Reading Paper 381 Report

ZFC Set Theory and the Category of Sets

Foundations for the Working Mathematician

Helen Broome
Supervisor: Andre Nies

Introduction

In presenting a brief exposition of the axioms of ZFC set theory and the category of sets the intent of this report is to look at what gets blithely called 'foundational' and occasionally stop to ponder the plight of the "working mathematician". This enigmatic figure is constantly invoked in mathematical literature as the arbiter of what is worthwhile, often with the ulterior motive to point out that foundational concerns are irrelevant to his job.

It can seem like a misnomer to call the disciplines of set theory and category theory foundational when they are not historically antecedent to the main body of mathematical thought. However, this talk of foundations became more of a focus with the employment of the modern axiomatic method. This is not because they are equivalent but the use of explicit primary assumptions that allow a greater abstraction in the structures discussed raises questions about the truth and security of proofs in general.

A key maxim of the axiomatic method is that the essential properties of isomorphic structures are mathematically indistinguishable [Mayberry, 1994]. This means that reference to the real numbers as abstract ontological objects is replaced by the axiomatically defined complete ordered fields. While the real numbers are a complete ordered field the axioms do not specifically describe 'the' real numbers. Instead, any two complete ordered fields can be shown to be order isomorphic. This means that the way the elements in these structures relate to one another is the same, only the names of these elements differ. By referring to the axiomatically defined structure of complete ordered fields we are being more explicit about the properties possessed by such a field without stating what the elements of such a structure are. For instance, π is a real number and so it is an element of a complete ordered field but the axioms do not tell us anything about π, only the way it relates to the other elements. This sidesteps the ontological difficulty of what abstract mathematical objects such as π are by making structures the primary subject matter.

When we compare the axioms of ZFC and the category of sets they diverge in the abstractness they allow. An element in a complete ordered field is not required to possess any specific properties however this is different to allowing the element to be so abstract as to have no properties. Lawvere points out that Cantor talked about an abstract set whose elements were devoid of properties except for their mutual distinctness. However Zermelo thought it was inconsistent to have a definite number of points that possess no distinguishing properties. Hence in the Zermelo-Fraenkel axioms there is a focus on the individual elements which are the starting point for building sets within the cumulative hierarchy.

Category theory allows abstract points as it begins with morphisms or mappings between 'objects'. This does not require an explicit statement about the nature of the elements of that object. This is in contrast to the constructive approach of set theory where the process of building sets out of elements plunges the elements into the limelight. The axiom of foundation or regularity in ZFC is a statement about what it means to talk of a set being an element of another set. This plays a large role in set theory yet the category of all sets and mappings in ZFC is isomorphic to the category of all sets and mappings in ZFC where the axiom of foundation is replaced with anti-foundation [Simpson]. This demonstrates that the exact nature of membership is not important from a categorical perspective.

Rather than focusing on the membership of structures, categories provide a context to look at the general notion of structure. However a structure is typically defined as a set with a defined morphology that can also be characterized by sets. As a set can be seen as a plurality that is limited in size it is at odds with a category which is not as discerning in its membership criteria, letting anything in. Category theory talks about types of structures based on what components and structural maps it requires. For instance graphs have 'arrows' and 'dots' as two component objects and 'source' and 'target' maps.

Based on the differing approaches to membership if we want to talk about a property of an entity such as a group there are different quantification requirements. In set theory we must quantify over a specific range of 'group' objects that are somehow fixed and given. This is because set theory builds upwards and so to satisfy this property any group constructed in this manner must possess this property. However category theory is more schematic and to state a property of a group it talks about the property of 'any group' rather than requiring all fixed or possible groups to be included in the statement. As a schematic statement about a group it allows the group structure to take different instances and is not characterising all possible groups from a universal perspective [Awodey].

The differing approaches to abstraction are in line with opinions on what a foundational system is or should provide. It is here that the figure of the "working mathematician" antagonistically steps forward, as always clothed in his inverted commas. From one perspective, espoused by the category theorist Lawvere, a mathematical foundation is not something that founds but is a description whose aim is to "concentrate the essence of practice and in turn use the result to guide practice." [Lawvere, 2003] This has a close relation with our working mathematician as it does not dictate his universe; it is exploring it with him.

But others will argue that the descriptive position leaves the working mathematician at an impasse: his job is involved in "the science which draws necessary conclusions" [Pierce quoted in Mayberry 1994] yet he has no basis for characterising the compelling truth of any statement or proof. Hence what is required is the knowledge that his proofs rest upon premises whose truth is generally accepted and that these premises are statements involving explicitly stated primitive terms to be used as a fixed reference point for the whole mathematical discourse. This desire to construct a universe for mathematics out of a select few basic ideas is analogous to the statement that "points pre-exist spaces which are made up of points". The incommensurable alternative that "spaces pre-exist points and points are extracted out of spaces or are at the boundaries and intersections of spaces" exemplifies the descriptive approach which surveys what is already talked about and then abstracts parts out of this for a generalised discussion.

The common rhetoric of category theory is that it is form and not content that is pivotal. While Cantor may have agreed with this, based on a rough popularity count the "working mathematician" prefers ZFC set theory with its concomitant membership content over the greater abstractness of categorical mapping forms.

However mathematics does not require a respite to the foundational bickering to get on with investigating and discovering/creating its structures. Besides which category theory was not initially developed as a foundational program and presents mathematics with many interesting and useful descriptions applicable in many fields regardless of any foundational claims. Similarly in set theory there are a variety of new objects. The rest of this report will give an explicit statement of the axioms of ZFC and the alternative Category of Sets and introduce some of the objects of these fields and the problems that arise with them.

