



UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2017:33

The relative consistency of the Axiom of Choice and the Generalized Continuum Hypothesis with the Zermelo-Fraenkel axioms: The constructible sets L

Christoffer Hindlycke

Examensarbete i matematik, 15 hp
Handledare: Vera Koponen
Examinator: Jörgen Östensson
Augusti 2017

A large, faint watermark of the Uppsala University seal is visible in the bottom right corner of the page. The seal features a sun with rays and the Latin motto "VERITAS LIBERABIT VOS".

Department of Mathematics
Uppsala University

The relative consistency of the Axiom of Choice and the
Generalized Continuum Hypothesis with the
Zermelo-Fraenkel axioms: The constructible sets **L**

Christoffer Hindlycke

August 4, 2017

Contents

Introduction	2
Historical background	2
Sources and overview	2
Prerequisite axioms, definitions and results	3
The axioms and GCH	3
Definitions and results	9
Constructible sets	15
Constructing what is constructible: Defining \mathbf{L}	15
\mathbf{L} as a model of the basic axioms	15
Simplifying relative proofs: The Axiom of Constructibility	20
AC and GCH in \mathbf{L}	23
At the end of all things: Excluded results	25

Introduction

Historical background

Set theory was, for all intents and purposes, created by Georg Cantor in 1874. It was eventually discovered (the interested reader is encouraged to look up Russell's Paradox) that naive set theory, wherein any collection of objects fulfilling a certain property was considered a set, led to contradictions. This in turn led to several axiomatizations of set theory, of which eventually the Zermelo-Fraenkel axioms (ZF) became the norm.

It was for roughly 30 years an open question as to whether the Axiom of Choice and the Generalized Continuum Hypothesis were consistent with the set-theoretic axioms. The Axiom of Choice in particular allows for a great many interesting results, and was at the time (and by some mathematicians, still today) considered quite controversial.

In 1938, Kurt Gödel published an article [2], followed in 1940 by a small book [1], the latter proving in detail that AC and GCH are indeed consistent. This was accomplished by a rather ingenious recursive construction of a set-theoretic universe called \mathbf{L} , using the ordinal numbers as a base. Though Gödel's most famous result is his Incompleteness Theorem, constructing \mathbf{L} must also be considered a monumental achievement.

As mentioned above, \mathbf{L} begins with the universe of the ordinal numbers. \mathbf{L} is then recursively constructed, starting with the empty set, by only taking as members such ordinal numbers that are intuitively definable using first-order logic.

With the Axiom of Choice now proven to be consistent, many new results were made possible, and many existing results (which assumed AC or a weaker version) validated. One exceptionally important such result, Tychonoff's Theorem, relates to topology: It states that the product of any collection of compact topological spaces is compact with respect to the product topology. There are a great many other theorems in virtually all areas of mathematics, mainly because the Axiom of Choice seems to be (intentionally or not) assumed to be valid by many mathematicians.

Sources and overview

This paper is a literature study of Set Theory: An introduction to independence proofs (1980) by Kenneth Kunen, and all results originate from this book. The author's meager contributions consist of occasionally clarifying definitions (some are originally stated in an informal manner), fixing obvious typos, adding missing proofs, and expanding on/formalizing some informal proofs.

Particular interest has been paid to chapter VI, wherein the class of constructible sets \mathbf{L} is defined. However, chapters I, III, IV, V are essential to understanding \mathbf{L} and so many definitions and results from these chapters make an appearance (chapter II is necessary only to prove combinatorial properties of \mathbf{L} and so has been omitted).

The purpose of the paper is to define \mathbf{L} in a mathematically rigorous way, and then proceed to prove that \mathbf{L} fulfills all relevant set-theoretic axioms along with GCH.

Note that some previous experience with mathematical logic is required on the part of the reader: We do not define the logical operators/quantifiers here, and a certain familiarity with a number of set theoretical and logical notions (union, intersection, transfinite induction, classes and sets etc.) is assumed.

Prerequisite axioms, definitions and results

Here are laid out the axioms, definitions and results we need to describe what constructible sets are, with accompanying comments aimed at facilitating understanding of the concepts.

All axioms, definitions and results are taken from [3]. Some minor alterations, particularly to definitions, have been made in the interest of clarity and/or compactness.

The axioms and GCH

The foundation of our foray into set theory shall be ten basic axioms, from which all results will be derived. These axioms are as follows:

Axiom 0 (Set Existence).

$$\exists x(x = x)$$

This axiom states that there exists a set. Clearly, there must exist a set for our fledgling set theory to go anywhere, and so this basic axiom is traditionally labelled as Axiom 0.

Axiom 1 (Extensionality).

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

Extensionality states that a set is uniquely determined by its members. Note that we do not define "order" for members of a set yet (i.e. which member comes "before" another).

Axiom 2 (Foundation).

$$\forall x (\exists y (y \in x) \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y)))$$

Foundation implies that no set is an element of itself, and has several other interesting implications, as we shall see later on.

For the next axiom, we need to make a few definitions. In these definitions and those to come, note that v_0, v_1, v_2, \dots are symbols called variables. We are not restricted to these however; x, y, z, X, Y, u and so on may also denote variables, depending on context. A variable is simply a way to refer to something, an object, within our universe.

Definition 1. A formula is any expression constructed by the following rules:

- (1) $v_i \in v_j, v_i = v_j$ are formulas for any i, j
- (2) If ϕ and ψ are formulas, so are $\phi \wedge \psi, \phi \vee \psi, \neg \phi, \exists v_i(\phi), \forall v_i(\phi), \phi \rightarrow \psi$ and $\phi \leftrightarrow \psi$

Definition 2. A subformula of a formula ϕ is a consecutive sequence of symbols of ϕ which form a formula.

Definition 3. The scope of an occurrence of a quantifier $\exists v_i$ or $\forall v_i$ is the unique subformula beginning with that $\exists v_i$ or $\forall v_i$.

Definition 4. An occurrence of a variable in a formula is called bound if it lies in the scope of a quantifier acting on that variable, otherwise it is called free.

So a formula is made up of the basic symbols $=$, \neq (short for $\neg(a = b)$), \in , \notin (short for $\neg(a \in b)$), variables, and the logical operators/quantifiers. Parentheses are used to partition formulas, so that it is clear which operators/quantifiers act on which expressions.

However, when there is no risk of confusion, parentheses are typically left out. Two such examples are $\forall x \in y \phi$, being short-hand for $\forall x(x \in y \rightarrow \phi)$, and likewise for $\exists x \in y \phi$, meaning $\exists x \in y(x \in y \rightarrow \phi)$. Evidently, there are more short-hands than we have explained here; hopefully they will be self-explanatory as they appear.

Axiom 3 (Comprehension Scheme). For each formula ϕ with free variables among x, z, w_1, \dots, w_n ,

$$\forall z \forall w_1, \dots, w_n \exists y \forall x (x \in y \leftrightarrow x \in z \wedge \phi)$$

Comprehension says that for every set the collection of elements in it satisfying a specific property is also a set.

