of course are not always aware that that is what they are doing—for example, when arguing that if a point in a Euclidean space is a point of accumulation of a set, then there is a sequence of points of the set converging to the point.

5. WELL ORDERING.
An ordered set is said to be *well ordered* if every nonempty subset has a least (= first) element. Trivially, every ordering of a finite set is a well ordering. More significantly, the set $\mathbf{N}$ of natural numbers is well ordered (in its usual order), a fact well known to be equivalent to the principle of mathematical induction.

The *Well-Ordering Theorem* asserts that every (infinite) set can be well ordered. It is due to Ernst Zermelo [**12**]. It is arguably the most important application of the Axiom of Choice. Conversely, the Axiom of Choice is an easy consequence of the theorem.

Ordinal numbers (or ordinals). Whereas the cardinal of a set measures its quantity, the ordinal of a (well-ordered) set measures its "length." The formal definition of ordinal is recursive, each new one being defined as the set of all preceding ordinals:

$$0 = \varnothing, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \ldots, \quad n + 1 = \{0, 1, \ldots, n\}, \ldots$$

$$\omega = \{0, 1, \ldots, n, \ldots\}, \quad \omega + 1 = \{0, 1, \ldots, n, \ldots, \omega\}, \ldots.$$

It may seem at first glance that the "transfinite" sequence generated by this process must be countable, but the fact is that it reaches and surpasses cardinalities of almost unimaginable size.

Recall that the "second principle" of induction for $\mathbf{N}$ proceeds by passing from *all* predecessors of n to n. In the realm of arbitrary infinite sets, this principle is known as *transfinite induction*. It is viable on a set if and only if the set is well ordered.

Ordinals are well-ordered sets—indeed, they are the models for well-ordered sets. The class of all ordinals is well ordered by inclusion, $\alpha \subset \beta$ implying $\alpha \leq \beta$. Every well-ordered set is similar to a unique ordinal, which represents its order type. As suggested by the foregoing display, the ordinal of $\mathbf{N}$ is ω. The subset $\mathbf{N}_0$ of even numbers and the subset $\mathbf{N}_1$ of odd numbers are also of type ω. Ordinals beyond $\omega + 1$ are not commonly encountered in everyday life. Here's one: the ordered set that lists $\mathbf{N}_0$ in its natural order followed by $\mathbf{N}_1$ in its natural order. That it is well ordered is easy to

verify. Because it consists of a set of type ω followed by a set of type ω, its ordinal is designated as $\omega + \omega$. Evidently, none of the familiar sets $\mathbf{R}$, $\mathbf{Q}$, or $\mathbf{Z}$ (the integers) is well ordered.

Segments. For each element w of a well-ordered set W, the set

$$\{x \in W : x < w\}$$

(in which it is understood that '$<$' denotes the ordering relation on W) is known as a *segment* of W, specifically, the segment determined by w. The following theorems about well-ordered sets and their segments are fundamental:

  a. *Every subset of a well-ordered set is well ordered.*
  b. *Every well-ordered set W is similar to a unique ordinal, which is greater than the ordinal of any of the segments of W. In particular, a well-ordered set is not similar to any of its segments.*
  c. *Distinct ordinals are dissimilar.*
  d. *Of two dissimilar well-ordered sets, one is similar to a segment of the other. In particular, of two different ordinals, one is a segment of the other.*
  e. *Every segment of an ordinal is an ordinal.*
  f. *The ordinal number of an ordinal α is α itself.*
  g. *Every well-ordered set is similar to its set of segments ordered by set inclusion under the mapping that takes each element to the segment it determines.*

6. THE ALEPHS. An *aleph* is the cardinal number of an infinite *well-ordered* set. Since subsets of well-ordered sets are well ordered, we can state:

Any infinite cardinal less than an aleph is an aleph.

In the presence of the Axiom of Choice, all sets are well orderable and all infinite cardinals are alephs.

