VII : The Axiom of Choice and related properties

Near the end of Section **VI.4** we listed several basic questions about transfinite cardinal numbers, and we shall restate them here for the sake of convenience:

1. Is the partial ordering of cardinal numbers a linear ordering?
2. Is $\aleph_0$ the smallest transfinite cardinal number?
3. If **A** is an infinite set, does it follow that the idempotent identities $|A| \cdot |A| = |A|$ and $|A| + |A| = |A|$ always hold?
4. If there is a surjection from **A** to **B,** does it follow that $|B| \leq |A|$?
5. Given a cardinal number α, is there a unique minimal cardinal number β such that $\beta > \alpha$?

One purpose of this section is to discuss the issues that arise when one studies such questions, and the overall answer may be summarized as follows:

> *If certain valid constructions and operations for subsets of the natural numbers* **N** *can be extended to arbitrary sets, then the answers to the questions stated above (and several others) are all affirmative.*

The good news in this statement is that it generates optimism about finding positive answers to the sorts of questions we have described. However, there is also some bad news. The "valid constructions and operations" for subsets of **N** can be described very explicitly, but for arbitrary sets the best we can expect are ***nonconstructive existence principles***. This is particularly well illustrated by the following attempt to prove the answer to the fourth question is yes:

> Suppose that **f** is a surjection from **A** to **B.** Then for each $b \in B$ we know that the inverse image is $f^{-1}[\{b\}]$ is nonempty. For each **b** pick some element $g(b) \in A$ in this inverse image. Since **g(b)** lies in $f^{-1}[\{b\}]$ it follows that $f(g(b)) = b$ for all **b** and hence the composite **fg** is the identity on **B.** But now **g** must be $1-1$ by one of the exercises for Section **IV.3,** and therefore we have $|B| \leq |A|$.

There are two important points to notice about this:

1. The ideal of picking an element out of the set has a great deal of intuitive appeal.
2. On the other hand, there is no information on exactly how one should pick an element from the given nonempty subset. — In contrast, if we are dealing with subsets of **N** then there is a simple explicit method for making such choices; one simply takes the first element of a given nonempty subset.

Taken together, these suggest that we may need to assume it is possible to pick out "possibly random" elements from nonempty subsets in some unspecified manner. During the first few decades of the 20th century mathematicians studied this question extensively. The first phase of this work produced several logically equivalent versions of the crucial assumption described above, the second sows that such the logical consistence of set theory is not compromised if one makes such assumptions, and the third shows that one has acceptable models for set theory in which such assumptions are true and equally acceptable models in which they are false. Since affirmative answers to the given questions (and others) are convenient for many purposes, most mathematicians are willing to make the sorts of assumptions need to justify the informal argument given above, sometimes reluctantly but generally with few reservations.

We shall begin by motivating and stating three standard ways of formulating the nonconstructive existence principle that arises in connection with the questions above. This is done in Sections 1 and 2, with equivalence proofs in Section 3; a reader who prefers to skip the details of the latter may do so without loss of continuity. Section 4 contains answers to those questions in the list which are not answered in Section 2. The final two sections are commentaries on two related issues. We have noted that assuming the nonconstructive existence principles does not compromise the logical soundness of set theory, and Section 5 explains the situation in a little more detail, and it also discusses the "acceptable models" mentioned above. Finally, Section 6 deals with a question dealing with Cantor's original work: All the specific infinite subsets of the real numbers that arose in his studies either had the same cardinal number as the integers or the real numbers, and Cantor's ***Continuum Hypothesis*** states that there are no cardinal numbers α such that $|\mathbf{N}| < \alpha < |\mathbf{R}|$. It turns out that the formal status of this assumption (and an associated ***Generalized Continuum Hypothesis***) is completely analogous to the nonconstructive existence hypothesis discussed in previous sections.

VII.1 : Nonconstructive existence principles

(Halmos, §§ 15 – 17; Lipschutz, §§ 5.9, 9.1 – 9.4)

We have repeatedly noted that the initial and most important motivation for set theory came from questions about infinite sets. As research on such sets progressed during the late nineteenth and early twentieth century, it eventually became evident that most of the underlying principles involved constructing new sets from old ones and the existence of the set of natural numbers. However, it also became clear that some results in set theory depended upon some nonconstructive existence principles. In particular, when mathematicians attempted to answer questions like 1 – 5 at the beginning of this unit, their arguments used ideas that seemed fairly reasonable but could not be carried out explicitly. In the introduction to this unit, we discussed the role of nonconstructive existence principles in analyzing Question 4. Here we shall begin with a similar analysis of Question 2 from the list. We would like to prove the following result.

<u>**Theorem 1.**</u> *If* **A** *is an infinite set, then* **A** *has a countably infinite subset and hence we have* $\aleph_0 \leq |\mathbf{A}|$.

It will follow from Theorem 1 that $\aleph_0$ ***is the unique smallest infinite cardinal number.***

In Section **V.2** we proved a related fact; namely, if A is countably infinite and B is an infinite subset of **A,** then $|B| = \aleph_0$. One important step in the proof relied on the existence of a well – ordering on the standard countably infinite set **N;** using the **1 – 1** correspondence between **N** and **A,** it follows that **A** also has a well – ordering if it is countably infinite.

The preceding discussion suggests that ***if an infinite set*** **A** ***has a well – ordering, then perhaps one can generalize the previous argument for countably infinite sets*** **A** ***to cover other infinite sets as well.*** The idea that every set has a well – ordering originally appeared in Cantor's work; he accepted the statement as true but noted that a convincing argument (or a postulate) was needed. Here is a formal statement:

Well – Ordering Principle. *For every nonempty set* **A**, *there is a* ***well-ordering*** *of* **A** *(recall that this is a linear ordering such that each nonempty subset* **B** *of* **A** *has a least element).*

Proof that the Well – Ordering Principle implies Theorem 1. The basic idea is again the same. One defines a **1 – 1** function from **N** to **A** recursively as follows: Let **f(0)** be the first element of A, and if **f(x)** is defined for $x < n$ then let **f(n)** be the first element not in the set $\{ f(0), \dots, f(n-1) \}$. Such a first element always exists, for the fact that **A** is infinite implies that $A - \{ f(0), \dots, f(n-1) \}$ is nonempty.■

In order to illustrate the significance of Theorem 1, we shall use it to prove some generalizations of other results from Sections **VI.3** and **VI.4.**

Theorem 2. *If* **A** *is a countable set and* **B** *is an infinite set, then* $|A| + |B| = |B|$.

Corollary 3. (Dedekind – C. S. Peirce) *A set is infinite if and only if it can be put into a* **1 – 1** *correspondence with a proper subset of itself*.■

Proof that Theorem 1 implies Theorem 2. By Theorem 1 we know that **B** contains a countably infinite subset **C.** Let $D = B - C$. It follows immediately that

$$|B| = |C| + |D| = \aleph_0 + |D|$$

and therefore we have

$$|A| + |B| = |A| + |C| + |D| = |A| + \aleph_0 + |D|.$$

The results of Section **VI.4** imply that $\aleph_0 = |A| + \aleph_0$, and if we combine this with the two lines of equations displayed above we conclude that $|A| + |B| = |B|$, as required.■

Here is another important implication of the Well – Ordering Principle for transfinite cardinal numbers. Given the simplicity of the statement and its obvious validity for countable cardinals, it is somewhat surprising that all known proofs use the Well – Ordering Principle or some equivalent statement.

Theorem 4. *If* **A** *and* **B** *are sets, then either* $|A| \leq |B|$ *or* $|B| \leq |A|$.

Informally, this means that the cardinalities of sets are linearly ordered.

Proof. Choose well – orderings for **A** and **B .** The results of Section **VI.6** then show that either **A** is in order – preserving **1 – 1** correspondence with a subset of **B** or vice versa.■

Although Cantor regarded the Well – Ordering Principle as a **"**fundamental principle of thought**,"** one disadvantage of assuming this is that the result is difficult to illustrate by means of nontrivial examples. In particular, ***no one has ever constructed a well – ordering of the real numbers*****,** and most if not all mathematicians find it very difficult to imagine how one might explicitly construct such a relation.