Axiom 4 (Pairing).

$$\forall x \forall y \exists z (x \in z \wedge y \in z)$$

Pairing, as the name suggests, states that for any two elements, there exists a set containing them. Before we state the Union axiom, we define what a subset is.

Definition 5. A is a subset of B , denoted $A \subset B \Leftrightarrow \forall x \in A (x \in B)$.

Axiom 5 (Union).

$$\forall \mathcal{F} \exists A \forall Y \forall x (x \in Y \wedge Y \in \mathcal{F} \rightarrow x \in A)$$

Union states that, for any set \mathcal{F} , there exists a set A such that each member of \mathcal{F} is a subset of A . In other words, for any set C , we can take a set containing the elements **of the elements** of C , essentially allowing us to "boil down" sets. Union, in conjunction with Pairing and Comprehension, also allows us to take the union of sets.

Axiom 6 (Replacement Scheme). For each formula ϕ with free variables among x, y, A, w_1, \dots, w_n ,

$$\forall A \forall w_1, \dots, w_n (\forall x \in A \exists! y (\phi) \rightarrow \exists Y \forall x \in A \exists y \in Y (\phi))$$

Replacement says that, if for each $x \in A$ there exists a unique y such that $\phi(x, y)$ holds, we can form a set containing these y .

Another two definitions are required for our next two axioms.

Definition 6. 0 (also called the empty set) is the unique set such that $\forall x(x \notin 0)$.

Definition 7. The successor of α , $S(\alpha)$, is defined as $S(\alpha) = \alpha \cup \{\alpha\}$.

So the empty set, as one might deduce, contains no objects (thereby making it a subset of every set, including itself!), and the successor of any set A is the set A in union with the set containing the set A . We can now move on to Axiom 7.

Axiom 7 (Infinity).

$$\exists x(0 \in x \wedge \forall y \in x(S(y) \in x))$$

Infinity stipulates that there is a set of natural numbers (map the empty set to 0, the successor of the empty set to 1, etc., modified slightly if you prefer your natural numbers sans 0).

Axiom 8 (Power Set).

$$\forall x \exists y \forall z (z \subset x \rightarrow z \in y)$$

The Power Set axiom lets us define the power set of a set:

Definition 8. For a set x , the power set $\mathcal{P}(x)$ is defined as $\mathcal{P}(x) = \{z : z \subset x\}$.

The power set of a set a is then the set consisting of all possible subsets of a (including a itself), and the Power Set axiom, together with Comprehension, states that this set always exists.

Our final axiom will require a bit of work. We first define an ordered pair.

Definition 9. The ordered pair $\langle x, y \rangle$ is the set $\{\{x\}, \{x, y\}\}$.

So an ordered pair is simply two elements with a means of keeping track which element comes "first". Next, we define a relation.

Definition 10. A relation R is a set, all of whose elements are ordered pairs. We define $\text{dom}(R) = \{x : \exists y(\langle x, y \rangle \in R)\}$, $\text{ran}(R) = \{y : \exists x(\langle x, y \rangle \in R)\}$. We write xRy when $\langle x, y \rangle \in R$.

Now we can begin defining different orderings (we shall need two).

Definition 11. A total ordering is a pair $\langle A, R \rangle$ where A is a set, R is a relation and the following holds:

1. R is transitive: $\forall x, y, z \in A(xRy \wedge yRz \rightarrow xRz)$.
2. R satisfies trichotomy: $\forall x, y \in A(xRy \vee yRx \vee x = y)$.
3. R is irreflexive: $\forall x \in A(\neg(xRx))$.

Definition 12. $\langle A, R \rangle$ is a well-ordering (R well-orders A) if $\langle A, R \rangle$ is a total ordering, and every non-empty subset of A has an R -least element; i.e., for any $B \subset A$, $B \neq \emptyset$, $\exists x \in B \forall y \in B(x \neq y \rightarrow xRy)$.

We now have enough background to define our final axiom.

Axiom 9 (Choice).

$$\forall X \exists R (R \text{ well-orders } X)$$

The Axiom of Choice (AC) says that for any set, there exists a well-ordering for that set.

This collection of ten axioms is known as ZFC (Zermelo-Fraenkel-Choice).

Finally, we need to define GCH, the Generalized Continuum Hypothesis.

This requires quite some work; we need to understand both ordinals and cardinals in order to proceed. Below is a very brief introduction on the subject, sufficient to allow us to state our definition of GCH.

Definition 13. A set x is transitive if every element of x is a subset of x .

Definition 14. x is an ordinal if x is transitive and well-ordered by \in .

Definition 15. α is a successor ordinal if $\exists \beta (\alpha = S(\beta))$.

α is a limit ordinal if $\alpha \neq 0$ and α is not a successor ordinal.

Definition 16. $\mathbf{ON} = \{x : x \text{ is an ordinal}\}$.

Note that \mathbf{ON} is not a set, but rather a proper class (a concept we are taking care in not formally defining). Essentially, the ordinals are "too large" to constitute a set.

In addition to being necessary for defining GCH, the class of ordinals (also called the ordinal numbers) \mathbf{ON} will later form the base from which we create **L**. Thankfully, successor ordinals are not difficult to visualize. We shall call the empty set 0 (as we defined it earlier), the ordinal number $S(0) = \{0\}$ shall be called 1 , $S(1) = \{0, \{0\}\}$ shall be called 2 etc.

So for any successor ordinal j , we have $j = \{0, 1, \dots, j-2, j-1\}$. Limit ordinals are slightly more difficult; it may be easiest to simply think of them as infinity (though there's more than one infinity here).

We shall also state as a fact that, in any non-empty set of ordinal numbers, there exists a least ordinal number with respect to \in (this follows directly from definition 12 and 14).

Definition 17. ω is the set of natural numbers: $0 \in \omega \wedge \forall x \in \omega (S(x) \in \omega)$.

Theorem 1. *If $\langle A, R \rangle$ is a well-ordering, then there is a unique ordinal C such that $\langle A, R \rangle \cong C$ (where, for $\alpha, \beta \in \mathbf{ON}$, $\alpha \cong \beta$ means that there exists an order-preserving isomorphism between α and β).*

The proof of this theorem will be excluded. For details, please see [3] Ch. 1 §7 Theorem 7.6.

Definition 18. If $\langle A, R \rangle$ is a well-ordering, $\text{type}(A, R)$ is the unique ordinal C such that $\langle A, R \rangle \cong C$.

The type of a well-ordering is the unique ordinal which, along with \in , is isomorphic to that well-ordering. By Theorem 1 above, such a unique ordinal always exists.

Definition 19. For $\alpha, \beta, \xi, \eta \in \mathbf{ON}$, $\alpha + \beta = \text{type}(\alpha \times \{0\} \cup \beta \times \{1\}, R)$ where $R = \{\langle \xi, 0 \rangle, \langle \eta, 0 \rangle : \xi < \eta < \alpha\} \cup \{\langle \xi, 1 \rangle, \langle \eta, 1 \rangle : \xi < \eta < \beta\} \cup ((\alpha \times \{0\}) \times (\beta \times \{1\}))$.