The alephs are indexed and their sizes well ordered by the ordinals; hence any two alephs are comparable, and every nonempty set of alephs has a least member. The smallest aleph is $\aleph_0$. One can show without much difficulty that the set Z_0 of all ordinals of cardinal $\aleph_0$ is uncountable; the number $\aleph_1$ is defined to be the cardinal of Z_0. Next, for each finite n, $\aleph_{n+1}$ is by definition the cardinal of the set Z_n of all ordinals of cardinal $\aleph_n$. The cardinal $\aleph_\omega$ is then defined to be the sum of the $\aleph_n$ over all finite n, i.e., the cardinal of the union of the Z_n for all finite n. Likewise, for an arbitrary ordinal α, $\aleph_{\alpha+1}$ is the cardinal of Z_α, the set of all ordinals of cardinal $\aleph_\alpha$. Finally, for a limit ordinal λ (an ordinal that, like ω, has no immediate predecessor), $\aleph_\lambda$ is the sum of all alephs of smaller index.

We state for later reference the following result:

The Axiom of Choice and the Well-Ordering Theorem are each equivalent to the proposition that every infinite cardinal is an aleph. (2)

Proof. We pointed out in Section 5 that the Axiom of Choice is equivalent to the Well-Ordering Theorem. In turn, simply comparing the definitions shows that the Well-Ordering Theorem is equivalent to the proposition that every infinite cardinal is an aleph. ■

7. TRICHOTOMY AND THE AXIOM OF CHOICE. This section and the next derive the Axiom of Choice from certain propositions. Obviously, we do not assume this axiom in the discussion. The results needed along the way would be trivial in the presence of the axiom, but in its absence, some of the proofs will be a bit complicated. In particular, the proofs of Theorem 1 and Lemma 2 are a little tricky—while the ideas themselves are elementary, keeping track of the details can be a challenge.

Theorem 1 (Hartogs-Sierpiński). *To each infinite cardinal* $\mathfrak{m}$ *is associated an aleph* $\aleph(\mathfrak{m})$ *satisfying the relations*

$$\aleph(\mathfrak{m}) \not\leq \mathfrak{m} \tag{3}$$

and

$$\aleph(\mathfrak{m}) \leq 2^{2^{2^{\mathfrak{m}}}}. \tag{4}$$

Hartogs's results were (3) and its corollary (stated following the proof of the theorem), together with Theorem 2. They were published in [**5**]. Our proof of Theorem 1 is based on Sierpiński's account in [**9**, pp. 410–412, Theorem 1 and Corollary].

Proof of Theorem 1. Let $\mathfrak{m}$ be an infinite cardinal, and let M be a set of cardinal $\mathfrak{m}$. Since 2^M is the set of all subsets of M, a member of 2^M is a subset of M and a subset N of 2^M is a set of subsets of M. Now, it may happen that the members of N are well ordered by set inclusion. Let W denote the set of *all* subsets N of 2^M whose members are well ordered by set inclusion (as subsets of M). Since W is a set of subsets of 2^M, $W \subset 2^{2^M}$.

Each member of W is a well-ordered collection of sets. We may therefore partition W into similarity classes. Let E denote the set of these classes. Now to each such class we can associate the ordinal common to all its members and interpret E as the set of these ordinals. Then E is well ordered in the natural way.

We now show that $|E| \not\leq |M|$. Suppose on the contrary that $|E| \leq |M|$. Then E is equipotent with some subset M_1 of M. The one-to-one correspondence between E and M_1 defines a well ordering of M_1 similar to that of E. Let S denote the set of segments of M_1. Then

$$\operatorname{ord} S = \operatorname{ord} M_1 = \operatorname{ord} E, \tag{5}$$

"ord X" denoting the ordinal of X. Since S is a set of subsets of M well ordered by set inclusion, it belongs to W; hence S belongs to some similarity class K in the collection E. The segment of E determined by K is then similar to S. But then by (5) this segment of E is similar to E itself, which we know is not possible. Accordingly, we must have $|E| \not\leq |M|$.