There are many equivalent ways of formulating set – theoretic assumptions that are logically equivalent to the Well – Ordering Principle. Perhaps the most widely used in the development of set theory is the following, which was introduced by E. Zermelo as an **"**unobjectionable logical principle**."**

AXIOM OF CHOICE. *If* **A** *is a nonempty set and* $\mathbf{P_+(A)}$ *denotes the set of all nonempty subsets of* **A,** *there is a function* $\mathbf{f : P_+(A) \to A}$ *such that* $\mathbf{f(B) \in B}$ *for every nonempty subset* $\mathbf{B \subset A}$*.*

A function of the type described in the conclusion is often called a ***choice function*** on the nonempty subsets of **A.**

Most mathematicians subjectively regard this statement as far more plausible than the Well – Ordering Principle, but as noted below (and in Section 3) ***the two statements are in fact logically equivalent*****.** Both the Well – Ordering Principle and the Axiom of Choice are nonconstructive existence statements.

The Axiom of Choice is precisely what we need to justify the argument sketched in the introduction to prove the following result:

Theorem 5. *Suppose that* **A** *is a set and* $\mathbf{f : A \to B}$ *is a surjection. Then* $\mathbf{|B| \leq |A|}$**.**

Proof that the Axiom of Choice implies Theorem 5. Once again the basic idea is similar to the corresponding proof in the previous section. Let $\mathbf{g : P_+(A) \to A}$ be a choice function for the nonempty subsets of **A.** Define a function $\mathbf{h : B \to A}$ by the formula.

$$\mathbf{h(b) \;=\; g\left(f^{-1}\left[\{\,b\,\}\right]\right)}\,.$$

Then the choice function condition $\mathbf{h(b) = f^{-1}[\{\,b\,\}]}$ implies that $\mathbf{f\,h(b) = b}$**.** The theorem will follow if we can show that **h** is a **1 – 1** mapping., and the latter follows because $\mathbf{h(x) = h(y)}$ implies $\mathbf{x = f\,h(x) = f\,h(y) = y}$**.**■

Equivalent statements

For some time there was uncertainty whether the Axiom of Choice, or some equivalent statement, should be included in the axioms for set theory. In an effort to understand the situation more clearly, many statements equivalent to the Axiom of Choice were introduced. Each had its own advantages and disadvantages. The sites listed below give 27 different statements that play a significant role in higher mathematics and are logically equivalent to the axiom of choice:

http://www.math.vanderbilt.edu/~schectex/ccc/excerpts/equivac1.gif

http://www.math.vanderbilt.edu/~schectex/ccc/excerpts/equivac2.gif

A full discussion of these equivalent statements is beyond the scope of these notes, but we shall mention one particularly important and frequently used example.

“Zorn’s Lemma.” *If* **A** *is a partially ordered set in which linearly ordered subsets have upper bounds, then* **A** *has a maximal element.*

Zorn's lemma was first discovered by K. Kuratowski (1896 – 1980) and independently a decade later by M. Zorn (1906 – 1993); it is also sometimes known as the Kuratowski – Zorn Lemma. This statement is arguably the most useful of all the statements that are logically equivalent to the Axiom of Choice for reasons to be discussed in Section 2.

Issues for further consideration

There are several points that arise naturally in connection with the three nonconstructive existence statements (the Well – Ordering Principle, the Axiom of Choice and Zorn’s Lemma) that we have formulated.

1. How does one show that the three nonconstructive existence principles are logically equivalent?
2. Is there a simple example to illustrate the uses of Zorn’s Lemma?
3. What sorts of logical problems, if any, arise if one assumes the three statements we have introduced?
4. To what extent are mathematicians willing to accept these statements?

We shall address the first question in Section 3 and the second in Section 2. A detailed discussion of the last two questions appears in Section 5, but for the time being we note that any logical problems that might exist in set theory are present regardless of whether or not one assumes the three nonconstructive existence statements we have introduced in this section; if logical difficulties exist under the assumption of these statements, then by results of K. Gödel there are already logical difficulties even if one does not make these assumptions. Also, the general (but not unanimous) acceptance of such statements in present day mathematics is reflected by our extensive discussion of them in these notes.

VII.2 : Extending partial orderings

(Lipschutz, § 7.6)

In the previous section we made no attempt to motivate Zorn's Lemma, but we shall try to do so here with an example illustrating its use in mathematics. The following type of problem is standard in discrete mathematics courses:

<u>Problem.</u> *Suppose that* **A** *is a finite set, and let* $\boldsymbol{P} \subset \mathbf{A} \times \mathbf{A}$ *be a partial ordering. Is there a linear ordering* $\boldsymbol{Q} \subset \mathbf{A} \times \mathbf{A}$ *such that* $\boldsymbol{P} \subset \boldsymbol{Q}$**?**

The existence of such linear orderings is important for practical purposes. Suppose one has a list **A** of things to be completed, with requirements that certain items on the list must be finished before others. These requirements correspond to a partial ordering ***P*** of the items on the list, and finding a linear ordering ***Q*** containing ***P*** then puts the items into a linear sequence in which they can be completed. An example is described in one of the exercises for this section.

It turns out that one can always find a linear ordering ***Q*** which solves the problem stated above, and this is essentially worked out in Lipschutz using equivalent language (the concept is called ***consistent enumeration*** in Lipschutz). Specifically, given a partial ordering ***P*** on a finite set **A** with **n** elements, Theorem **7.1** on page 172 of Lipschutz proves the existence of a strictly increasing function **f** from the set **A** to $\{1, \dots, n\}$; the proof is given in Problem **7.17** on page 187(also see pages 195 – 196)**.** If we define a binary relation ***Q*** on **A** by the rule $x\, Q\, y$ if and only if $f(x) \leq f(y)$, then it is a routine exercise to check that ***Q*** is a linear ordering which contains ***P*.**

We shall use Zorn's Lemma to prove that one can find similar linear orderings even if the set **A** is not finite.

<u>Theorem 1.</u> *Let* **A** *be a set, and let* $\boldsymbol{P} \subset \mathbf{A} \times \mathbf{A}$ *be a partial ordering. Then there is a linear ordering* $\boldsymbol{Q} \subset \mathbf{A} \times \mathbf{A}$ *such that* $\boldsymbol{P} \subset \boldsymbol{Q}$**.**

We frequently say that ***Q*** is a ***compatible linear ordering*** or ***Q*** <u>is compatible with</u> ***P*.**

As noted above, a result of this type is useful for many purposes. For example, if **X** is a finite set and **A** is a family of subsets of **X,** then sometimes one wants prove a fact about the elements of **A** by mathematical induction, where **A** is linearly ordered such that for each pair of elements **B, C** in **A** such that $B \subset C$ we also have $B < C$.

The nonconstructive nature of Theorem 1 is illustrated by one simple fact: A compatible linear ordering for the set **P(N)** of subsets of the natural numbers (ordered by inclusion) has not been explicitly constructed. In contrast, given an arbitrary partial ordering on a finite set, one can use the proof in Lipschutz to construct an explicit compatible linear ordering.

***<u>Proof of Theorem</u>* <u>1. (∗∗)</u>** We follow the approach outlined above, first showing that there is a maximal partial ordering containing the given one and then showing that such a maximal partial ordering must be a linear ordering.

Let **C** be the collection of all partial orderings of **A** that contain ***P*.** Then **C** is partially ordered by set – theoretic inclusion. Let **D** be a subset of **C** that is linearly ordered by inclusion. If we can show that **D** has an upper bound in **C,** then Zorn's Lemma will imply that **C** has a maximal element.