When performing the operation $\alpha + \beta$, imagine that we "paint" every element in α blue, and every element in β red. When comparing two elements from $\alpha + \beta$, we say that any blue element is always "less than" any red element, but when comparing blue elements to blue or red elements to red, we use the regular ordinal ordering (i.e. \in). This then allows us to find an ordinal isomorphic to $\alpha + \beta$ using our blue-red ordering, where ordinals are isomorphic if there exists a bijective function between them that is order-preserving. Ordinal addition functions as you would expect, except when it comes to infinite ordinals, where it is not commutative: While $\omega + 1$ is indeed a larger ordinal than ω , $1 + \omega$ is the same as ω , as we can find a bijective order-preserving function $g : 1 + \omega \rightarrow \omega$ (where the \rightarrow arrow means that the function is bijective). Simply define

$$g(\langle \alpha, \beta \rangle) = \begin{cases} 0 & \text{if } \beta = 0 \\ \alpha + 1 & \text{otherwise} \end{cases}$$

wherein we shift every element of ω "one step to the right" to make room for the smallest element in $1 + \omega$, almost verbatim a re-enactment of Hilbert's Hotel. This preserves the ordering (the smallest element in $1 + \omega$ becomes the smallest element in ω). This also explains why $\omega + 1 > \omega$; if we were to create a bijection $h : \omega + 1 \rightarrow \omega$, we would have to map the 1 to the largest element in ω to preserve order, but ω has no largest element, and therefore no such order-preserving bijection is possible.

Definition 20. If a set A can be well-ordered, the cardinality of A , denoted $|A|$, is the least ordinal α such that there exists a bijective function $f : \alpha \rightarrow A$.

The cardinality of a set is simply the "number" (where we use a cardinal to denote that number) of elements of the set. A cardinal is then simply an ordinal such that we can find no bijection from the cardinal to a "smaller" ordinal.

Definition 21. An ordinal α is a cardinal if $|\alpha| = \alpha$.

Definition 22. For every ordinal α , α^+ is the least cardinal larger than α . κ is a successor cardinal if $\kappa = \alpha^+$ for some cardinal α . κ is a limit cardinal if $\kappa > \omega$ and is not a successor cardinal.

Definition 23. ω_α is defined by transfinite recursion on $\alpha \in \mathbf{ON}$ by

- (a) $\omega_0 = \omega$.
- (b) $\omega_{\alpha+1} = (\omega_\alpha)^+$.
- (c) For a limit ordinal γ , $\omega_\gamma = \sup\{\omega_\alpha : \alpha < \gamma\}$.

Note that $\sup\{\omega_\alpha : \alpha < \gamma\}$ is then the same as $\bigcup\{\omega_\alpha : \alpha < \gamma\}$.

It is clear that all finite ordinals are cardinals: If not, we would be able to, for at least one finite ordinal, find a bijection onto a smaller ordinal (essentially meaning that, for some $j, i, j < i$ while simultaneously $j = i$). All ordinals of the form ω_α are also cardinals. Note that the definition of cardinal does not require an **order-preserving** bijection to exist; hence, $\omega + 1$ is not a cardinal, as since we do not care about preserving the order, we can simply create a similar bijection as that between ω and $1 + \omega$ earlier.

Definition 24. $A^n = \{f : f \text{ is a function} \wedge \text{dom}(f) = n \wedge \text{ran}(f) \subset A\}$.

Normally we would interpret A^n as the set of ordered n -tuples of elements from A . However, in set theory, an ordered n -tuple of elements from A is considered a function from $n = \{0, 1, \dots, n-1\}$ to A .

Definition 25. For κ, λ cardinals, $\kappa^\lambda = |\kappa^\lambda|$.

The above definition requires some explaining. Here, κ^λ stands for the cardinal κ raised to the power of the cardinal λ , while $|\kappa^\lambda|$ is the cardinality of the set of functions from λ to κ . The intended meaning hereafter should be deducible from the context.

So cardinal exponentiation is defined in terms of the "number" (again defined in terms of a cardinal) of possible functions from one cardinal to the other.

Definition 26. The generalized continuum hypothesis (GCH) states that, for every ordinal α , $2^{\omega_\alpha} = \omega_{\alpha+1}$.

GCH states that, for each infinite cardinal λ , you have no cardinal "between" λ and the cardinality of its power set. This makes a certain amount of intuitive sense, especially when you consider the non-generalized Continuum Hypothesis: There exists no set β such that $|\mathbb{Z}| < |\beta| < |\mathbb{R}|$.

Our foundations thus laid, we can move on to prerequisite results and their accompanying definitions.

Definitions and results

A number of definitions and results are necessary for creating the constructible sets, and will therefore be laid out here. Attempts have typically been made to provide brief explanations (where definitions are not entirely self-explanatory) and proof ideas, with a few exceptions to the latter: Certain proofs are quite involved and would detract from the purpose of this paper, and so have been left out (we have provided references to where in [3] to find the excluded proofs when this is done).

Definition 27. A sentence is a formula with no free variables.

Definition 28. For \mathcal{F} a set, define $\bigcup \mathcal{F} = \{x : \exists Y \in \mathcal{F}(x \in Y)\}$

As we remarked on above with the union and comprehension axioms, the union operation returns the elements **of the elements** of a set \mathcal{F} . The "regular" union that we are accustomed to, for say sets A, B , is then simply equal to $\bigcup\{A, B\}$ (we get all the elements of A and B together, as expected). For the definition below, note that, for a function f , $f \upharpoonright s$ means f restricted to the domain s .

Definition 29. We define the definable functions as follows: For A a set, R a relation, $n \in \omega$, and $i, j < n$,

- (a) $\text{Proj}(A, R, n) = \{s \in A^n : \exists t \in R(t \upharpoonright n = s)\}$.
- (b) $\text{Diag}_{\in}(A, n, i, j) = \{s \in A^n : s(i) \in s(j)\}$.
- (c) $\text{Diag}_{=} (A, n, i, j) = \{s \in A^n : s(i) = s(j)\}$.
- (d) By recursion on $k \in \omega$, define $\text{Df}'(k, A, n)$ by:
 - (i) $\text{Df}'(0, A, n) = \{\text{Diag}_{\in}(A, n, i, j) : i, j < n\} \cup \{\text{Diag}_{=} (A, n, i, j) : i, j < n\}$.
 - (ii) $\text{Df}'(k+1, A, n) = \text{Df}'(k, A, n) \cup \{A^n \setminus R : R \in \text{Df}'(k, A, n)\} \cup \{R \cap S : R, S \in \text{Df}'(k, A, n)\} \cup \{\text{Proj}(A, R, n) : R \in \text{Df}'(k, A, n+1)\}$.
- (e) $\text{Df}(A, n) = \bigcup \{\text{Df}'(k, A, n) : k \in \omega\}$

This definition, which will turn out to be of critical importance later, warrants some explanation. What we are doing is essentially "coding" all possible atomic claims (of which there are only two: Given a, b , possible atomic claims are $a = b$ and $a \in b$). This is the intuitive backdrop to $\text{Proj}(A, R, n)$, $\text{Diag}_{\in}(A, n, i, j)$ and $\text{Diag}_{=} (A, n, i, j)$.