The Axioms of ZFC

Zermelo and Fraenkel came up with the following axioms for set theory which are the most commonly used variety. It is called ZFC due to the inclusion of the axiom of choice to differentiate from situations where choice is not used and we are working in ZF.

Axiom of Extension

For any sets X, Y they are equal if and only if they have the same elements.
$\forall X \forall Y (X = Y \leftrightarrow \forall z (z \in X \leftrightarrow z \in Y))$

This expresses the foundational assumption of set theory that a set is uniquely determined by its elements.

Axiom of Power Set

If X is a set there exists a set $Y = \mathcal{P}(X)$, the set of all subsets of X.
$Y = \{ A \mid \forall x \in A, x \in X \}$

Axiom of Union

For any set X there exists a set $Y = \bigcup X$, the union of all elements of X.
$Y = \{ A \mid \exists Z (A \in Z \wedge Z \in X) \}$

Axiom Schema of Replacement

If a class F is a function then for any set X, there exists a set $Y = F(X)$.

Alternatively, if a class F is a function and the domain of F is a set then the range of F is a set.

This is called an axiom schema because for each formula $\varphi(x, y, p)$, where p is a parameter, the following is an axiom:

$$\forall x \forall y \forall z (\varphi(x, y, p) \wedge \varphi(x, z, p) \rightarrow y = z)$$
$$\rightarrow \forall X \exists Y \forall y (y \in Y \leftrightarrow (\exists x \in X) \varphi(x, y, p))$$

Axiom of Foundation or Axiom of Regularity

Every nonempty set X has an $\in$-minimal element z.
$\forall X (X \neq \emptyset \rightarrow (\exists z \in X) X \cap z = \emptyset)$.

This axiom restricts the inclusion of some things in the universe of sets and it is useful for the construction of models. It allows all sets to be arranged in a cumulative hierarchy which we can define by recursion of partial universes. This definition will be stated although it requires the notion of an ordinal which will not be given till later.

$V_0 = \emptyset$
$V_{\alpha+1} = \mathcal{P}(V_\alpha)$ for any ordinal α
$V_\delta = \bigcup_{\alpha<\delta} V_\alpha$ for any limit ordinal δ

Sets of the form V_α are called partial universes. Using this definition there is an equivalent form of the Axiom of Foundation, namely:
Every set, X, belongs to some partial universe.

Axiom of Empty Set

There is exactly one X such that for any y, $y \notin X$, $X = \emptyset$.

Axiom of Pairing

For any a, b there exists a set $X = \{a, b\}$ that contains exactly a and b.

This axiom is redundant as it can be derived from the other axioms:
$\emptyset$ is a set, hence $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$ is a set.
By Replacement we can define a function

$$F(x) = \begin{cases} a, & \text{x=}\emptyset \\ b, & \text{x=}\{\emptyset\} \end{cases}$$

Hence $X = \{a, b\}$ exists.

Axiom Schema of Separation

For any property, P, and for any set, X, there exists a set, Y, of all the elements in X which have the property P.
$Y = \{x \in X \mid P(x)\}$

One, but not both, of the Axiom of Empty Set and Axiom Schema of Separation are needed. The other can be derived within the remaining axioms of ZF.

Regardless of whether it is explicitly stated or merely derived, the presence of the axiom of separation means set theory avoids Russell's paradox that;

$$A = \{x \mid x \notin x\} \text{ does not exist because } A \in A \Leftrightarrow A \notin A$$

This paradox is avoided due to the extra condition that $x \in X$, for some set X, before looking at whether x satisfies a certain property such as $x \notin x$. A consequence of this is that there is not a universal set U which contains all sets. If U existed then $\{x \in U \mid x \notin x\}$ would be a valid set by the Separation axiom and we would be faced with Russell's paradox again.

While there exists some collections that cannot be described in ZFC it is possible to talk about them as a class of sets possessing a certain property, i.e. sets that satisfy a formula ψ. Although sets are the only object in ZFC, the informal notion of a class, $C(\psi) = \{x \mid \psi(x)\}$ is used as it is easier to manipulate than formulas, although $C(\psi)$ is synonymous with the formula

ψ. With the notion of class we can talk about intersection or union of classes as $C(\psi) \cup C(\phi) = C(\psi \vee \phi)$. Similarly the inclusion of a class $C(\phi)$ in a class $C(\psi)$ is equivalent to $(\phi \rightarrow \psi)$ being logically valid. However we cannot talk about one class being the member of another class.

With the axioms stated so far only finite collections are sets meaning all infinite collections are proper classes. This is due to the bottom-up construction beginning with the empty set as the most basic object and building a cumulative hierarchy of sets with reference to the other axioms. To be able to talk about an infinite collection as being a set we need another axiom.

Axiom of Infinity

There exists an infinite set. Or equivalently; there exists an inductive set.
$\exists X(\emptyset \in X \wedge (\forall x \in X)\, x \cup \{x\} \in X)$

The axiom of infinity is independent of the other axioms as there exists a consistent model of ZF minus the axiom of infinity. The model is $(\mathbb{N}, \in)$ where $x \in y$ if there is a 1 in the $x+1$ position of the binary representation of y.

Similarly the axiom of choice is independent of ZF. I will state the axiom here but will look at it in greater detail later on.

Axiom of Choice

Let F be a function with domain I and $F(i) \neq \emptyset$ for each $i \in I$ then $X = (F(i) \mid i \in I)$ is an indexed family of sets.