Denote the elements of **D** by $\boldsymbol{Q}_{\mathbf{x}}$ where s runs through some indexing set **X,** and let ***Q*** be the union of all the sets $\boldsymbol{Q}_{\mathbf{x}}$**.** Clearly ***Q*** contains ***P*** since each $\boldsymbol{Q}_{\mathbf{x}}$ does; we would like to show that ***Q*** is also a partial ordering. The relation ***Q*** is reflexive because ***Q*** contains ***P*** and ***P*** is reflexive. To verify the relation ***Q*** is asymmetric, suppose that both **(a, b)** and **(b, a)** belong to ***Q*.** Then there are partial orderings $\boldsymbol{Q}_{\mathbf{x}}$ and $\boldsymbol{Q}_{\mathbf{y}}$ such that **(a, b)** belongs to $\boldsymbol{Q}_{\mathbf{x}}$ and **(b, a)** belongs to $\boldsymbol{Q}_{\mathbf{y}}$**.** Since **D** is linearly ordered by inclusion it follows that one of $\boldsymbol{Q}_{\mathbf{x}}$ and $\boldsymbol{Q}_{\mathbf{y}}$ contains the other. If $\boldsymbol{Q}_{\mathbf{z}}$ is the larger relation, then both **(a, b)** and **(b, a)** belong to $\boldsymbol{Q}_{\mathbf{z}}$**,** and since the latter is a partial ordering this means that **a = b.** Finally, suppose that both **(a, b)** and **(b, c)** belong to ***Q*.** Then there are partial orderings $\boldsymbol{Q}_{\mathbf{x}}$ and $\boldsymbol{Q}_{\mathbf{y}}$ such that **(a, b)** belongs to $\boldsymbol{Q}_{\mathbf{x}}$ and **(b, c)** belongs to $\boldsymbol{Q}_{\mathbf{y}}$**.** Since **D** is linearly ordered by inclusion it follows that one of $\boldsymbol{Q}_{\mathbf{x}}$ and $\boldsymbol{Q}_{\mathbf{y}}$ contains the other. If $\boldsymbol{Q}_{\mathbf{z}}$ is the larger relation, then both **(a, b)** and **(b, c)** belong to $\boldsymbol{Q}_{\mathbf{y}}$**,** and since the latter is a partial ordering this means that **(a, c)** belongs to $\boldsymbol{Q}_{\mathbf{z}}$**,** which is contained in ***Q*.** Therefore ***Q*** is a partial ordering. By construction, it is an upper bound for the elements of **D,** and thus Zorn's lemma implies that **C** must have a maximal element.■

The second part of the proof of the theorem is contained in the following result.

<u>Proposition 2.</u> *Let* **A** *be a set, and let* ***P*** $\subset$ **A** × **A** *be a maximal partial ordering. Then* ***P*** *is a linear ordering***.**

<u>Proof.</u>* <u>(∗∗∗)</u>** Suppose that ***P is not a linear ordering. Then we can find **x, y** in **A** such that neither **(x, y)** nor **(y, x)** lies in ***P*.** We shall obtain a contradiction by expanding ***P*** to a partial ordering that contains **(x, y).** In order to express the argument in familiar notation we shall write $\mathbf{u} \leq_{\boldsymbol{P}} \mathbf{v}$ to signify that **(u, v)** lies in ***P*.**

Define a new binary relation ***Q*** such that **(u, v)** lies in ***Q*** if and only if either $\mathbf{u} \leq_{\boldsymbol{P}} \mathbf{v}$ or else both $\mathbf{u} \leq_{\boldsymbol{P}} \mathbf{x}$ and $\mathbf{y} \leq_{\boldsymbol{P}} \mathbf{v}$**.** The proof of the proposition then reduces to showing that ***Q*** is a partial ordering.

*<u>The relation **Q** is reflexive.</u>* Since ***P*** is a partial ordering, for each $\mathbf{a} \in \mathbf{A}$ we know that $(a, a) \in \boldsymbol{P} \subset \boldsymbol{Q}$**.**

*<u>The relation **Q** is transitive.</u>* Suppose that $\mathbf{(a, b)} \in \boldsymbol{Q}$ and $\mathbf{(b, c)} \in \boldsymbol{Q}$*.* Then there are two options for each of the ordered pairs in the preceding sentence and thus a total of four separate cases to consider:

1. We have $\mathbf{a} \leq_{\boldsymbol{P}} \mathbf{b}$ together with $\mathbf{b} \leq_{\boldsymbol{P}} \mathbf{c}$**.**
2. We have $\mathbf{a} \leq_{\boldsymbol{P}} \mathbf{b}$ together with both $\mathbf{b} \leq_{\boldsymbol{P}} \mathbf{x}$ and $\mathbf{y} \leq_{\boldsymbol{P}} \mathbf{c}$**.**

3. We have both **a** $\leq_P$ **x** and **y** $\leq_P$ **b** together with **b** $\leq_P$ **c.**
4. We have both **a** $\leq_P$ **x** and **y** $\leq_P$ **b** together with both **b** $\leq_P$ **x** and **y** $\leq_P$ **c.**

In the first case, since ***P*** is a partial ordering we have **a** $\leq_P$ **c,** so that **(a, c)** $\in$ ***Q.*** In the second case, since ***P*** is a partial ordering we have **a** $\leq_P$ **x,** and therefore **(a, c)** satisfies the second criterion to be an element of ***Q.*** In the third case, since ***P*** is a partial ordering we have **y** $\leq_P$ **c,** and therefore **(a, c)** satisfies the second criterion to be an element of ***Q.*** Finally, in the fourth case since ***P*** is a partial ordering the middle two conditions imply that **y** $\leq_P$ **x,** which contradicts our original hypothesis that neither of the relations **x** $\leq_P$ **y** or **y** $\leq_P$ **x** is valid. Therefore the fourth case is impossible, and this completes the proof of transitivity.

<u>*The relation **Q** is antisymmetric.*</u> Suppose that **(a, b)** $\in$ ***Q*** and **(b, a)** $\in$ ***Q.*** Then we have the same four cases as in the proof of transitivity, the only difference being that one must replace **c** by **a** in each case. In the first case, since ***P*** is a partial ordering we must have **a** = **b.** In all the remaining cases, since ***P*** is a partial ordering the given conditions combine to imply **y** $\leq_P$ **x,** which contradicts the assumption on ***Q.*** Thus only the first case is possible, and this completes the proof that the relation ***Q*** is antisymmetric.■

As noted in Section 1, for many decades mathematicians have generally found Zorn's Lemma to be particulary effective for proving theorems that depend upon the Axiom of Choice, partly because most of these results translate easily into the existence of a maximal object of some sort. From this perspective, the proofs usually have two distinct parts:

1. Showing that a maximal object of some type must exist using Zorn's Lemma.
2. Showing that such maximal objects must have certain desired properties.

Here is another application of Zorn's Lemma to partially ordered sets; as indicated by the name, this statement was formulated by F. Hausdorff (1868 – 1942) and in fact was known before Zorn's Lemma was discovered.

<u>**Theorem 3. (Hausdorff Maximal Principle.)**</u> *Every nonempty partially ordered set contains a maximal linearly ordered subset.*

<u>***Proof.***</u> Let **X** be the nonempty partially ordered set, let ***R*** be the partial ordering and consider the family **Y** of all subsets **A** of **X** such that

$$R|A \quad = \quad R \cap A \times A$$

Is a linear ordering on **A,** with the partial ordering of **Y** given by set – theoretic inclusion. The family **Y** is nonempty, for if **x** $\in$ **X** then one has the trivial linear ordering

$$\{x\} \times \{x\} \quad = \quad R \cap \left(\{x\} \times \{x\}\right)$$

on the one point subset $\{x\} \subset$ **X.**

Suppose that we have a linearly ordered subfamily of subsets $\mathbf{X_a}$ as above. If we take $\mathbf{W} = \cup_{\mathbf{a}} \mathbf{X_a}$ then we claim that $\boldsymbol{T} = \boldsymbol{R}|\mathbf{W}$ is a linear ordering on **W.** By construction it is a partial ordering, so the only point to prove is the dichotomy property. Suppose now that $\mathbf{x, y} \in \mathbf{W}$. Then one can find **a** and **b** such that $\mathbf{x} \in \mathbf{X_a}$ and $\mathbf{y} \in \mathbf{X_b}$. The linear ordering property implies that one of **a** or **b** is greater than or equal to the other; if **c** denotes this element, then we have $\mathbf{x, y} \in \mathbf{X_c}$. Since the latter set is linearly ordered with respect to

$$\boldsymbol{S}_{\mathbf{c}} = \boldsymbol{R}|\mathbf{X_c}$$

it follows that either $(\mathbf{x, y}) \in \boldsymbol{S}_{\mathbf{c}}$ or $(\mathbf{y, x}) \in \boldsymbol{S}_{\mathbf{c}}$, and since the latter is contained in ***T*** it follows that one of the two pairs must lie in ***T*.** Therefore ***T*** is a linear ordering, and therefore W is an upper bound in **Y** for all of the linearly ordered subsets $\mathbf{X_a}$.