The recursion that follows is almost identical to the way we define formulas in first order logic: The different sets that are added are then a means of "coding" equivalents of negation (complement), conjunction (intersection) and existential quantification (projection). We do not need to explicitly add equivalents to \forall and \wedge , as they can be "rewritten" using existential quantification and conjunction; see the explanation following definition 30 below.

Definition 30. Let \mathbf{M} be any class; then for any formula ϕ we define $\phi^{\mathbf{M}}$, the relativization of ϕ to \mathbf{M} , by induction on ϕ as follows:

- (a) $(x = y)^{\mathbf{M}}$ is $x = y$.
- (b) $(x \in y)^{\mathbf{M}}$ is $x \in y$.
- (c) $(\phi \wedge \psi)^{\mathbf{M}}$ is $\phi^{\mathbf{M}} \wedge \psi^{\mathbf{M}}$.

- (d) $(\neg\phi)^{\mathbf{M}}$ is $\neg(\phi^{\mathbf{M}})$.
- (e) $(\exists x \phi)^{\mathbf{M}}$ is $\exists x(x \in \mathbf{M} \wedge \phi^{\mathbf{M}})$.

We do not define $(\forall x \phi)^{\mathbf{M}}$, as this is equal to $(\neg\exists x (\neg\phi))^{\mathbf{M}}$, which is already defined. For the same reason, disjunction is not defined: $(x \vee y)^{\mathbf{M}}$ is equivalent to $(\neg(\neg x \wedge \neg y))^{\mathbf{M}}$.

Definition 31. $\mathbf{V} = \{x : x = x\}$.

\mathbf{V} is the universe we are working in.

Definition 32. Let \mathbf{M} be any class.

- (a) For a sentence ϕ , " ϕ is true in \mathbf{M} " means that $\phi^{\mathbf{M}}$ is true in \mathbf{V} .
- (b) For a set of sentences S , " S is true in \mathbf{M} " or " \mathbf{M} is a model of S " means that each sentence in S is true in \mathbf{M} .

In the definition of relativization, we start with the basic statements that two sets are equal, and one set belongs to another set. The following steps then allow us to inductively add statements that use negation, conjunction, disjunction and quantifiers.

Relativizing a formula to a class \mathbf{M} is then simply a matter of "translating" it into the language of, i.e. the objects available in, the universe \mathbf{M} , thus allowing us to determine if it holds or not.

Definition 33. If s and t are functions with $\text{dom}(s) = \alpha$ and $\text{dom}(t) = \beta$, the function $s \frown t$ with domain $\alpha + \beta$ is defined by: $(s \frown t) \upharpoonright \alpha = s$ and $(s \frown t)(\alpha + \xi) = t(\xi)$ for all $\xi < \beta$.

This definition simply states that we can extend the function s with the function t , by letting s "handle" any input from its domain α , and similarly letting t "handle" any input from its domain β , and thereby creating a function defined on $\alpha + \beta$. Thus, if $s \in A^n$, $t \in A^m$, we have that $s \frown t$ is equal to the concatenation of s and t ; i.e. the $(n + m)$ -tuple that first lists all elements of s , followed by all elements of t .

Definition 34. For S a set of sentences, we say that S is consistent (denoted $\text{Con}(S)$) if for no ϕ does $S \vdash \phi$ and $S \vdash \neg\phi$. If S is not consistent, it is inconsistent.

A set of sentences being consistent simply means they do not give rise to any contradictions (we cannot both prove and disprove the same thing).

Definition 35. For A a set, R a relation, R is extensional on A if $\forall x, y \in A (\forall z \in A (zRx \leftrightarrow zRy) \rightarrow x = y)$

An extensional relation then allows us to uniquely identify sets using it. Replace R with \in in the above definition and you have the Axiom of Extensionality.

Definition 36. By transfinite recursion, define $R(\alpha)$ for $\alpha \in \mathbf{ON}$ by

- (a) $R(0) = 0$.
- (b) $R(\alpha + 1) = \mathcal{P}(R(\alpha))$.
- (c) $R(\alpha) = \bigcup_{\xi < \alpha} R(\xi)$ when α is a limit ordinal.

Definition 37. $\mathbf{WF} = \bigcup \{R(\alpha) : \alpha \in \mathbf{ON}\}$.

Definition 38. Let ϕ be a formula with at most x_1, \dots, x_n free, and \mathbf{M}, \mathbf{N} be classes.

1. If $\mathbf{M} \subset \mathbf{N}$, ϕ is absolute for \mathbf{M}, \mathbf{N} if

$$\forall x_1, \dots, x_n \in \mathbf{M} (\phi^{\mathbf{M}}(x_1, \dots, x_n) \leftrightarrow \phi^{\mathbf{N}}(x_1, \dots, x_n)).$$

2. ϕ is absolute for \mathbf{M} if ϕ is absolute for \mathbf{M}, \mathbf{V} ; equivalently

$$\forall x_1, \dots, x_n \in \mathbf{M} (\phi^{\mathbf{M}}(x_1, \dots, x_n) \leftrightarrow \phi(x_1, \dots, x_n)).$$

Absoluteness of a formula implies that said formula holds in any model "larger" than the smallest possible model required for it to hold. Absoluteness is generally very useful; if we can establish that a formula is absolute, showing that a model in which it holds is a subset (or subclass) of the universe we are in then suffices to prove that the formula holds in our universe.

Definition 39. If $x \in \mathbf{WF}$, $\text{rank}(x)$ is the least $\beta \in \mathbf{ON}$ such that $x \in R(\beta + 1)$.

Definition 40. For $\alpha, \beta, \xi, \eta, \xi', \eta' \in \mathbf{ON}$, let $\alpha \cdot \beta = \text{type}(\beta \times \alpha, R)$, where R is a lexicographic order on $\beta \times \alpha$:

$$\langle \xi, \eta \rangle R \langle \xi', \eta' \rangle \leftrightarrow (\xi < \xi' \vee (\xi = \xi' \wedge \eta < \eta')).$$

Definition 41. For $\alpha, \beta \in \mathbf{ON}$, α^β is defined by recursion on β by

- (a) $\alpha^0 = 1$.
- (b) $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$.
- (c) If β is a limit, $\alpha^\beta = \sup\{\alpha^\xi : \xi < \beta\}$.

Ordinal multiplication simply creates β "number" of copies of α and lays them out, "end-to-end". This preserves order so that you will get an ordinal isomorphic to $\alpha \cdot \beta$ that is what you would expect for finite ordinals. As with ordinal addition, ordinal multiplication is not commutative for infinite ordinals: $2 \cdot \omega \neq \omega \cdot 2$.