The axiom of choice states that there exists a choice function, f, on X such that for each $i \in I,\ f(i) \in F(i)$.

With this basic framework for ZFC it is possible to give explicit formulations of ordered pairs, functions and relations in set theory. This allows us to talk about structures within set theory as not only the domain is a set but also the morphology or relation defined on it can be conceived of in terms of sets. This is important for the claim that it is possible to do all of mathematics in a set theory using only the notion 'belongs to'.

Ordered pairs are used throughout mathematics but the order is a matter of notation. In set theory $\{a, b\} = \{b, a\}$ so it is not sufficient to represent the ordered pair (a, b) as the set $\{a, b\}$. The set theoretical convention, due to C. Kuratowski, is to say $(a, b) = \{\{a\}, \{a, b\}\}$. This prevents the need to introduce a second primitive notion for an ordered set, as Kuratowski's definition only requires the primitive notion $\in$.

Using the definition of an ordered pair we can define;

The Cartesian product $A \times B = \{(a, b) \mid a \in A, b \in B\}$;

A relation R which holds between x and y, xRy, if $(x, y) \in R$;

A function f which is a relation with the condition that
$\forall x, y, z\, (x, y), (x, z) \in f \Rightarrow y = z$

Ordinals and Cardinals

Cantor used bijective functions to compare the sizes of two sets. This method was particularly necessary for infinite sets and highlights the paradoxical case that with infinity it is not true that the whole is greater than the part. To be able to talk about the size of these sets Cantor introduced ordinals and cardinals as new mathematical objects.

Ordinals

Ordinal numbers behave in such a way that

$$\alpha < \beta \Leftrightarrow \alpha \in \beta, \quad \beta = \{\alpha \mid \alpha < \beta\}$$

A set is an ordinal if the set is transitive and well ordered by $\in$.

A set, T, is transitive if $\forall x, y \;\; x \in y \in T \Rightarrow x \in T$. Alternatively T is transitive if $\forall x, x \in T \Rightarrow x \subseteq T$.

One conception of the ordinals is the von Neumann ordinals

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, ...$$

Beginning with the empty set, each von Neumann ordinal is the set of all preceding von Neumann ordinals. But regardless of how the ordinals are conceived, every well ordered set is isomorphic to a unique ordinal. A consequence of the axiom of choice is that every set can be well ordered and hence every set has an ordinal.

For each ordinal, α, we define the successor of α to be

$$\alpha + 1 = \alpha \cup \{\alpha\} = \inf\{\beta \mid \beta > \alpha\}$$

If there does not exist α such that $\beta = \alpha + 1$ then β is a limit ordinal and $\beta = \sup\{\alpha \mid \alpha < \beta\}$. The supremum of $\emptyset$ is defined to be 0. This makes 0 the first limit ordinal and if the axiom of infinity is not included it is also the only limit ordinal.

Cardinals

The cardinality of a set X is denoted by $|X|$. This refers to the size of the set X and is like a property shared by all sets Y such that there exists a bijective function $f : X \to Y$. This relationship between X and Y is written $X \approx Y$.

There are two ways to define cardinals depending on whether the axiom of choice is included.

For a well ordered set W, there exists an ordinal α such that $|W| = |\alpha|$. If we assume the axiom of choice then by Zermelo's Well-Ordering theorem all sets can be well ordered. Hence we can define the cardinality of any set W as

$$|W| = \text{the least ordinal such that } |W| = |\alpha|$$

To define cardinals in ZF look at the equivalence classes

$$C_X = \{Y \mid X \approx Y\}$$

For $X \approx Y$ to be a relation it has to be a relation on some set. However we need the set of all sets, V, to be the domain of $\approx$ which is not a set but a proper class. To talk about cardinals that are sets and not proper classes let

$$F(X) = \min\{\alpha \mid \exists Y \in V_\alpha (X \approx Y)\}$$

By the axiom of regularity there exists such a partial universe, V_α.

$$\text{Then } |X| = \{Y \in V_{F(X)} \mid (X \approx Y)\}$$

However without the axiom of choice not all cardinals are comparable. As a result in ZF there exists a set A such that $n < |A|$ for all $n \in \mathbb{N}$ but there there does not exist a one-to-one function $f : \omega \to A$.

Every cardinal is an ordinal and in the finite case the reverse is true. Looking at the infinite case only limit ordinals are cardinals starting with $|\mathbb{N}| = \omega$. This follows from the definition that an ordinal, α is a cardinal if there does not exist a bijection between α and a section of α or $|\alpha| \neq |\beta|$ for any $\beta < \alpha$.

For notational convenience the infinite limit ordinals, or cardinals, are called alephs and are defined as:

$\aleph_0 = \omega$

$\aleph_{\alpha+1} = \aleph_\alpha^+$, the successor of $\aleph_\alpha$ where α is a successor ordinal.

$\aleph_\delta = \sup\{\aleph_\beta \mid \beta < \delta\}$ if δ is a limit ordinal.

A cardinal $\aleph_\alpha$ is a successor cardinal if $\alpha = \beta + 1$ for some β, similarly if δ is a limit ordinal then $\aleph_\delta$ is a limit cardinal. Along with the aleph notation I will use the greek letters κ, λ, μ to refer to cardinals.

Cofinality and Inaccessible Cardinals

The cofinality of a cardinal κ, written $cf(\kappa)$, is the least cardinal λ such that if $\mu_i \leq \lambda$ for all $i \in I$ where $|I| = \lambda$ then

$$\kappa = \sum_{i \in I} \mu_i$$

The first infinite cardinal is $\aleph_0 = \omega$. This is not equal to a finite sum of finite cardinals so $cf(\aleph_0) = \aleph_0 = \omega$.