We can now use Zorn's Lemma to conclude that **Y** has a maximal element, which is given by a subset **M** with the linear ordering $\boldsymbol{L} = \boldsymbol{R}|\mathbf{M}$. It follows immediately that **M** is a maximal linearly ordered subset.■

For the sake of completeness we note that ***the Hausdorff Maximal Principle is also logically equivalent to Zorn's Lemma*** (or the Axiom of Choice or the Well – Ordering Principle).

VII.3 : Equivalence proofs

(Halmos, §§ 15 – 20; Lipschutz, §§ 5.9, 9.1 – 9.5, 9.7)

> [From a purely intuitive viewpoint, it appears that] the Axiom of Choice is obviously true, the well-ordering principle [is] obviously false, and who can tell about Zorn's lemma?
>
> J. Bona (1945 –)

Although the Axiom of Choice, the Well – Ordering Principle and Zorn's Lemma are logically equivalent, most mathematicians do not view them as equally easy to accept as assumptions. As indicated in the quotation, the Axiom of Choice seems intuitively easier to believe than the others, while the Well – Ordering Principle is often seen as counter – intuitive and Zorn's Lemma is viewed as too complex for any intuition. Therefore, proofs that these three statements are logically equivalent are not only needed for the sake of logical completeness, for they also provide reassurance that the less intuitive statements are equally valid. The purpose of this section is to give (or at least sketch) the proofs that the three basic statements are logically equivalent. This material will not be used in later sections and may be skipped without loss of continuity. At some points we shall need properties of well – ordered sets that were stated without full proofs in Section **VI.6.**

Proving that the Well – Ordering Principle implies the Axiom of Choice. This is the simplest of all the arguments: Let **A** be a nonempty set, suppose we are give a well – ordering, and let $\mathbf{P}_+(\mathbf{A})$ denote the set of all nonempty subsets of **A.** Define a function $\mathbf{f} : \mathbf{P}_+(\mathbf{A}) \to \mathbf{A}$ such that for every nonempty subset $\mathbf{B} \subset \mathbf{A}$, the image **f(B)** is equal to the ***unique minimal element*** of **B** with respect to the well – ordering. Then by construction we always have $\mathbf{f(B)} \in \mathbf{B}$.■

***Proving that the Axiom of Choice implies the Well – Ordering Principle.* (****)** A fully rigorous proof requires many of the results on ordinals from the previous section as well as a strong version of transfinite recursion. In many ways this is the most difficult implication to prove, so we shall merely outline the argument here.

Let **X** be a set, and let $\mathbf{k} : \mathbf{P}_+(\mathbf{X}) \to \mathbf{X}$ be a choice function. By Hartogs' Theorem there is an ordinal λ such that there is no **1 – 1** mapping from λ to **X.** Define $\mathbf{f} : \lambda \to \mathbf{X} \cup \{\mathbf{X}\}$ recursively as follows for a given $\alpha \in \lambda$; there are two cases depending upon whether or not the set $\mathbf{J}_\alpha = \mathbf{f}\big[[0, \alpha)\big]$ is a proper subset of **X.**

1. If $\mathbf{J}_\alpha$ is a proper subset of **X,** take $\mathbf{f}(\alpha) = \mathbf{k}(\mathbf{X} - \mathbf{J}_\alpha)$.
2. If $\mathbf{J}_\alpha$ is not a proper subset of **X,** take $\mathbf{f}(\alpha) = \mathbf{X}$.

By construction, if $\mathbf{f}(\alpha) \in \mathbf{X}$, then the restriction of **f** to the closed interval $[0, \alpha]$ is **1 – 1.** Furthermore, **f** is **1 – 1** on the inverse image of **X.**

By the choice of λ, we know there is a $\gamma \in \lambda$ such that $\mathbf{f}\,|\,[0, \gamma]$ is not **1 – 1;** let β be the least such ordinal. It then follows that **f** is **1 – 1** on $[0, \beta)$ and $\mathbf{f}(\gamma) = \mathbf{X}$ for $\gamma \geq \beta$. Furthermore, it also follows that **f** defines a **1 – 1** from $[0, \beta)$ to **X.**■

***Proving that the Axiom of Choice and the Well – Ordering Principle imply Zorn'sLemma.* (**)** If Zorn's Lemma is false, then there exists a partially ordered set **X** such that every linearly ordered subset has an upper bound, and for each element of **X** it is possible to find a larger one.

Using Hartogs' Theorem we can find an ordinal λ such that there is no **1 – 1** mapping from λ to **X;** alternatively, we can find λ by taking a well – ordering of the power set **P(X).** We claim it is possible to define a strictly increasing map **f** from λ to **X** by transfinite recursion. If we can do this, we shall have a contradiction because there is no **1 – 1** map from λ to **X.** Let $\mathbf{k} : \mathbf{X} \to \mathbf{P}(\mathbf{X})$ be a choice function.

Define $\mathbf{f}(0_\mathbf{X}) = \mathbf{k}(\mathbf{X})$ to begin the process. Suppose now that we have defined the function on $[0, \alpha)$, and let $\mathbf{J}_\alpha = \mathbf{f}\big[[0, \alpha)\big]$. By hypothesis the latter is a linearly ordered subset of **X** and as such it has an upper bound. Use the choice function **k** to select a particular upper bound $\mathbf{u}(\alpha)$. We are also assuming that **X** has no maximal element so the set of all elements strictly greater than $\mathbf{u}(\alpha)$ is nonempty; use the choice function **k** again to select some $\mathbf{f}(\alpha) > \mathbf{u}(\alpha)$. Since **f** is strictly increasing for $\beta < \alpha$ and $\mathbf{f}(\alpha)$ is greater than every element of $\mathbf{J}_\alpha$ by construction, it follows that **f** is $1-1$ on the closed interval $[0, \alpha]$. This completes the recursive step in the definition of the strictly increasing map $\mathbf{f} : \lambda \rightarrow \mathbf{X}$.

As noted in the second paragraph of the argument, this yields a contradiction. Where is the problem? The construction of **f** relies heavily on the fact that **X** has no maximal element, so this must be false. Thus **X** must have a maximal element, and the existence of such an element is exactly what is needed to prove Zorn's Lemma.■

Proving that Zorn's Lemma implies the Well – Ordering Principle. **(**)** This is a typical example of how Zorn's Lemma is used in mathematics. General comments on this were given in Section 2, so our discussion here will be very brief. The idea is to start with a set **X** and to consider an auxiliary partially ordered set **W** of well – orderings, with $\alpha \leq \beta$ if and only if α corresponds to an initial segment of β. Then one shows that **W** satisfies the hypotheses of Zorn's Lemma and hence has a maximal element. The final step is to check that this maximal element is a well – ordering for the entire set **X.**■

Here are some online references for more information about the Axiom of Choice and related topics:

http://en.wikipedia.org/wiki/Axiom_of_choice

http://www.math.vanderbilt.edu/~schectex/ccc/choice.html

http://planetmath.org/encyclopedia/MultiplicativeAxiom.html

VII.4 : Additional consequences

(Halmos, § 15; Lipschutz, §§ 9.1, 9.7)

In this section we shall complete the discussion of the questions about cardinal numbers that were raised at the beginning of this unit, and we shall also discuss a few other basic mathematical facts which logically depend upon the Axiom of Choice or an equivalent statement. Many other examples arise in virtually all basic graduate level mathematics courses.