Ordinal exponentiation functions as you would expect exponentiation for the natural numbers to work.

We shall simply state the following definition for later use.

Definition 42. By recursion on $m \in \omega$, $\text{En}(m, A, n)$ is defined by the following:

- (a) If $m = 2^i \cdot 3^j$ and $i, j < n$, then $\text{En}(m, A, n) = \text{Diag}_{\subset}(A, n, i, j)$.
- (b) If $m = 2^i \cdot 3^j \cdot 5$ and $i, j < n$, then $\text{En}(m, A, n) = \text{Diag}_{=} (A, n, i, j)$.
- (c) If $m = 2^i \cdot 3^j \cdot 5^2$, then $\text{En}(m, A, n) = A^n \setminus \text{En}(i, A, n)$.
- (d) If $m = 2^i \cdot 3^j \cdot 5^3$, then $\text{En}(m, A, n) = \text{En}(i, A, n) \cap \text{En}(j, A, n)$.
- (e) If $m = 2^i \cdot 3^j \cdot 5^4$, then $\text{En}(m, A, n) = \text{Proj}(A, \text{En}(i, A, n + 1), n)$.
- (f) If m is not of any of the forms specified above, then $\text{En}(m, A, n) = 0$.

Theorem 2 (Generalized Reflection Theorem). *Suppose \mathbf{Z} is a class and, for each $\alpha, \beta \in \mathbf{ON}$, $Z(\alpha)$ is a set, and assume*

1. $\alpha < \beta \rightarrow Z(\alpha) \subset Z(\beta)$.
2. *If γ is a limit ordinal, then $Z(\gamma) = \bigcup_{\alpha < \gamma} Z(\alpha)$.*
3. $\mathbf{Z} = \bigcup_{\alpha \in \mathbf{ON}} Z(\alpha)$.

Then, for any formulas ϕ_1, \dots, ϕ_n ,

$$\forall \alpha \exists \beta > \alpha (\phi_1, \dots, \phi_n \text{ are absolute for } Z(\beta), \mathbf{Z}).$$

The proof of this theorem will be excluded. The sceptical reader is encouraged to check [3] Ch. 4 §7 Theorem 7.5 for a complete proof.

Lemma 1. *If \mathbf{N} is transitive, then the \in relation is extensional on \mathbf{N} .*

Proof. Assume $x, y \in \mathbf{N}$. We need to show that $x = y \Leftrightarrow \forall z \in \mathbf{N} (z \in x \leftrightarrow z \in y)$. As \mathbf{N} is transitive, we have $x, y \subset \mathbf{N}$. It then follows that $\forall z \in \mathbf{N} (z \in x \leftrightarrow z \in y)$. By Axiom 1, $x = y$. The other direction is trivial. \square

Lemma 2. *If $R, S \in \text{Df}(A, n)$, then $A^n \setminus R \in \text{Df}(A, n)$ and $R \cap S \in \text{Df}(A, n)$. If $R \in \text{Df}(A, n+1)$, then $\text{Proj}(A, R, n) \in \text{Df}(A, n)$.*

Proof. Follows immediately from definition of $\text{Df}(A, n)$. \square

The following lemma now clarifies the connection between $\text{Df}(A, n)$ and first-order logic.

Lemma 3. *Let $\phi(x_0, \dots, x_{n-1})$ be any formula whose free variables are among x_0, \dots, x_{n-1} ; then*

$$\forall A (\{s \in A^n : \phi^A(s(0), \dots, s(n-1))\} \in \text{Df}(A, n)). \quad (1)$$

Proof. By induction on the length of ϕ .

If ϕ is $x_i \in x_j$, (1) follows as $\text{Diag}_{\in}(A, n, i, j) \in \text{Df}(A, n)$.

If ϕ is $x_i = x_j$, (1) follows as $\text{Diag}_{=}(A, n, i, j) \in \text{Df}(A, n)$.

If ϕ is $\psi \wedge \chi$, (1) follows as we know that (1) holds for ψ and χ , and $\text{Df}(A, n)$ is closed under finite intersections by Lemma 2.

If ϕ is $\neg\psi$, (1) follows as $\text{Df}(A, n)$ is closed under complements by Lemma 2.

Finally, if ϕ is $\exists y(\psi)$, there are two cases to consider. If y is not one of the variables x_0, \dots, x_{n-1} , applying (1) for ψ yields

$$\{s \in A^n : \phi^A(s(0), \dots, s(n-1))\} = \text{Proj}(A, \{t \in A^{n+1} : \psi^A(t(0), \dots, t(n))\}, n) \in \text{Df}(A, n).$$

If y is x_j , then $\phi(x_0, \dots, x_{n-1})$ is $\exists x_j \psi(x_0, \dots, x_{n-1})$, so x_j is not free in ϕ . Then let z be a variable not occurring anywhere in ϕ , let $\psi'(x_0, \dots, x_{n-1}, z)$ be $\psi(x_0, \dots, x_{j-1}, z, x_{j+1}, \dots, x_{n-1})$, and let ϕ' be $\exists z \psi'$; then ϕ' and ϕ are logically equivalent and the preceding argument shows that (1) holds for ϕ' , and therefore also for ϕ . \square

Lemma 4. *For any $\alpha \in \mathbf{ON}$, $R(\alpha) = \{x \in \mathbf{WF} : \text{rank}(x) < \alpha\}$.*

Proof. For $x \in \mathbf{WF}$ and $\alpha, \beta \in \mathbf{ON}$, $\text{rank}(x) < \alpha$ if and only if

$$\exists \beta < \alpha (x \in R(\beta + 1)) \Leftrightarrow x \in R(\alpha).$$

This uses the fact that $\beta < \alpha \Rightarrow R(\beta) \subset R(\alpha)$, which follows immediately from definition 36. \square

Lemma 5. *The Axiom of Foundation is true in any $\mathbf{M} \subset \mathbf{WF}$.*

Proof. The relativization of the Axiom of Foundation to \mathbf{M} becomes

$$\forall x \in \mathbf{M} (\exists y \in \mathbf{M} (y \in x) \rightarrow \exists y \in \mathbf{M} (y \in x \wedge \neg \exists z \in \mathbf{M} (z \in x \wedge z \in y)))$$

Now, if $\mathbf{M} \subset \mathbf{WF}$, given x , take $y \in \mathbf{M} \cap x$ of minimal rank. We need to prove that $\text{rank}(y) < \text{rank}(x)$. Let $\alpha = \text{rank}(x)$; then $x \in R(\alpha + 1) = \mathcal{P}(R(\alpha))$. Now, as $y \in x$, $x \notin R(\alpha)$, we have $y \in R(\alpha)$. Then $\text{rank}(y) < \text{rank}(x)$ by Lemma 4. \square

Lemma 6. *Suppose that for each formula $\phi(x, z, w_1, \dots, w_n)$ with no variables besides the displayed ones free,*

$$\forall z, w_1, \dots, w_n \in \mathbf{M} (\{x \in z : \phi^{\mathbf{M}}(x, z, w_1, \dots, w_n)\} \in \mathbf{M}).$$

Then the Comprehension Axiom is true in \mathbf{M} .