If $cf(\kappa) = \kappa$ then κ is a regular cardinal.
If $cf(\kappa) < \kappa$ then κ is singular.

The cofinality of a cardinal is a regular cardinal as $cf(cf(\lambda)) = cf(\lambda)$.

A successor cardinal, κ^+, is regular because if we have $|I| = \kappa$ and $\lambda_i \leq \kappa$ for all $i \in I$ then

$$\sum_{i \in I} \lambda_i \leq \kappa$$

Hence there does not exist a cardinal, $\mu \leq \kappa$ which is less than κ^+ for which κ^+ is the sum of μ many cardinals that are strictly smaller than κ^+.

For an uncountable limit cardinal $\kappa = \aleph_\alpha$, where α is a limit ordinal,

$$cf(\aleph_\alpha) = cf(\alpha)$$

If the limit cardinal is also regular then

$$cf(\aleph_\alpha) = cf(\alpha) = \alpha \text{ and } \aleph_\alpha = \alpha$$

A cardinal is **weakly inaccessible** if it is an uncountable regular limit cardinal, i.e. $cf(\aleph_\alpha) = cf(\alpha) = \alpha$ for $\alpha > 0$.

An uncountable cardinal, κ is **inaccessible** if it is regular and $2^\lambda < \kappa$ for all $\lambda < \kappa$.

For all finite n, $2^n < \omega$ so $\aleph_0$ has the same properties as an inaccessible cardinal.

Inaccessible Cardinals and the Consistency of ZFC

If α is a limit ordinal then the partial universe V_α satisfies the axioms of ZFC except for possibly the replacement axiom [Cameron, p131].

However if α is an inaccessible cardinal then the partial universe V_α satisfies all of the axioms of ZFC. This means that any sets that can be build from sets within V_α are also contained in V_α.

We can not prove the existence of an inaccessible cardinal with recourse to the axioms of ZFC. This is similar to the existence of ω for which we had to include the axiom of infinity. In fact inaccessible cardinals can be thought of as generalisations of ω.

If we assume that an inaccessible cardinal α exists then V_α is a model for ZFC which shows that ZFC is consistent. However Godel's Second Incompleteness Theorem shows that the consistency of ZFC can not be proven from the axioms of ZFC. Hence ZFC cannot prove the existence of an inaccessible cardinal as this is equivalent to proving its own consistency.

The Axiom of Choice

The axioms of set theory do not always include choice. This is due to the controversy that has surrounded it from the beginning. This section will look at some variations of this axiom and the undesirable consequences of its inclusion.

The Axiom of Choice is not always used in the form stated earlier. Two equivalent and common variations are Zermelo's Well-Ordering Principle,

> Every set can be well-ordered

and Zorn's Lemma,

> For any partially ordered set $(X, <)$, if every subset of X that is ordered by $<$ has an upper bound then X has a maximal element.

There are many other equivalent forms of this axiom which can result in it going unnoticed in a proof. Hardy showed that to index a set of cardinality $2^{\aleph_0}$, Borel had used the axiom of choice in his proof of a continuous function $f : \mathbb{R} \to \mathbb{R}$ which does not have a double series polynomial representation. This is despite the fact that Borel objected to the axiom of choice (Herrlich 21).

The axiom of choice is independent of the ZF axioms and entails some very useful results in a wide range of fields that would not be possible in ZF alone. This includes Tychonoff's Theorem in topology, the existence of a basis for any vector space and the unique (up to isomorphism) algebraic closure of a field F.

However the full axiom of choice is not always needed. Recall that the axiom states the existence of a choice function, f on an indexed family of non-empty sets, $X = (F(i) \mid i \in I)$, such that for each $i \in I$, $f(i) \in F(i)$ and $|f(i) \cap F(i)| = 1$. This can be weakened by three different approaches:

1. Restrict the size of I, the indexing set.

2. Restrict the nature of each $F(i)$ in the indexed family of sets.

3. Change the requirement that the choice function takes only one element from each set $F(i)$.

One version that uses the first approach is **The Countable Axiom of Choice;**
Every countable family, A, of nonempty sets has a choice function.

Howard and Rubin list 383 variations of weakened choice although there are undoubtedly many more. Countable Choice is among the most commonly used forms and is also implied by **The Principle of Dependent Choice;**
If R is a binary relation on a nonempty set A and for all $x \in A$ there exists $y \in A$ such that $\langle x, y \rangle \in R$, then there exists a sequence $(x_n)_{n \in \mathbb{N}}$ in A such that $\langle x_n, x_{n+1} \rangle \in R$ for all $n \in \mathbb{N}$.

Countable Choice is sufficient to show that the countable union of countable sets is countable and to prove the closure of the Borel sets (to be defined in the following section). Dependent choice allows for countably many consecutive choices and is used in Solovay's Theorem later on.

Despite the advantages that come from including the axiom of choice there are also some paradoxical consequences in measure theory.

Basic Concepts of Measure Theory

A $\sigma - algebra$ X is a collection of subsets of a given set S, i.e. a subset of $\mathcal{P}(S)$, that satisfy the conditions

1. $S \in X$,

2. if $A \in X$ and $B \in X$ then $A \cup B \in X$,
3. if $A \in X$ then the complement $X - A \in X$,
4. if $A_n \in X$ for all n, $\bigcup_{n=0}^{\infty} A_n \in X$

X is also closed under intersections and countable intersections as these can be written in terms of union and complement.