Observe next that, since M is infinite, E must be infinite as well; otherwise we would have $|E| < |M|$, which has just been ruled out. Thus E is an infinite well-ordered set, so $|E|$ is an aleph; we define $\aleph(\mathfrak{m})$ to be this aleph. Recalling that $|M| = \mathfrak{m}$, we see that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$, which is (3).

Finally, because E is a set of subsets of W, we have $E \subset 2^W$. Recalling that $W \subset 2^{2^M}$, it follows that $E \subset 2^{2^{2^M}}$. In terms of cardinals, $\aleph(\mathfrak{m}) \leq 2^{2^{2^{\mathfrak{m}}}}$, which is (4). ∎

From (3), we quickly obtain the celebrated results of Hartogs announced in the introduction. The first of these is:

Corollary. *No cardinal is greater than all the alephs.*

Indeed, by the theorem, for every infinite cardinal there is an aleph that it is not less than it.

Hartogs's principal result is:

Theorem 2. *Trichotomy is equivalent to the Axiom of Choice and to the Well-Ordering Theorem.*

Proof. First we derive Trichotomy from the other two propositions. If either one (and hence both) hold, then by (2) every infinite cardinal is an aleph. Since any two alephs are comparable, we conclude that any two cardinals are comparable—which is Trichotomy. Conversely, assume Trichotomy, and consider any infinite cardinal $\mathfrak{m}$. (Now comes the *coup de grace*.) From Theorem 1, $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$. Hence by Trichotomy, $\aleph(\mathfrak{m}) > \mathfrak{m}$. Thus $\mathfrak{m}$ is less than some aleph and therefore is itself an aleph. Since $\mathfrak{m}$ was arbitrary, all infinite cardinals are alephs. By (2), this implies the Axiom of Choice and the Well-Ordering Theorem. ∎

8. THE GENERAL CONTINUUM HYPOTHESIS AND THE AXIOM OF CHOICE. Recall that the General Continuum Hypothesis asserts: *for every infinite cardinal $\mathfrak{m}$, there is no cardinal $\mathfrak{n}$ satisfying $\mathfrak{m} < \mathfrak{n} < 2^{\mathfrak{m}}$.* Sierpiński was the first to establish a connection between the General Continuum Hypothesis and the Axiom of Choice [**8**]. Many years earlier, in [**6**], Tarski had announced the same implication (Theorem 3 following) but without supplying even a hint of a proof.

Theorem 3. *The General Continuum Hypothesis implies the Axiom of Choice.*

Assuming the General Continuum Hypothesis, we will derive the Axiom of Choice in its equivalent version that every infinite cardinal is an aleph. First we establish three lemmas.

Lemma 1. *If $\mathfrak{p} \geq \aleph_0$, then $2^{\mathfrak{p}} + \mathfrak{p} = 2 \cdot 2^{\mathfrak{p}} = 2^{\mathfrak{p}}$.*

Proof. We know from (1) that $1 + \mathfrak{p} = \mathfrak{p}$. Hence

$$2^{\mathfrak{p}} \leq 2^{\mathfrak{p}} + \mathfrak{p} \leq 2 \cdot 2^{\mathfrak{p}} = 2^{1+\mathfrak{p}} = 2^{\mathfrak{p}},$$

and the result follows. ∎

Lemma 2. *If $\mathfrak{a}$ and $\mathfrak{p}$ are cardinals satisfying $2\mathfrak{p} = \mathfrak{p}$ and $\mathfrak{a} + \mathfrak{p} = 2^{\mathfrak{p}}$, then $\mathfrak{a} \geq 2^{\mathfrak{p}}$.*

Proof. Let P and P' be disjoint sets of power $\mathfrak{p}$, and let A be a set of power $\mathfrak{a}$ disjoint from P. Then

$$|A \cup P| = \mathfrak{a} + \mathfrak{p} = 2^{\mathfrak{p}} = 2^{\mathfrak{p}+\mathfrak{p}} = |2^{P \cup P'}|.$$