Proof. We check, for each ϕ as above, that

$$\forall z, w_1, \dots, w_n \in \mathbf{M} \exists Y \in \mathbf{M} (x \in Y \leftrightarrow x \in z \wedge \phi^{\mathbf{M}}(x, z, w_1, \dots, w_n)),$$

as this is a relativized instance of Comprehension. Given z, w_1, \dots, w_n , take $Y = \{x \in z : \phi^{\mathbf{M}}(x, z, w_1, \dots, w_n)\} \in \mathbf{M}$. Then for all x , and therefore for all $x \in \mathbf{M}$,

$$x \in Y \leftrightarrow x \in z \wedge \phi^{\mathbf{M}}(x, z, w_1, \dots, w_n).$$

\square

Lemma 7. *If \mathbf{M} is transitive, the Power Set Axiom holds in \mathbf{M} if*

$$\forall x \in \mathbf{M} \exists y \in \mathbf{M} (\mathcal{P}(x) \cap \mathbf{M} \subset y).$$

Proof. The Power Set axiom relativized to \mathbf{M} is equal to

$$\forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z \in \mathbf{M} (z \cap \mathbf{M} \subset x \rightarrow z \in y)$$

However, for transitive \mathbf{M} , we have $z \cap \mathbf{M} = z$ for $z \in \mathbf{M}$, and so for $z, y \in \mathbf{M}$,

$$(z \subset y)^{\mathbf{M}} \leftrightarrow z \subset y$$

Thus for transitive \mathbf{M} , Power Set holds in \mathbf{M} if

$$\forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z \in \mathbf{M} (z \subset x \rightarrow z \in y),$$

which is equivalent to the statement in the lemma. \square

Lemma 8. *If*

$$\forall x, y \in \mathbf{M} \exists z \in \mathbf{M} (x \in z \wedge y \in z)$$

and

$$\forall x \in \mathbf{M} \exists z \in \mathbf{M} (\bigcup x \subset z),$$

then the Pairing and Union Axioms are true in \mathbf{M} .

Proof. The first statement is just Pairing relativized to \mathbf{M} . The second statement is Union relativized to \mathbf{M} , slightly rewritten using the \bigcup operation. \square

Lemma 9. *Suppose we can show, for each formula $\phi(x, y, A, w_1, \dots, w_n)$ and each $A, w_1, \dots, w_n \in \mathbf{M}$: If*

$$\forall x \in A \exists! y \in \mathbf{M} \phi^{\mathbf{M}}(x, y, A, w_1, \dots, w_n),$$

then

$$\exists Y \in \mathbf{M} (\{y : \exists x \in A \phi^{\mathbf{M}}(x, y, A, w_1, \dots, w_n)\} \subset Y).$$

Then the Replacement Scheme is true in \mathbf{M} .

Proof. This is just Replacement relativized to \mathbf{M} , rewritten using \subset . \square

Corollary 1 (Uses Axiom of Choice). *Let \mathbf{Z} be any transitive class. Let ϕ_1, \dots, ϕ_n be sentences. Then*

$$\forall X \subset \mathbf{Z} (X \text{ is transitive} \rightarrow \exists M (X \subset M \wedge \bigwedge_{i=1}^n (\phi_i^M \leftrightarrow \phi_i^{\mathbf{Z}}) \wedge M \text{ is transitive} \wedge |M| \leq \max(\omega, |X|))$$

The proof of this corollary will be excluded. For details, see [3] Ch. IV §7 Corollary 7.10.

Constructible sets

Here we present the essential definitions and results (the latter complete with proofs) describing the universe of constructible sets \mathbf{L} , and expand on their meaning. Note that some proofs have been reworked and extended, compared to those found in [3], in order to be more comprehensive.

Constructing what is constructible: Defining \mathbf{L}

Our endeavour begins with constructing \mathbf{L} , taking great care to be strict in our definitions. By virtue of its construction, \mathbf{L} will turn out to have several properties essential to a model of ZFC + GCH.

We begin by defining the definable power set operation, \mathcal{D} . For A a set, one can think of $\mathcal{D}(A)$ as the set of subsets of A definable from a finite number of elements of A by a formula relativized to A . Note that $\langle x_0, \dots, x_{n-1} \rangle$ denotes the function s such that $\text{dom}(s) = n = \{0, \dots, n-1\}$, and $s(i) = x_i$ for each $i \in n$.

Definition 43. $\mathcal{D}(A) = \{X \subset A : \exists n \in \omega \exists s \in A^n \exists R \in \text{Df}(A, n+1)(X = \{x \in A : s \frown \langle x \rangle \in R\})\}$.

We are now ready to define \mathbf{L} .

Definition 44. By transfinite recursion, define $L(\alpha)$ for $\alpha \in \mathbf{ON}$ by

- (a) $L(0) = 0$.
- (b) $L(\alpha + 1) = \mathcal{D}(L(\alpha))$.
- (c) $L(\alpha) = \bigcup_{\xi < \alpha} L(\xi)$ when α is a limit ordinal.

Definition 45. $\mathbf{L} = \bigcup \{L(\alpha) : \alpha \in \mathbf{ON}\}$.

\mathbf{L} can then be viewed as all sets that are definable (where we have been careful to give a strict definition of what definable means) using the ordinal numbers. One notes that $\mathcal{D}(x)$ bears a striking resemblance to $\mathcal{P}(x)$, the power set. Indeed, as we shall see, for any set A , we have $\mathcal{D}(A) \subset \mathcal{P}(A)$. This is probably the easiest way to think about $\mathcal{D}(x)$; namely, as a (strict) subset of $\mathcal{P}(x)$ where all members of $\mathcal{D}(x)$ can be easily described using first-order formulas relativized to x , and parameters from x (recall Lemma 3).

\mathbf{L} as a model of the basic axioms

We proceed with showing that \mathbf{L} models the first nine axioms (we deal with the Axiom of Choice, as well as the Generalized Continuum Hypothesis, later). A number of lemmas will be required for the proof of the theorem towards this effect. Thus, we state them here for later reference.

Lemma 10. *Let $\phi(v_0, v_1, \dots, v_{n-1}, x)$ be any formula with all free variables shown. Then*

$$\forall A \forall v_0, \dots, v_{n-1} \in A (\{x \in A : \phi^A(v_0, \dots, v_{n-1}, x)\} \in \mathcal{D}(A)).$$

Proof. Follows immediately from Lemma 3. □

Lemma 11. *For any A ,*

- (a) $\mathcal{D}(A) \subset \mathcal{P}(A)$.
- (b) *If A is transitive, then $A \subset \mathcal{D}(A)$.*
- (c) $\forall X \subset A (|X| < \omega \rightarrow X \in \mathcal{D}(A))$.
- (d) $|A| \geq \omega \rightarrow |\mathcal{D}(A)| = |A|$.