The smallest $\sigma - algebra$ containing the open sets of $\mathbb{R}$ is B, the collection of Borel sets. These are generated by the collections $\sum_{\alpha}^{0}$ and $\prod_{\alpha}^{0}$ for $\alpha < \omega_1$ defined as;

$\sum_{1}^{0}$ = all the open sets,

$\prod_{1}^{0}$ = all the closed sets,

$\sum_{\alpha}^{0}$ = the collection of sets A, such that A is the countable union of sets belonging to $\prod_{\beta}^{0}$ for $\beta < \alpha$,

$\prod_{\alpha}^{0}$ = the collection of all the complements of sets in $\sum_{\alpha}^{0}$,
= the collection of sets A, such that A is the countable intersection of sets belonging to $\sum_{\beta}^{0}$ for $\beta < \alpha$.

Using the countable axiom of choice we can verify that the following collection is a $\sigma - algebra$ that is closed under countable intersection and union:

$$\bigcup_{\alpha<\omega_1} \sum_{\alpha}^{0} = \bigcup_{\alpha<\omega_1} \prod_{\alpha}^{0}$$

All Borel sets are Lebesgue measurable although the converse does not hold. To define the Lebesgue measure I will first define an outer measure $\mu_*(X)$ for a set $X \subset \mathbb{R}^n$.

$$\mu_*(X) = \inf \left(\sum_{k \in \mathbb{N}} v(I_k) \right)$$

Where $\{I_k \mid k \in \mathbb{N}\}$ is a set of spheres such that $X \subset \bigcup_{k \in \mathbb{N}} I_k$ and $v(I_k)$ is the volume of each sphere defined in the normal way. In $\mathbb{R}^2$ a sphere is an interval.

A set A is Lebesgue measurable if for all $X \subset \mathbb{R}^n$,

$$\mu(A) = \mu_*(A) = \mu_*(X - A) + \mu_*(X \cap A)$$

Alternatively a set A is Lebesgue measurable if and only if there exists a Borel set, B, such that the symmetric difference $A \Delta B$ has measure zero.

Some important properties of the Lebesgue measure are as follows:

- $\mu(A) \geq 0$
- The empty set and discreet points, {x}, have measure zero
- $\mu(A) \leq \mu(B)$ if $A \subset B$, this is called monotonicity.
- $\mu(I) = b - a$ where I is an interval with endpoints a, b and $a < b$
- If a set is translated by c then the measure, $\mu(A + c) = \mu(A)$, is translation invariant.
- Countable subadditivity, $\mu\left(\bigcup_1^\infty A_k\right) \leq \sum_1^\infty \mu(A_k)$. This is a strict equality if the sets A_k are disjoint.

As $\mu(\{x\}) = 0$, by the property of countable subadditivity the measure of the rationals in the interval $I = [0, 1]$ is zero. Let Q be the set of all the rationals in the interval I and R the set of all irrationals, then I is the disjoint union of Q and R. As $\mu([0, 1]) = 1$ and $\mu(Q) = 0$ then $\mu(R) = 1$ showing that the uncountable addition of discreet points all of measure zero does not necessarily give measure zero.

Vitali Set

An example of the undesirable consequences of what can be proven with the axiom of choice is the existence of the Vitali Set, a subset of the real line which is not Lebesgue measurable.

For $x \in [0, 1]$, let $V_x = \{\ y \mid\ y \in [0, 1],\ x - y \in \mathbb{Q}\}$.
The equivalence classes form a partition, $\{V_i \mid i \in I\}$, of $[0, 1]$ where,
$|I| = |\mathbb{R}|$
$|V_i| = \omega$ for all $i \in I$

By the axiom of choice we can have a selector $M = \{x_i \mid i \in I\}$ of the partition $\{V_i \mid i \in I\}$ such that $|M \cap V_i| = 1$ for all $i \in I$.

Assume for a contradiction that M is measurable.

For all distinct $x, y \in M, x - y \notin \mathbb{Q}$

Let $M_q = \{x + q \mid x \in M\}$ for all $q \in \mathbb{Q}$

Then $\bigcup_{q\in[-1,1]\cap\mathbb{Q}} M_q$ is a union of distinct sets that covers $[0,1]$. For the remainder of this proof I shall use $q \in [-1,1]$ to refer to the rationals in that interval.

$$[0,1] \subseteq \bigcup_{q\in[-1,1]} M_q \subseteq [-1,2]$$

From the monotonicity of the Lebesgue measure,

$$\mu([0,1]) \leq \mu\left(\bigcup_{q\in[-1,1]} M_q\right) \leq \mu([-1,2])$$

Due to countable sub additivity and M_q being distinct for all q,

$$\mu\left(\bigcup_{q\in[-1,1]} M_q\right) = \sum_{q\in[-1,1]} \mu(M_q)$$

As the Lebesgue measure is invariant under translation

$$\mu(M_q) = \mu(M)$$

$$1 \leq \sum_{q\in[-1,1]} \mu(M) \leq 3$$

There is no value for $\mu(M)$ such that this is true.

Hence M is not measurable.

Banach-Tarski Paradox

The Banach-Tarski paradox states that any ball it can be partitioned into five pieces that are moved using only translations and rotations and are reassembled to form two balls, each the same size as the original. It is in the partitioning of the ball that the axiom of choice is used resulting in the measure on the partition being undefined in a similar way to the Vitali set [Just and Weese].