Some of the preceding online references contain thorough, but not overwhelming, summaries of basic mathematical results whose proofs require the Axiom of Choice. In this subsection we shall restrict attention to a few that involve material from lower level undergraduate courses in the mathematical sciences or topics previously covered in this course.

The first simple result is essentially a restatement of the definition of a general Cartesian product; in fact, the conclusion of the theorem is the version of the Axiom of Choice stated on page 59 of Halmos, and therefore the theorem implies that our version is equivalent to the version in Halmos.

Theorem 1. (Nontriviality Principle for Products.) *If the Axiom of Choice is true, then a product of any nonempty family* **F** *of nonempty sets is nonempty (we assume that the elements of* **F** *indexed by* **F** *itself).*

Proof. Given a family **F** of sets a choice function defines an element of the product

$$\Pi\{B \mid B \in F\}.$$

In fact, the converse is also true, for a choice function corresponds to an element of the Cartesian product displayed above.■

Consequences for transfinite cardinal numbers

Zorn's Lemma also provides a particularly effective means for proving the following basic property of transfinite cardinals which generalizes an earlier result (Theorem **VI.4.8**) for the first infinite cardinal number $\aleph_0$:

Theorem 2. (Idempotent Laws for infinite cardinals). *If* **A** *is an infinite set, then we have* $|A| + |A| = |A|$ *and* $|A| \cdot |A| = |A|$.

Corollary 3. *If* **A** *and* **B** *are nonempty sets and at least one is infinite, then*

$$|A| + |B| = |A| \cdot |B| = |C|$$

where $|C|$ *is the larger of* $|A|$ *and* $|B|$.

The final portion of this statement relies on the fact that cardinal numbers are linearly ordered, which was established in Theorem **VII.2.4** above. Of course, the corollary is generally (in fact, almost always) false if both **A** and **B** are finite.

Proof that Theorem 2 implies Corollary 3. Without loss of generality, *we might as well assume that* $|A|$ *is the larger of the two cardinal numbers.* If we can prove the result in this case, the proof when $|B|$ is the larger will follow by interchanging the roles of **A** and **B** systematically throughout the argument. Such "without loss of generality" reductions are used frequently in mathematical proofs to simplify the discussion.

Since we are assuming $|A| \geq |B|$, we may combine the conclusion of Theorem 2 with the basic formal properties of cardinal addition and multiplication to conclude that

$$|A| \leq |A| + |B| \leq |A| + |A| = |A|$$

so that $|A| + |A| = |A|$, and similarly

$$|A| \leq |A|\cdot|B| \leq |A|\cdot|A| = |A|$$

so that $|A|\cdot|B| = |A|$.■

Proof of Theorem 2. We begin with the additive identity, both because it is simpler and because it is needed to prove the multiplicative identity. Both arguments are based upon Zorn's Lemma.

Proof that $|A| + |A| = |A|$. — Let U_A be the set of all pairs (B, f) where $B \subset A$ is a nonempty subset and $f : B \amalg B \to B$ is a bijection (1 – 1 correspondence). If we set $(B, f) \leq (C, g)$ if and only if $g(b, n) = f(b, n)$ for $n = 1, 2,$ then routine calculations show that $\leq$ defines a partial ordering on U_A.

The set U_A is nonempty because A contains a countably infinite subset C, and by Theorem VI.4.8 there is a bijection from $C \amalg C$ to C.

Suppose now that we have a linearly ordered subset of U_A whose elements have the form (B_t, f_t), where t lies in some indexing set. For each t let G_t denote the graph of t, let B be the union of the sets B_t, and let G be the union of the graphs G_t. We claim that G is the graph of a bijection from $B \amalg B$ to B. If so, then $(B, f) \geq (B_t, f_t)$ for all t and hence the hypotheses of Zorn's Lemma apply.

Suppose that $z \in B$, and choose t such that $z \in B_t$. Then there is a uniqute $w \in B_t$ such that $(z, w) \in G_t$; we claim there are no other points in G with first coordinate equal to z. If $(z, x) \in G$, then there is some s such that $(z, x) \in G_s$. Choose r so that G_r is the larger of G_s and G_t; then (z, w) and $(z, x) \in G_r$ imply $w = x$ because G_r is the graph of a function. Thus G is the graph of a function. What is the domain of G? If $(z, w) \in G$, then $z \in B_t \amalg B_t \subset B \amalg B$ for some t, and conversely if $z \in B \amalg B$ then for some t we have $z \in B_t \amalg B_t$, and consequently there is an ordered pair of the form $(z, w) \in G_t \subset G$.

Next, we need to show that the function f with graph G is a bijection. If $f(x) = f(y)$ then as before one can find a single set t such that $x, y \in B_t \subset B \amalg B$ for some t, and conversely if $z \in B \amalg B$ then for some t we have $z \in B_t \amalg B_t$. Then we have

$$f_t(x) = f(x) = f(y) = f_t(y)$$

and since f_t is 1 – 1 it follows that $x = y$. Also, if $z \in B$, choose t such that $z \in B_t$, so that $z = f_t(w) = f(w)$ for some w and hence f is onto. This completes the proof that linearly ordered subsets of U_A have maximal elements.

By Zorn's Lemma there is a maximal element (M, h) of U_A, and by construction we have $|M| + |M| = |M|$. If $|M| = |A|$ then the proof is complete, so assume the cardinalities are unequal. Since M is a subset of A we must have $|M| < |A|$, and in fact by Theorem VII.1.2 it follows that $|A - M|$ must be infinite (if it were finite then we would have $|M| =$

|A|). Let $\mathbf{C} \subset \mathbf{M}$ be a countably infinite set, let $\mathbf{h_0 : C \amalg C \to C}$ be a bijection, and consider the map

$$\mathbf{k : (M \cup C) \amalg (M \cup C) \to M \cup C}$$

defined as the composite

$$\mathbf{(M \cup C) \amalg (M \cup C) = (M \amalg M) \cup (C \amalg C) \to M \cup C}$$

sending $\mathbf{x \in M \amalg M}$ to $\mathbf{h(x)}$ and $\mathbf{y \in C \amalg C}$ to $\mathbf{h_0(x)}$. It follows immediately that the element $\mathbf{(M \amalg C, k)}$ is strictly greater than **(M, h),** contradicting the maximilaity of the latter. The problem arises from our assumption that **|M|** and **|A|** are unequal, and thus we have $\mathbf{|M| = |A|}$ and we have proved the statement about $\mathbf{|A| + |A|}$.

Proof that $\mathbf{|A| \cdot |A| = |A|}$. — Let $\mathbf{V_A}$ be the set of all pairs **(B, f)** where $\mathbf{B \subset A}$ is a nonempty subset and $\mathbf{f : B \times B \to B}$ is a bijection ($1-1$ correspondence). If we set $\mathbf{(B, f) \leq (C, g)}$ if and only if $\mathbf{g(b_1, b_2) = f(b_1, b_2)}$ for $\mathbf{b_1, b_2 \in B}$, then routine calculations show that $\leq$ defines a partial ordering on $\mathbf{V_A}$.

The set $\mathbf{V_A}$ is nonempty because **A** contains a countably infinite subset **C,** and by Theorem **VI.4.8** there is a bijection from $\mathbf{C \times C}$ to **C.**

Suppose now that we have a linearly ordered subset of $\mathbf{V_A}$ whose elements have the form $\mathbf{(B_t, f_t)}$, where **t** lies in some indexing set. The argument in the previous part of the proof extends to show that this linearly ordered set has an upper bound, whose graph is again the union of the graphs of the functions $\mathbf{f_t}$. Therefore, once again Zorn's Lemma implies the existence of a maximal element **(M, h)** and once again the conclusion is true if $\mathbf{|M| = |A|}$, so suppose the latter is false. It follows that $\mathbf{|M| < |A|}$. We can now use the first part of the theorem to conclude that $\mathbf{|M| + |M| = |M|}$, and if we combine this with the equation $\mathbf{|M| + |A - M| = |A|}$ we conclude that $\mathbf{|M| < |A - M|}$. In fact, the first part of the theorem implies that $\mathbf{|M| = 3|M|}$ and consequently we have $\mathbf{3|M| < |A - M|}$.