Here the first equality uses the fact that $A \cap P = \varnothing$ and the last one that $P \cap P' = \varnothing$. Let f be a one-to-one mapping of $A \cup P$ onto $2^{P \cup P'}$. For E a subset of P', let E^* consist of the set E plus those elements x of P that do not belong to the set $f(x)$. Then $E^* \subset P \cup P'$, and for all x in P, $x \in E^*$ if and only if $x \notin f(x)$—in short, for all x in P, $E^* \neq f(x)$. It follows that $E^* = f(y)$ for some y in A. Now E is any one of the $2^{\mathfrak{p}}$ subsets of P', and the correspondence between E and E^* is one-to-one.

Therefore there are 2^p sets of the form E^*, hence 2^p corresponding elements y in A. Consequently, A has at least 2^p elements. Thus $\mathfrak{a} \geq 2^p$. ∎

Now consider an arbitrary infinite cardinal $\mathfrak{n}$. We will establish that $\mathfrak{n}$ is an aleph. To do this, we define

$$\mathfrak{m} = 2^{\aleph_0 + \mathfrak{n}}$$

and produce an aleph that majorizes $\mathfrak{m}$. It then follows that both $\mathfrak{m}$ and the smaller cardinal $\mathfrak{n}$ are alephs.

Introduce the abbreviations

$$\mathfrak{p}_0 = \mathfrak{m}, \quad \mathfrak{p}_1 = 2^{\mathfrak{p}_0} = 2^{\mathfrak{m}}, \quad \mathfrak{p}_2 = 2^{\mathfrak{p}_1} = 2^{2^{\mathfrak{m}}}, \quad \mathfrak{p}_3 = 2^{\mathfrak{p}_2} = 2^{2^{2^{\mathfrak{m}}}}. \tag{6}$$

These $\mathfrak{p}_n$ all satisfy $\mathfrak{p}_n \geq \mathfrak{m} \geq \aleph_0$ and thus by Lemma 1 satisfy

$$2 \cdot 2^{\mathfrak{p}_n} = 2^{\mathfrak{p}_n}. \tag{7}$$

The nub of the proof of Theorem 3 is our final lemma, in which we recall Hartogs's aleph $\aleph(\mathfrak{m})$ in preparation for its central role.

Lemma 3. *For $n = 1, 2,$ or 3, if*

$$\aleph(\mathfrak{m}) \leq \mathfrak{p}_n, \tag{8}$$

then either $\mathfrak{m}$ is an aleph or

$$\aleph(\mathfrak{m}) \leq \mathfrak{p}_{n-1}. \tag{9}$$

Proof. Using (8), (6), and (7), we have

$$\mathfrak{p}_{n-1} \leq \aleph(\mathfrak{m}) + \mathfrak{p}_{n-1} \leq \mathfrak{p}_n + \mathfrak{p}_n = \mathfrak{p}_n = 2^{\mathfrak{p}_{n-1}};$$

briefly,

$$\mathfrak{p}_{n-1} \leq \aleph(\mathfrak{m}) + \mathfrak{p}_{n-1} \leq 2^{\mathfrak{p}_{n-1}}.$$

By the General Continuum Hypothesis, one of the two weak inequalities must be an equality. If

$$\aleph(\mathfrak{m}) + \mathfrak{p}_{n-1} = 2^{\mathfrak{p}_{n-1}},$$

then Lemma 2 (with $\mathfrak{a} = \aleph(\mathfrak{m})$, $\mathfrak{p} = \mathfrak{p}_{n-1}$) and (6) yield