The unit ball U can be partitioned into two sets X and Y such that $X \approx U$ and $Y \approx U$.

The relation $\approx$ is defined on $\mathcal{P}(\mathbb{R}^3)$ where $A \approx B$ if there are partitions $(A_i)_{i<n}$ of A and $(B_i)_{i<n}$ of B for $n < \omega$ such that $A_i \cong B_i$ for all $i < n$. $A \cong B$ means there exists an isometry of the sphere, ϕ, such that $\phi[A] = B$.

Solovay's Theorem

The presence of the Vitali set and the Banach-Tarski paradox show that with the axiom of choice there exists non-measurable sets. That alone does not make the axiom of choice the culprit. However, Solovay showed that it is consistent to have dependent choice with all sets of real numbers being Lebesgue measurable. This shows that it is due to the inclusion of the axiom of choice that non-measurable sets occur.

Let κ be an inaccessible cardinal. Let INC stand for the statement "There exists an inaccessible cardinal."

Theorem 1 If there is a transitive model of ZFC + INC then there is a transitive model of ZF where the following propositions are valid;
(1) The principle of dependent choice.
(2) Every set of reals is Lebesgue measurable.
(3)-(5) See Solovay for a full statement.

Although we know there exists a set that does not have a Lebesgue measure in ZFC we have not given an explicit definition of it because we are unable to do so. Part of the issue is that it is not clear how to express 'definable' by a set theoretical formula.

Myhill and Scott showed that "X is definable from some countable sequence of ordinals" is expressible with set theoretical formula where X is any set of reals. Thus the following theorem, which is similar to Theorem 1, can be formulated in set theory.

Theorem 2 If ZFC + INC has a transitive model then ZFC + GCH has a transitive model where the analog of propositions (2)-(5) from Theorem 1 hold. The analog of (2) is;

(2') Every set of reals definable from a countable sequence of ordinals is Lebesgue measurable.

The proof of Theorem 1 follows from the proof of Theorem 2. I will give a brief sketch of the details that relate to the Lebesgue measurability of all sets of real numbers. For definitions of undefined terms and the many missed details see Jech or Solovay.

Let $\mathcal{M}$ be a transitive model of ZFC. Let $B = B(P)$ be the Levy collapse for κ where P is the collection of properties of forcing that collapse each $\alpha < \kappa$ onto $\aleph_0$. Let G be an $\mathcal{M}$-generic ultrafilter on B. The requirement that G is an ultrafilter on B means it is a subset of $\mathcal{P}(B)$ such that;

- $B \in G$ and $\emptyset \neq G$
- if $X, Y \in G$ then $X \cap Y \in G$
- if $X, Y \subset B$, $X \in G$ and $X \subset Y$ then $Y \in G$
- for all $X \subset B$ either X or its complement is in G

The requirement that G is $\mathcal{M}$-generic means that if D is a dense subset of B and $D \in \mathcal{M}$ then $G \cap D \neq \emptyset$.

A model for ZFC is $\mathcal{M}[G]$, a generic extension of $\mathcal{M}$. Every element in $\mathcal{M}[G]$ has a 'name' in $\mathcal{M}$ that describes how it was constructed and G interprets these names.

We want a submodel where every set of reals can be described by a countable sequence of ordinals. Let $\mathcal{N}$ be the set of elements that are hereditary definable from a sequence of ordinals in $\mathcal{M}[G]$. Every real and sequence of ordinals in $\mathcal{M}[G]$ is in $\mathcal{N}$ and dependent choice holds in $\mathcal{N}$.

For all sets of reals $X \in \mathcal{M}$, X is M-R-definable in $\mathcal{M}[G]$ and X is Lebesgue measurable in $\mathcal{M}[G]$. Hence there exists Borel sets C, D in $\mathcal{M}[G]$, where D is null meaning it has 0 measure, such that

$$C \Delta X \subseteq D$$

D is null in $\mathcal{N}$ so X is Lebesgue measurable in $\mathcal{N}$.

The Category of Sets

In contrast to set theory, category theory does not place primary importance on the element membership of an object. The element of a set A can be expressed in terms of a mapping. In talking about a mapping, u, from the domain A to the codomain B, I will use the notation $A \xrightarrow{u} B$. An element b, of a set A is equivalent to the mapping with the terminal object 1 as its domain and A as its codomain,

$$1 \xrightarrow{b} A$$

Looking at a composition

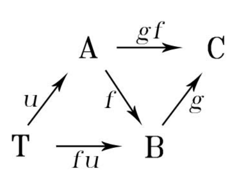
$$1 \xrightarrow{a} A \xrightarrow{f} B$$

reveals that fa is an element of B.

The associative law is a generalized version of this, for some T let

$$T \xrightarrow{u} A$$

$$\text{if } T \xrightarrow{u} A \xrightarrow{f} B \xrightarrow{g} C, \quad \text{then } g(fu) = gf(u)$$



With this it is possible to define a category as possessing the following data:

- A set of objects, O which are a special sort of mapping.
- A set of morphisms, M, also referred to as maps or arrows.
- For each arrow, f in M, there is an associated domain, A, and a codomain, B, where A and B are objects in O and

$$A \xrightarrow{f} B$$

- For arrows, f, g, with $codomain(f) = domain(g)$

$$A \xrightarrow{f} B \text{ and } B \xrightarrow{g} C$$

  there is an assigned composite arrow, gf such that

$$A \xrightarrow{gf} C$$

- For each object, A, in O there is an assigned arrow, 1_A called the identity on A

$$A \xrightarrow{1_A} A$$

The category of sets as articulated by the following axioms is capable of providing a foundation for number theory, analysis and much of algebra and topology without a clearly defined membership relation. This partially demonstrates that substance is not necessary to carry mathematical information as invariant form is sufficient.