The inequality $\mathbf{|M| < |A - M|}$ implies the existence of a subset $\mathbf{N \subset A - M}$ such that $\mathbf{|N| = |M|}$, and in fact the last sentence of the previous paragraph implies that we may write **N** as a union of pairwise disjoint subsets $\mathbf{N_1, N_2, N_3}$ which have the same cardinality as **M** and **N.** Define an extension of $\mathbf{h : M \times M \to M}$ to

$$\mathbf{k : (M \cup N) \times (M \cup N) \to M \cup N}$$

using the following breakdown by cases:

(1) On $\mathbf{M \times M}$, **k** is given by **h.**

(2) On $\mathbf{M \times N}$, **k** is given by the composite $\mathbf{M \times N \leftrightarrow N \times N \leftrightarrow M \times M \leftrightarrow M \leftrightarrow N_1}$, where the $1-1$ correspondences are determined by the standard maps $\mathbf{M \leftrightarrow N}$, $\mathbf{N \leftrightarrow N_1}$, and $\mathbf{M \times M \leftrightarrow M}$.

(3) On $\mathbf{N} \times \mathbf{M}$, $\mathbf{k}$ is given by the composite $\mathbf{N} \times \mathbf{M} \leftrightarrow \mathbf{N} \times \mathbf{N} \leftrightarrow \mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M} \leftrightarrow \mathbf{N_2}$, where the $1-1$ correspondences are determined by the standard maps $\mathbf{M} \leftrightarrow \mathbf{N}$, $\mathbf{N} \leftrightarrow \mathbf{N_2}$, and $\mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M}$.

(4) On $\mathbf{N} \times \mathbf{N}$, $\mathbf{k}$ is given by $\mathbf{N} \times \mathbf{N} \leftrightarrow \mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M} \leftrightarrow \mathbf{N_3}$, where the $1-1$ correspondences are determined by the standard maps $\mathbf{M} \leftrightarrow \mathbf{N}$, $\mathbf{N} \leftrightarrow \mathbf{N_3}$, and $\mathbf{M} \times \mathbf{M} \leftrightarrow \mathbf{M}$.

By construction we again have $(\mathbf{M} \cup \mathbf{N}, \mathbf{k})$ is strictly greater than $(\mathbf{M}, \mathbf{h})$, contradicting the maximilaity of the latter. The problem arises from our assumption that $|\mathbf{M}|$ and $|\mathbf{A}|$ are unequal, and thus we have $|\mathbf{M}| = |\mathbf{A}|$ and we have shown the statement of the theorem about $|\mathbf{A}| \cdot |\mathbf{A}|$.■

The following consequence of Theorem 2 and Corollary 3 is useful in many situations.

Proposition 4. *Let* $\{\mathbf{A_n}\}$ *be a countable sequence of infinite sets such that* $|\mathbf{A_n}| \leq \alpha$ *for all* $\mathbf{n}$ *and there is some nonnegative integer* $\mathbf{M}$ *such that* $|\mathbf{A_M}| = \alpha$. *Then we have* $|\cup_n \mathbf{A_n}| = \alpha$.

Proof. Let $\mathbf{B}$ denote the union. Then we clearly have $\alpha \leq |\mathbf{B}|$ since $|\mathbf{A_M}| = |\mathbf{B_M}|$ for some $\mathbf{B_M} \subset \mathbf{B}$. On the other hand, by the cardinality assumption we also have injections $\mathbf{f_n} : \mathbf{A_n} \to \mathbf{A_M}$ for all $\mathbf{n}$, and we can piece these together to obtain an injection

$$\varphi : \coprod_n \mathbf{A_n} \to \mathbb{N} \times \mathbf{A_M}$$

defined by the formula $\varphi(\mathbf{n}, \mathbf{x}) = (\mathbf{n}, \mathbf{f_n}(\mathbf{x}))$. There is also a surjection

$$\psi : \coprod_n \mathbf{A_n} \to \mathbf{B}$$

sending $\{\mathbf{n}\} \times \mathbf{A_n}$ bijectively to $\mathbf{A_n} \subset \mathbf{B}$. If we now apply Exercise **VII.1.2**, it follows that $|\mathbf{B}| \leq \aleph_0 \times \alpha$, and by Corollary 3 the right hand side is equal to α. We can now use the Schröder – Bernstein Theorem to conclude that $|\mathbf{B}| = \alpha$. ■

Corollary 5. *In the setting of the previous result, if* $|\mathbf{A_n}| = \alpha$ *for all* $\mathbf{n}$, *then* $|\mathbf{B}| = \alpha$.■

Zorn's Lemma in algebra

Several other applications of Zorn's Lemma to basic questions in algebra are worked out on page 226 of Lipschutz (in particular, see Problems 9.6 and 9.7); for example, Problem 9.6 uses Zorn's Lemma to prove that ***every infinite – dimensional vector space has a basis.***

A formal definition of cardinal numbers

We can use the Well – Ordering Principle to give a simple and mathematically sound definition of cardinal numbers. The key to doing so is contained in the following result:

Proposition 4. *Let* **X** *be a set, and let* $\mathbf{C_X}$ *be the collection of ordinal numbers* α *for which there is a* $1-1$ *mapping from* α *into* **X.** *Then* $\mathbf{C_X}$ *is a nonempty set.*

Definition. The least element of $\mathbf{C_X}$ is called the ***cardinal number*** of **X.** From this perspective we may view $\aleph_0$ as being equal to the first infinite ordinal, which is ω.

Proof. The class $\mathbf{C_X}$ is nonempty by the well – ordering principle. To show it is a set, it suffices to prove that there is some ordinal number β for which there is ***no*** $1-1$ mapping from β into **X.** It then follows that $\alpha < \beta$ for all $\alpha \in \mathbf{C_X}$, which implies that $\mathbf{C_X}$ is a set. There are two ways of doing this; either one can use Hartogs' Theorem or else one can take the ordinal number associated to a well – ordered set **Y** such that $|\mathbf{Y}| = |\mathbf{P(X)}|$; the latter is quicker and perhaps more convincing, but the former is logically more direct.■

Corollary 5. *The class of cardinal numbers is well – ordered by the restriction of the ordering relation on the ordinal numbers. In particular, given any cardinal number* α *there is a least cardinal number* β *such that* $\beta > \alpha$ *(****i.e.,*** *there is a* ***next largest cardinal number*** *— this statement was first formulated by Cantor)*.■

In fact, one can say more. Using a suitably strong version of transfinite recursion one can define a strictly order – preserving $1-1$ correspondence from the ordinal numbers to the infinite cardinal numbers. We have already denoted the first infinite cardinal by $\aleph_0$. Following Cantor's notation, it is customary to denote the next infinite cardinal, which is the image of 1 under the recursively defined mapping, by $\aleph_1$. More generally, the cardinal number which corresponds to the ordinal α is denoted by $\aleph_\alpha$.

VII.5: Logical consistency and acceptance

(Halmos, § 15; Lipschutz, §§ 9.1, 9.7)

Whenever it appears that one statement about a mathematical system cannot be derived as a mathematical consequence of the others, there are immediate questions whether this statement can or should be taken as an additional assumption, and thus near the beginning of the 20th century there were immediate questions about whether the Axiom of Choice or an equivalent statement should be added to the basic assumptions of set theory. Concern over the desirability of adding the Axiom of Choice or an equivalent statement to the axioms for set theory increased with the discovery of difficulties such as Russell's Paradox. Most of these difficulties were resolved within two decades by a careful foundation of the axioms for set theory, but it was still not known if adding the Axiom of Choice might still lead to a logical contradiction. We shall discuss subsequent developments about logical consistency later in this section.

As noted earlier, this section discusses some conceptual points about the following basic questions:

1. Does the inclusion of the Axiom of Choice (or an equivalent statement) lead to any further problems?
2. Should the Axiom of Choice (or an equivalent statement) be assumed as an axiom for set theory?

The following additional question will be addressed in the next section.