Proof. (a): Follows from the definition of $\mathcal{D}(A)$.

(b): Applying Lemma 10 with the formula $x \in v$ yields

$$\forall v \in A (\{x \in A : x \in v\} \in \mathcal{D}(A)),$$

which for a transitive A reduces to $\forall v \in A (v \in \mathcal{D}(A))$.

(c): We recall from the definition of $\text{Df}(A, n)$ and by Lemma 2 that if $R, S \in \text{Df}(A, n+1)$, then

$$(A^{n+1} \setminus R) \in \text{Df}(A, n+1) \text{ and } R \cap S \in \text{Df}(A, n+1)$$

and therefore also

$$R \cup S = A^{n+1} \setminus ((A^{n+1} \setminus R) \cap (A^{n+1} \setminus S)) \in \text{Df}(A, n+1).$$

Moreover $0 = R \cap (A^{n+1} \setminus R) \in \text{Df}(A, n+1)$. Now use induction on $m \leq n$ to show that

$$E_n^m = \{t \in A^{n+1} : \exists i < m (t(n) = t(i))\} \in \text{Df}(A, n+1).$$

The induction step uses that E_n^{m+1} is the union of E_n^m with $\{t \in A^{n+1} : t(n) = t(m)\}$, the latter being in $\text{Df}(A, n)$ by definition. So, for any $s \in A^n$,

$$\text{ran}(s) = \{x \in A : s \frown \langle x \rangle \in E_n^n\} \in \mathcal{D}(A),$$

and therefore $\forall n < \omega \forall X \subset A (|X| \leq n \rightarrow X \in \mathcal{D}(A))$.

(d): Note that this requires AC! However, by the time we need part (d) of this lemma, we will have already proven that AC holds in **L**.

By AC and $|A| \geq \omega$, $|A^n| = |A|$ for all n .

Next, we show that for any n, A , $\text{Df}(A, n) = \{\text{En}(m, A, n) : m \in \omega\}$ (keeping in mind definition 42).

By induction on m we get that $\forall n < \omega (\text{En}(m, A, n) \in \text{Df}(A, n))$, noting that $0 \in \text{Df}(A, n)$ (as $\text{Df}(A, n)$ is closed under intersections and complements by Lemma 2), so the case of $\text{En}(m, A, n) = 0$ is also covered.

Now, by induction on k , we get that $\forall n (\text{Df}^k(k, A, n) \subset \{\text{En}(m, A, n) : m \in \omega\})$: We then have $\text{Df}(A, n) = \{\text{En}(m, A, n) : m \in \omega\}$ and therefore also $|\text{Df}(A, n)| = |\{\text{En}(m, A, n) : m \in \omega\}| \leq \omega$.

By the argument above, $|\mathcal{D}(A)| \leq |A|$.

$|\text{Df}(A, n+1)| \geq |A|$ follows from $\forall x \in A (\{x\} \in \mathcal{D}(A))$, a special case of (c). \square

Lemma 12. For each $\alpha \in \mathbf{ON}$,

- (a) $L(\alpha)$ is transitive.
- (b) $\forall \xi \leq \alpha (L(\xi) \subset L(\alpha))$.

Proof. By induction on α . Assume the lemma holds for all $\beta < \alpha$, and prove that it holds for α . This is trivially true for $\alpha = 0$ or a limit, so assume $\alpha = \beta + 1$. Then by assumption $L(\beta)$ is transitive and $L(\alpha) = \mathcal{D}(L(\beta))$, so $L(\beta) \subset L(\alpha) \subset \mathcal{P}(L(\beta))$ by Lemma 11 (a) and (b), implying both (a) and (b) for α . \square

Definition 46. The \mathbf{L} -rank of x , $\rho(x)$ (for $x \in \mathbf{L}$), is the least β such that $x \in L(\beta + 1)$.

Lemma 13. For any $\alpha \in \mathbf{ON}$, $L(\alpha) = \{x \in \mathbf{L} : \rho(x) < \alpha\}$.

Proof. For $x \in \mathbf{L}$, $\rho(x) < \alpha$ if and only if

$$\exists \beta < \alpha (x \in L(\beta + 1)) \Leftrightarrow x \in L(\alpha).$$

\square

Lemma 14. For any $\alpha \in \mathbf{ON}$, $L(\alpha) \in L(\alpha + 1)$.

Proof. $L(\alpha) = \{x \in L(\alpha) : (x = x)^{L(\alpha)}\}$, which is in $\mathcal{D}(L(\alpha)) = L(\alpha + 1)$ by Lemma 10. \square

Lemma 15. $L(\alpha) \subset R(\alpha)$ for all $\alpha \in \mathbf{ON}$.

Proof. Use transfinite induction on α (or simply convince yourself that the lemma holds based on the similarity of definitions for $R(\alpha), L(\alpha)$). \square

We are now at long last in a position to prove that \mathbf{L} does indeed model the first nine axioms.

Theorem 3. \mathbf{L} is a model of ZF.

Proof. We proceed in order and show that each of the axioms 0-8 hold.

- (i) **Set Existence (Axiom 0):** Since $L(1) = \mathcal{D}(0) = \{0\} \Rightarrow$, the empty set is in \mathbf{L} , and so Set Existence holds.
- (ii) **Extensionality (Axiom 1):** Relativized to \mathbf{L} , Extensionality becomes

$$\forall x, y \in \mathbf{L} (\forall z \in \mathbf{L} (z \in x \leftrightarrow z \in y) \rightarrow x = y),$$

the definition of \in being extensional on \mathbf{L} . As $\mathbf{L} = \cup_{\alpha \in \mathbf{ON}} L(\alpha)$, it follows from Lemma 12 (a) that \mathbf{L} is transitive. Then by Lemma 1, Extensionality holds.

- (iii) **Foundation (Axiom 2):** By Lemma 15, we have $\mathbf{L} \subset \mathbf{WF}$ by virtue of their construction, and so by Lemma 5, Foundation holds in \mathbf{L} .
- (iv) **Comprehension Scheme (Axiom 3):** By Lemma 6, it is sufficient to show that for each

formula $\psi(x, z, v_1, \dots, v_n)$ with all free variables shown, we have

$$\forall z, v_1, \dots, v_n \in \mathbf{L} (\{x \in z : \psi^{\mathbf{L}}(x, z, v_1, \dots, v_n)\} \in \mathbf{L}).$$

This will work due to the definition of $L(\alpha + 1) = \mathcal{D}(L(\alpha))$; however, as $\mathcal{D}(L(\alpha))$ speaks of relativizations to $L(\alpha)$, not \mathbf{L} , we need to use the Generalized Reflection Theorem (Theorem 2). First check that $L(\alpha)$ and \mathbf{L} fulfill the criteria of $Z(\alpha)$ and \mathbf{Z} in the theorem. By Definition 45, \mathbf{L} satisfies requirement 3. By Definition 44, $L(\alpha)$ satisfies requirement 2. It remains to show that for $\alpha < \beta$, we have $L(\alpha) \subset L(\beta)$. By Lemma 12, $L(\alpha)$ satisfies requirement 1. All requirements thus met, we may proceed to use Reflection. Fix $z, v_1, \dots, v_n \in \mathbf{L}$, and fix α such that $z, v_1, \dots, v_n \in L(\alpha)$. Now let $\beta > \alpha$ be such that ψ is absolute for $L(\beta)$, \mathbf{L} ; then

$$\{x \in z : \psi^{\mathbf{L}}(x, z, v_1, \dots, v_n)\} = \{x \in L(\beta) : \phi^{L(\beta)}(x, z, v_1, \dots, v_n)\}, \quad (2)$$

where ϕ is $x \in z \wedge \psi$. Then the set in (2) is in $\mathcal{D}(L(\beta)) = L(\beta + 1)$ by Lemma 10, and thus Comprehension holds by Lemma 6.