Category Axiom

Axiom Abstract sets and maps form a category, S.

The objects are sets and the arrows are maps and S satisfies the conditions above. From now on I will talk specifically in relation to this category and refer to 'sets' instead of the general 'object' even if a statement is applicable to other object types.

Limit Axiom

Axiom The limits and colimits for any finite data are in S.

Limits and colimits are dual notions. To define these it is instructive to first look at the example of the dual sets 0 and 1.

Instead of referring to a singleton with a particular element we talk about the object 1, the terminal set, disregarding the particular element that is its single member. It does not matter if there is a unique terminal set or if there are many of them, the only properties of interest are the mappings between the terminal set and other sets. For any set A there exists a unique mapping $A \longrightarrow 1$.
The initial set is 0, which means for any set A there is a unique mapping $0 \longrightarrow A$. The initial set has no elements and like the empty set in ZFC it is unique.
The mapping $1 \longrightarrow A$ exists if A is nonempty and the number of mappings corresponds to the number of elements of A as seen above. However $1 \longrightarrow 0$ is not defined. The only set A for which $A \longrightarrow 0$ exists is the empty set, and there is only one mapping.

The limit property of the terminal set 1 is the existence of a unique map from every set A to 1. The dual property or colimit is the existence of a unique map from the initial or empty set 0, to every set A.

To give the formal definition of a limit requires a definition of data. The axiom only applies to data that is finite.

Let A_i be a family of sets and I the set of indices.
Let f_j be the family of mappings between the sets in A_i and let J be the set of indices of f_j.
A data type is of the form

$$J \underset{\mathrm{c}}{\overset{\mathrm{d}}{\rightrightarrows}} I$$

where the map d gives a set from A_i, namely with an index in I, to be the domain of a mapping with index in J, and the map c gives the set which is the codomain of that same mapping.

For an element j in J, there are maps d and c,

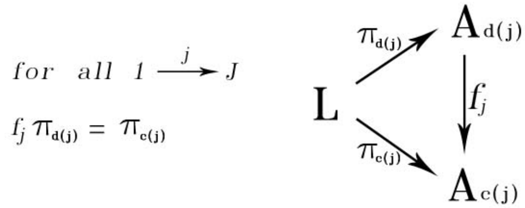
$$1 \xrightarrow{j} J \overset{\mathrm{d}}{\underset{\mathrm{c}}{\rightrightarrows}} I$$

such that there is a map between the two sets indexed by d(j), c(j) in I

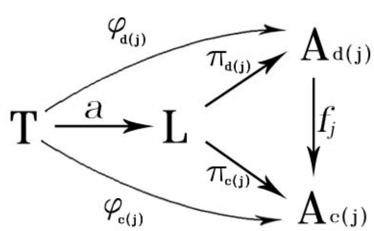
$$A_{d(j)} \xrightarrow{f_j} A_{c(j)}$$

The limit for some A_i, f_j as above is given by the single set L and a universal cone with vertex L and a base defined by the family of maps,

$$\text{for } 1 \xrightarrow{i} I, \quad L \xrightarrow{\pi_i} A_i$$



The cone is universal because for any set T such that T has a map associated with every set that L had a map associated with, then there exists a unique map $T \xrightarrow{a} L$



Axiom of Choice

Similar to the axiom of choice of ZFC this axiom means that every surjective map is invertible.

Axiom Every epimap has a section.

$$Let\ A \xrightarrow{f} B$$

then the map s is a section of the map f if s is injective and

$$B \xrightarrow{s} A$$

If s is a section of f then $fs = 1_B$.

f is an epimap if it has the right-cancellation property

$$\forall \phi, \psi[\phi f = \psi f \Rightarrow \phi = \psi]$$

$$\text{If } A \xrightarrow{f} B, \text{ then for arbitrary } C, \ A \xrightarrow{f} B \overset{\phi}{\underset{\psi}{\rightrightarrows}} C$$

Instead of referring to a map $A \xrightarrow{f} B$, f can be seen as a family of sets

$$A_b = \{a \mid f(a) = b\}$$

A section s for the map f is a rule that chooses exactly one element from each set in A_b.

$fs = 1_B$
$\Rightarrow f(sb) = b$
$\Rightarrow s(b) \in A_b$ for all b.

The category of order-preserving mappings between partially ordered sets satisfies all the axioms of the category of sets except the axiom of choice showing that choice is independent.

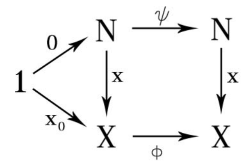
Dedekind-Peano Axiom

This is a statement about the existence of an infinite object called a natural number object, N. Its existence is expressed in terms of a sequence starting with an initial element and having the equivalent of a successor relationship. The term ‘sequence’ denotes a map in S with N as its domain.

Axiom There exists a mapping $1 \xrightarrow{0} N \xrightarrow{\psi} N$ in S such that for any mapping

$$1 \xrightarrow{x_0} X \xrightarrow{\phi} X$$

there exists a unique sequence x such that $x0 = x_0$ and $x\psi = \phi x$



Mapping Set Axiom

Axiom There is a mapping set Y^X for any objects X and Y in S.