3. Are there other set – theoretic statements that also should be included as axioms?

We have already noted that Cantor and his contemporaries recognized that something like the Axiom of Choice might have to be taken as an assumption if it could not be proved. Concern over the desirability of adding the Axiom of Choice to the axioms for set theory increased with the discovery of difficulties such as Russell's Paradox near the beginning of the 20^{th} century. Although most of these potential paradoxes in set theory were resolved by a careful foundation of the axioms for the subject, such work did not determine whether the Axiom of Choice and its equivalent statements led to logical consistency problems; in other words, it was still not known if adding the Axiom of Choice or an equivalent statement might eventually lead to a logical contradiction. We shall discuss subsequent developments about logical consistency later in this section; historically, the next development raised further questions about assuming statements like the Axiom of Choice.

The Banach – Tarski Paradox

A new reason for concern about the Axiom of Choice was discovered in the 1920s. The so-called ***Banach – Tarski paradox*** showed that the Axiom of Choice had some extremely strong consequences which seemed to contradict common sense. These raised additional questions about whether the Axiom of Choice should be included in the axioms for set theory. In its original form, the relevant result of S. Banach (1892 – 1945) and A. Tarski (1902 – 1983) states that if the Axiom of Choice is assumed, then it is possible to take a solid ball in **3** – dimensional space, cut it up into finitely many pieces, and moving them — using only rotation and translation — reassemble the pieces into two balls having the same size as the original one**!!**

Such a bizarre result raises serious questions whether one could prove even more results and perhaps even use the Axiom of Choice to obtain a logical contradiction. In particular, at first glance the Banach – Tarski result may seem to violate the basic laws of physics (***e.g.,*** Conservation of Matter). Fortunately, this does not reflect a problem with the underlying mathematics, for it is important to note that *the sets in question are* **mathematical** *rather than* **physical** *objects*. In particular, there is no meaningful way to define the volumes of the individual pieces, and it is impossible to carry out the construction physically because if one does cut the solid ball into pieces physically (say with a knife or saw), each piece will have a specific volume (physically, one can find the volumes by sticking the pieces into a large cylinder which contains enough water or other fluid that will not dissolve the pieces). However, even though the Banach – Tarski paradox does not yield a logical contradiction to the axioms of set theory or the fundamental laws of experimental physics, it does raise two fundamental questions:

1. If set theory with the Axiom of Choice yields bizarre conclusions like the existence of the sets described above, is it possible that further work will lead to a contradiction?

2. Is it worthwhile to consider such objects, and if not is it appropriate to have an axiomatic system for set theory that will imply the existence of such physically unreal entities?

One way of answering the second question is that the Axiom of Choice also implies the existence of many things that mathematicians do want for a variety of reasons, and it is definitely simpler to do mathematics with the Axiom of Choice rather than without it. ***The preceding applications to transfinite cardinal numbers strongly illustrate this point.***

This leads directly to the issue of ***whether the Axiom of Choice should be included in our axioms for set theory.*** As indicated above and in these notes, the assumption of the Axiom of Choice allows mathematicians to do many things that would otherwise be difficult or impossible. Although some mathematicians think that the subject should only consider objects given by suitably **"**constructive**"** methods, the existence and other consequences the Axiom of Choice are so useful and powerful that most mathematicians would prefer to include it as part of the axioms if at all possible. By the middle of the 20th century the Axiom of Choice was generally accepted (but in many cases grudgingly) by most **"**ordinary**"** mathematicians — ***i.e.,*** most of those who are not logicians or set theorists.

Here are some further online references for the Banach – Tarski paradox.

http://mathworld.wolfram.com/Banach-TarskiParadox.html

http://www.math.hmc.edu/~su/papers.dir/banachtarski.pdf

http://www.kuro5hin.org/story/2003/5/23/134430/275

http://en.wikipedia.org/wiki/Banach-Tarski_Paradox

Relative consistency of the Axiom of Choice

Of course, if the Axiom of Choice leads to a logical contradiction, then it should not be part of the axioms for set theory, so this brings us back to the first question. Two extremely important and fundamental pieces of research by K. Gödel in the nineteen thirties clarified the role of the Axiom of Choice. The first of these was his work on the incompleteness properties of axiomatic systems, and the essential conclusion is that mathematics can ***never*** be absolutely sure that ***any*** reasonable set of axioms for an infinite set theory is logically consistent. His subsequent result showed that the Axiom of Choice was ***relatively consistent*** with the other axioms for set theory. Specifically, ***if there is a logical contradiction in set theory with the inclusion of the Axiom of Choice, then there is also a logical contradiction if one does not assume the Axiom of Choice.*** This is entirely analogous to the situation for the Axiom of Foundation that was discussed in Section **III.4** of these notes.

Formally, the relatively consistency properties are often stated in terms of the system of axioms for set theory developed by E. Zermelo (1871 – 1953) and A. Fraenkel (1891 –

1965) which is generally known as **ZF.** In these terms, Gödel's results state that if **ZF** plus either the Axiom of Foundation or the Axiom of Choice is logically inconsistent, then **ZF** is already logically inconsistent **without** either assumption.

Here are some further online references related to these topics:

http://planetmath.org/encyclopedia/MultiplicativeAxiom.html

http://mathworld.wolfram.com/AxiomofChoice.html

http://www.miskatonic.org/godel.html

http://www.time.com/time/time100/scientist/profile/godel.html

http://en.wikipedia.org/wiki/Kurt_Gödel

http://scienceworld.wolfram.com/biography/Goedel.html

http://www.cs.uwaterloo.ca/~alopez-o/math-faq/node69.html

Since most mathematicians would prefer to include as many objects as possible in set theory so long as these objects do not lead to a logical contradiction, the effective consequence of relative consistency is that inclusion of the Axiom of Choice in the axioms for set theory is viewed as appropriate by most "ordinary" mathematicians. From a purely formal viewpoint, there is nothing to lose and much to gain by adding this extra assumption. The system obtained by including the Axioms of Foundations and Choice with **ZF** is frequently denoted by **ZFC.**

Axiomatic systems for set theory. Having mentioned **ZF,** we should note that our approach to set theory is slightly different because our setting includes collections called classes that are too large to be sets while **ZF** does not (in **ZF** such objects simply do not exist). Our formulation is based on a variant of **ZF** that is due to von Neumann, P. Bernays (1888 – 1977) and Gödel, and is often denoted by **NBG;** this formulation is closely related to **ZF** and is very widely used (although this is generally not stated explicitly outside of mathematical writings on set theory and the foundations of mathematics). As suggested by the first sentence in this paragraph, one major innovation in the latter is its use of classes for collections that are too large to be sets. Another important difference is that the Axiom of Specification is simplified in a significant manner (in particular, it can be replaced by a finite list of assumptions). Both formulations yield the same logical consequences, and each is logically consistent if and only if the other is. This equiconsistency of **ZF** and **NBG** was established in the nineteen sixties and is generally attributed to W. Easton and R. Solovay. The following online references contain additional information about both **ZF** and **NBG:**

http://en.wikipedia.org/wiki/ZFC

http://www.bookrags.com/Zermelo%E2%80%93Fraenkel_set_theory

http://mathworld.wolfram.com/vonNeumann-Bernays-GoedelSetTheory.html

http://en.wikipedia.org/wiki/Von_Neumann-Bernays-G%C3%B6del_axioms

Having noted the impossibility of proving that set theory is logically consistent, the next question is more or less unavoidable.