$$\aleph(\mathfrak{m}) \geq 2^{\mathfrak{p}_{n-1}} \geq \mathfrak{m},$$

whence $\mathfrak{m}$ is an aleph. If, on the other hand,

$$\aleph(\mathfrak{m}) + \mathfrak{p}_{n-1} = \mathfrak{p}_{n-1},$$

then

$$\aleph(\mathfrak{m}) \leq \mathfrak{p}_{n-1},$$

which is (9). ∎

Proof of Theorem 3. Theorem 1 tells us that $\aleph(\mathfrak{m}) \le \mathfrak{p}_3$, i.e., (9) holds for $n = 3$. By Lemma 3, either $\mathfrak{m}$ is an aleph or (9) holds for $n = 2$. Iterating, we conclude that either $\mathfrak{m}$ is an aleph or (9) holds for $n = 1$. Reiterating, either $\mathfrak{m}$ is an aleph or (9) holds for $n = 0$. But this last alternative is not possible, as it states that

$$\aleph(\mathfrak{m}) \le \mathfrak{p}_0 = \mathfrak{m},$$

contradicting Hartogs's theorem (3). It follows that $\mathfrak{m}$ is an aleph. ∎

REFERENCES

1. G. Cantor, Über eine Eigenschaft des Inbegriffes aller reelen algebraischen Zahlen, *J. Reine Angew. Math.* **77** (1874) 258–262.
2. G. Cantor, Über eine elementare Frage der Mannigfaltigkeitslehre, *Jahresber. Deutsch. Math. Verein.* **I** (1890–91) 75–78.
3. P. Cohen, The independence of the continuum hypothesis, *Proc. Nat. Acad. Sci. USA* **50** (1963) 1143–1148.
4. K. Gödel, The consistency of the axiom of choice and of the generalized continuum hypothesis, *Proc. Nat. Acad. Sci. USA* **24** (1938) 556–557.
5. F. Hartogs, Über das Problem der Wohlordnung, *Math. Ann.* **76** (1915) 438–443.
6. A. Lindenbaum et A. Tarski, Communication sur les recherches de la théorie des ensembles, *C. R. Soc. Sc. et Lett. de Varsovie, Cl, III* **19** (1926) 299–330.
7. G. Peano, *Rend. Circ. Mat. Palermo* **21** (1906) 860.
8. W. Sierpiński, L'hypothèse généralisée du continu et l'axiome du choix, *Fund. Math.* **34** (1947) 1–5.
9. W. Sierpiński, *Cardinal and Ordinal Numbers*, 2nd ed., Monografie Matematyczne **34**, PWN-Polish Scientific Publishers, Warsaw, 1965.
10. A. Tarski, Quelques théorèmes sur les Alephs, *Fund. Math.* **7** (1925) 1–14.
11. E. Zermelo, *Revue de Metaph. et de Morale* **14** (1906) 314; *Math. Ann.* **65** (1908) 271.
12. E. Zermelo, Beweis dass jede Menge wohlgeordnet werden kann, *Math. Ann.* **59** (1904) 514–516.

LEONARD GILLMAN held a piano fellowship at the Juilliard Graduate School for five years before spending nine years in Naval Operations Research and then completing his Ph.D. at Columbia University in transfinite numbers under the direction of E. R. Lorch and the unofficial direction of Alfred Tarski (UC Berkeley). He then taught at Purdue, Rochester, and Texas for a total of thirty-five years (including two on leave at the Institute for Advanced Study), retiring in 1987. He is the author of two MAA booklets, *You'll Need Math* (1967), for high school students, and *Writing Mathematics Well* (1987), for authors; coauthor with R. H. McDowell of a calculus text (1973, 1978), and coauthor with Meyer Jerison of *Rings of Continuous Functions* (1960, 1976), a graduate text. He was MAA Treasurer for thirteen years (1973–86) and President for the canonical two (1987–89). He received a Lester R. Ford award for his paper "An axiomatic approach to the integral" in this MONTHLY (January 1993, pp. 16–25) and the 1999 Gung-Hu Award for Distinguished Service to Mathematics. He has performed at the piano at five national meetings and several MAA section meetings.
Department of Mathematics, The University of Texas at Austin, Austin, TX 78712
len@math.utexas.edu