For each arrow $B \to Y^X$ there is an assigned arrow in $B \times X \to Y$ and vice versa. This is written,

$$\frac{B \to Y^X}{B \times X \to Y} \uparrow\downarrow$$

When B is 1 we can see that the number of elements in Y^X must be the same as the number of arrows or mappings $X \to Y$.

In particular for each map $B \times X \xrightarrow{f} Y$ there is a unique map $B \xrightarrow{g} Y^X$ for which $g \times 1_X = f$.

Axiom of Truth Value Representation

Axiom There exists a truth value object $1 \xrightarrow{v_1} V$ and a one to one correspondence between parts (up to equivalence) of an object A and the mappings $A \to V$.

Let V be a truth value set and $1 \xrightarrow{v_1} V$ a fixed element of V which can be called 'true'.

A part, i, of a set A is a mapping into A which is a monomorphism (it has left cancellation) meaning it keeps the elements of the domain distinct. For $U = domain(i)$, $U \xrightarrow{i} A$.

There exists a characteristic function φ, $A \xrightarrow{\varphi} V$ on a part i of a set A if and only if the elements of A which are members of the part i are exactly the elements which the function φ gives the value 'true' in V.

As this is a universal property, for any T and mapping $T \xrightarrow{a} A$

$$a \in_A i$$
$$\Leftrightarrow \varphi a = v_1 T$$

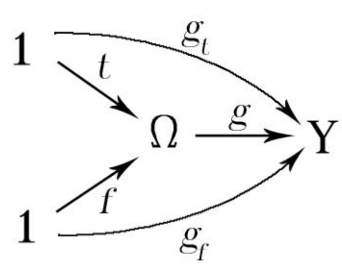
Where $a \in_A i$ means $\exists \overline{a}\ T \xrightarrow{\overline{a}} U$ such that $a = i\overline{a}$ and $v_1 T$ is the constant map $T \xrightarrow{T} 1 \xrightarrow{v_1} V$.

When $V = 2$ all parts of all sets have a unique characteristic function.

Boolean Axiom

Axiom S is Boolean.

There is an object Ω such that $\begin{cases} t \\ f \end{cases} : 1 + 1 \rightarrow \Omega$ where t, f are injections and as Ω is the sum of the two sets 1 and 1 then for all Y there is a unique mapping g such that



As g is unique 1 and 1 exhaust Ω meaning there is no element of Ω which is not mapped to by either t or f.

Two-Valued Axiom

Axiom S is Two-Valued.

This simply asserts the existence of an object with more than one element.

That completes the axioms for the category of sets.

These axioms are not able to talk about cardinals greater than $\aleph_\omega$. However, the category of sets was devised as a foundation for analysis and most of algebra and topology where such large cardinals rarely occur. It is possible to extend these axioms but in Lawvere's opinion if one wanted to go beyond this it would be better to use the category of categories.

Conclusion

The "working mathematician" is wise not to be taken in by a quixotic desire for a complete consistent formal system. There is no direct answer for what 'the' foundation of mathematics should be and so this is not a conclusive conclusion. Set theory and category theory are not solely concerned with foundations although they offer many different version, ZFC and the Category of Sets are only two possibilities.

Bibliography

Awodey, S
An Answer to Hellman's Question: 'Does Category Theory Provide a Framework for Mathematical Structuralism?', in Philosophia Mathematica, Vol. 12, (2004), pp.54-64.

Burk, F.
'Lebesgue Measure and Integration'. John Wiley and Sons, Inc : New York, 1998.

Cameron, P.
'Sets, Logic and Categories'. Springer : London, 1999.

Herrlich, H.
'Axiom of Choice'. Springer : The Netherlands, 2006.

Jech, T.
'Set Theory'. 3rd Edition. Springer : Berlin, 2003.

Just, W. and Weese, M.
'Discovering Modern Set Theory. I'. American Mathematical Society : 1996.

Landry, E. and Marquis, J.
Categories in Context: Historical, Foundational, and Philosophical in Philosophia Mathematica, Vol. 13, (2005), pp.1-43.

Lawvere, F.W.
Cohesive Toposes and Cantor's 'lauter Einsen' in Philosophia Mathematica, Vol. 2, (1994), pp.5-15.

An Elementary Theory of the Category of Sets (Long Version) with Commentary, in Reprints in Theory and Applications of Categories, No. 11, (2005), pp.1-35.

Foundations and Applications: Axiomatization and Education, in The Bulletin of Symbolic Logic, Vol. 9, No. 2. (Jun., 2003), pp 213-224.

Lawvere, F.W. and Rosebrugh, R.
'Sets for Mathematics'. Cambrigde University Press : Cambridge, 2003.

Mayberry, J.P.
What is Required of a Foundation for Mathematics?, in Philosophia Mathematica, Vol. 2, (1994), pp.16-35.

'The Foundations of Mathematics in the Theory of Sets'. Cambridge University Press : New York, 2001.

Shapiro, S.
Categories, Structures, and the Frege-Hilbert Controversy: The Status of Metamathematics, in Philosophia Mathematica, Vol. 13, (2005), pp.61-77.

Simpson, S.
Anti-foundation and the Category of Sets, (June 8, 2000), from Foundations of Mathematics forum viewed at http://cs.nyu.edu/pipermail/fom/2000-June/004042.html

Solovay, R.
A Model of Set Theory in Which Every Set of Reals is Lebesgue Measurable in The Annals of Mathematics, 2nd Ser., Vol. 92, No. 1. (Jul., 1970), pp. 1-56.

Vaught, R.
'Set Theory: An Introduction'. 2nd Edition. Birkhauser : Berlin, 1995.