What if set theory is logically inconsistent? Although we can never be absolutely sure about this, there is a great deal of encouraging evidence. The basic axiomatic structure for set theory has now been in place and in its current form for about three quarters of a century, and no new concerns have arisen over that time. Of course, there are no guarantees that new difficulties will never emerge, but the absence of new problems over 75 years of intense critical study of foundational questions and enormous progress in all areas of mathematics lead to an important subjective conclusion: ***The current axiomatic system has proven to be highly reliable even if we cannot be sure it is absolutely perfect.***

Even if some new problems arise, most mathematicians strongly believe that they can be handled effectively, and the following annotated quote from the first page of the online document

http://www.math.ku.dk/~kiming/courses/2004/matm/real_numbers.pdf

seems worth including at this point:

> Do not worry too much about this [*the possibility that there are some hidden contradictions*] **…** No contradictions have turned up after a century of scrutiny, and if a contradiction should turn up you can be sure that bridges will not suddenly start to collapse [*because of such a contradiction*] or that space ships will miss their destinations because of that [*of course, this might happen for other reasons*]. If a contradiction turned up we would simply have to reconsider the situation and construct a new axiomatic system that does for us what we want of it [*this would probably be far more difficult than the comments suggest, but in principle it would resemble the sort of work that is needed whenever one finds a nontrivial logical problem in some complicated piece of computer software that has proven to be pretty reliable over an extended period of time — everyone is confident that the program can be repaired, but a great deal of time and effort may be needed to complete the job*].

Logical independence of the Axiom of Choice

Fundamental results of P. M. Cohen (1934 –) from the nineteen sixties have completed our current understanding of the logical status of the Axiom of Choice. Specifically, he showed that one can construct models for set theory such that the Axiom of Choice was true for some models and false for others; this conclusion is slightly more concrete than the one obtained by Gödel, which did not yield comparable information about constructing alternative models for set theory. Here are some online references with further information**:**

http://plato.stanford.edu/entries/set-theory/#7

http://publish.uwo.ca/~jbell/CHOICE.pdf

http://en.wikipedia.org/wiki/Axiom_of_choice#Independence

http://www-math.mit.edu/~tchow/mathstuff/forcingdum

http://en.wikipedia.org/wiki/Forcing_(mathematics)

The Axiom of Countable Choice

There are also several weaker statements which are not equivalent to the axiom of choice, but which are closely related. One simple one is the ***Axiom of Countable Choice***, which states that a choice function exists for any ***countable*** set **X**. It states that a ***countable*** collection of sets must have a choice function. The previously mentioned methods and results of P. Cohen also show that the Axiom of Countable Choice is not provable in **ZF.**

The Axiom of Countable Choice is required for the rigorous development of calculus and the theory of functions of a real variable in its standard form; in particular, many results in these subjects depend on having a choice function for a countable set of real numbers (considered as sets of Cauchy sequences of rational numbers). Some mathematicians who have reservations about the Axiom of Choice are willing to accept the Axiom of Countable Choice.

VII.6: The Continuum Hypothesis

(Halmos, § 25)

The third issue raised above was whether there are other statements which might deserve to be taken as axioms for set theory. One widely known statement of this type is the the ***Continuum Hypothesis*,** which emerged very early in the study of set theory.

CONTINUUM HYPOTHESIS. *If* **A** *is an infinite subset of the real numbers* **R,** *then either there is a* **1 – 1** *correspondence between* **A** *and the natural numbers* **N,** *or else there is a* **1 – 1** *correspondence between* **A** *and* **R.**

This question arose naturally in Cantor's work establishing set theory, the motivation being that he did not find any examples of subsets whose cardinal numbers were strictly between those of **N** and **R.**

Since there is a **1 – 1** correspondence between the real numbers **R** and the set **P(N)** of all subsets of **N,** one can reformulate this as the first case of a more sweeping conjecture known as the ***Generalized Continuum Hypothesis*:**

GENERALIZED CONTINUUM HYPOTHESIS. *If* ***S*** *is an infinite set and* **T** *is a subset of* **P(*S*)***, then* ***either***

(*i*) *there is a one-to-one correspondence between* **T** *and a subset of* ***S,*** **or else**

(*ii*) *there is a one-to-one correspondence between* **T** *and* **P(*S*)** *.*

In analogy with his results on the Axiom of Choice, the work of Gödel showed that if a contradiction to the axioms for set theory arose if one assumes the Continuum Hypothesis or the Generalized Continuum Hypothesis, then one can also obtain a contradiction without such an extra assumption. On the other hand, the previously mentioned fundamental work of P. M. Cohen shows that one can construct models for set theory such that the Continuum Hypothesis was true for some models and false for others. In fact, one can construct models for which the number of cardinalities between those of $\mathbf{N}$ and $\mathbf{R}$ can vary to some extent; some aspects of this are discussed below. Because of Cohen's work, many mathematicians are ***not*** willing to assume the Continuum Hypothesis or the Generalized Continuum Hypothesis for the same reason that they are willing to assume the Axiom of Choice: They would prefer to include as many objects as possible in set theory so long as these objects do not lead to a logical contradiction. Cohen's own viewpoint on this matter is summarized in the third online reference listed below.

Here are some online references which discuss Cohen's methods and results:

http://mathworld.wolfram.com/ContinuumHypothesis.html

http://en.wikipedia.org/wiki/Forcing_(mathematics)

http://en.wikipedia.org/wiki/Paul_Cohen_(mathematician)

Cohen's methods show that several other natural questions in set theory are true in some models but false in others; the preceding references contain details on numerous results of this type. We shall limit our discussion to a related question concerning cardinal numbers:

> *Suppose that* **A** *and* **B** *are sets whose power sets satisfy the cardinality equation* $|\mathbf{P(A)}| = |\mathbf{P(B)}|$. *Does it follow that* $|\mathbf{A}| = |\mathbf{B}|$?

For finite sets this is a trivial consequence of the fact that the function $\mathbf{2^x}$ is strictly increasing over the real numbers. For infinite sets, there is a curious relation between this question and the Generalized Continuum Hypothesis: *If the latter is true, then the answer to the question is* **YES.** This follows because for every infinite set **A** we know that $|\mathbf{P(A)}|$ is the unique first transfinite cardinal number that is strictly larger than $|\mathbf{A}|$, and conversely $|\mathbf{A}|$ is the largest cardinal number that is strictly less than $|\mathbf{P(A)}|$.

On the other hand, the condition on cardinal numbers is not strong enough to imply the Generalized Continuum Hypothesis, and one can also construct models of set theory containing sets **A** and **B** such that $|\mathbf{A}| < |\mathbf{B}|$ but $\mathbf{2}^{|\mathbf{A}|} = \mathbf{2}^{|\mathbf{B}|}$. More generally, very strong results on the possible sequences of cardinal numbers that can be written as $\mathbf{2}^{|\mathbf{A}|}$ for some $|\mathbf{A}|$ are given by results of W. B. Easton which build upon Cohen's methods; Easton's result essentially states that a few relatively straightforward necessary conditions on such sequences of cardinal numbers are also sufficient to realize it as the set of cardinalities for power sets. These results first appeared in the following paper by Easton: ***Powers of regular cardinals***, Ann. Math Logic **1** (1970), 139 – 178. A more recent paper by T. Jech covers subsequent work on this problem: ***Singular cardinals and the* PCF *theory***, Bull. Symbolic Logic **1** (1995), 408 – 424.

Possibilities for the cardinality of the real numbers. Since Cohen's results imply that $|\mathbf{R}|$ may or may not be equal to $\aleph_1$ depending upon which model for set theory is being considered, one can ask which cardinal numbers are possible values for $|\mathbf{R}|$. Results on this and more general questions of the same type follow from Easton's work. In particular, it turns out that $|\mathbf{R}|$ can be equal to $\aleph_n$ for every positive integer **n** but it cannot be equal to the cardinal number $\aleph_\omega$ (all these are defined as above). A proof of the last assertion appears in the exercises on page 66 of the following book:

I. Kaplansky, ***Set theory and metric spaces*** (2^{nd} Ed.). Chelsea, New York, 1977. ISBN: 0–8284–0298–1.

Recently there has been some further thought about whether or not one should assume the Continuum Hypothesis, and much of it has been generated by the following articles:

W. H. Woodin, *The continuum hypothesis*, Parts **I** – **II**. Notices of the American Mathematical Society **48** (2001), 567 – 576, 681 – 690. [Available online at http://www.ams.org/notices/200106/fea-woodin.pdf and http://www.ams.org/notices/200107/fea-woodin.pdf.]

The following online site includes a fairly extensive scholarly analysis of Woodin's articles:

http://www.math.helsinki.fi/logic/LC2003/presentations/foreman.pdf