- (v) **Pairing (Axiom 4)**: Will be proven in conjunction with Union, see below.
- (vi) **Union (Axiom 5)**: We shall prove that Pairing and Union holds in \mathbf{L} simultaneously. Utilizing Lemma 8, we must prove two things:

$$\forall x, y \in \mathbf{L} \exists z \in \mathbf{L} (x \in z \wedge y \in z), \quad (3)$$

and

$$\forall x \in \mathbf{L} \exists z \in \mathbf{L} (\bigcup x \subset z). \quad (4)$$

We show (3) first. For any $x, y \in \mathbf{L}$, simply choose $z = L(\sup\{\rho(x), \rho(y)\})$. Then by Lemma 13, $x, y \in z$.

For (4), $z = L(\rho(x))$ implies $\bigcup x \subset z$ by definition of $L(\alpha)$.

Thus, both Pairing and Union hold in \mathbf{L} .

- (vii) **Replacement Scheme (Axiom 6)**: We shall utilize Lemma 9. For each formula $\phi(x, y, A, w_1, \dots, w_n)$ and each $A, w_1, \dots, w_n \in \mathbf{L}$, assume

$$\forall x \in A \exists! y \in \mathbf{L} \phi^{\mathbf{L}}(x, y, A, w_1, \dots, w_n). \quad (5)$$

Then it is sufficient to prove

$$\exists Y \in \mathbf{L} (\{y : \exists x \in A \phi^{\mathbf{L}}(x, y, A, w_1, \dots, w_n)\} \subset Y). \quad (6)$$

So assume (5). Let $\alpha = \sup\{\rho(y) + 1 : y \in \mathbf{L} \exists x \in A \phi^{\mathbf{L}}(x, y, A, w_1, \dots, w_n)\}$. Now simply take $Y = L(\alpha)$, which is in \mathbf{L} by Lemma 14, which will satisfy (6), and so Replacement holds in \mathbf{L} .

- (viii) **Infinity (Axiom 7)**: Infinity holds in \mathbf{L} if we can show $\omega \in \mathbf{L}$. As $\omega + 1 \in \mathbf{ON}$ and $\omega \in \mathcal{D}(\omega)$ (the latter following immediately from Lemma 10), this follows immediately from the definition of \mathbf{L} , and so Infinity holds.
- (ix) **Power Set (Axiom 8)**: We shall use Lemma 7 to do the heavy lifting. We established in our

proof of Extensionality that \mathbf{L} is transitive, and furthermore note that $\mathcal{P}(x) \cap \mathbf{L}$ is simply equal to $\mathcal{D}(x)$. So it remains to show that

$$\forall x \in \mathbf{L} \exists y \in \mathbf{L} (\mathcal{D}(x) \subset y).$$

Let $x = L(\alpha)$. Then pick $y = L(\alpha + 1) = \mathcal{D}(L(\alpha))$. Then by Lemma 14 and \mathbf{L} being transitive, this requirement is fulfilled, and so by Lemma 7, Power Set holds in \mathbf{L} .

□

So, by Theorem 3, \mathbf{L} models ZF (Axioms 0 - 8).

As an aside, we note that $A \subset B \Rightarrow \mathcal{D}(A) \subset \mathcal{D}(B)$. To see this, note that for each $\alpha \exists y \in \mathbf{L} : \mathcal{D}(L(\alpha)) \subset y$: Simply choose $y = \alpha + 2$.

Simplifying relative proofs: The Axiom of Constructibility

Herein we endeavour to show that $\mathbf{V} = \mathbf{L}$ is consistent with ZF. However, other results (beyond the scope of this paper) shows that $\mathbf{V} \neq \mathbf{L}$ is also consistent with ZF. So why is this interesting? When we later prove that AC and GCH hold in \mathbf{L} , in order to simplify things, we do not want to continually have to relativize everything to \mathbf{L} . If, for instance, we are trying to prove that a formula ϕ holds in \mathbf{L} , it is much easier to simply assume $\mathbf{V} = \mathbf{L}$ and prove ϕ , as opposed to trying to prove $\phi^{\mathbf{L}}$. In order to do this, we need to show that $\mathbf{V} = \mathbf{L}$ is consistent with ZF, so that we can indeed assume it.

Let us define what we are trying to prove.

Definition 47. The Axiom of Constructibility is the statement $\mathbf{V} = \mathbf{L}$, i.e. $\forall x \exists \alpha (x \in L(\alpha))$.

This may seem a trivial thing to prove, but appearances can be deceiving. Clearly, $\forall x \in \mathbf{L} \exists \alpha (x \in L(\alpha))$, but $(\mathbf{V} = \mathbf{L})^{\mathbf{L}}$ is in fact the statement that $\forall x \in \mathbf{L} \exists \alpha \in \mathbf{L} ((x \in L(\alpha))^{\mathbf{L}})$. So to prove $(\mathbf{V} = \mathbf{L})^{\mathbf{L}}$, we need to verify that the formula $x \in L(\alpha)$ is absolute. The result we want then follows almost immediately from the following two lemmas:

Lemma 16. *Let $\varphi(x, y)$ be a formula such that for every $\alpha \in \mathbf{ON}$, $\varphi(\alpha, y)$ holds if and only if $y = L(\alpha)$ (such a formula exists). Then $\varphi(x, y)$ is absolute for transitive models of ZF - P (note: ZF - P stands for the first 8 axioms minus Power Set).*

Proof sketch. Exact details of this proof will be omitted. However, it can be shown that Df is absolute ([3] Ch. V §1 Lemma 1.7). Similarly, \mathcal{D} can be shown to be absolute (apply the methods found in [3] Ch. IV §5). As $L(\alpha)$ is defined by transfinite recursion from \mathcal{D} , it too is absolute (functions defined recursively using absolute notions are absolute). \square

Lemma 17. *For every $\alpha \in \mathbf{L}$, $\alpha = L(\alpha) \cap \mathbf{ON}$.*

Proof. By induction on α . By definition, $0 = 0 \cap \mathbf{ON}$. Now suppose $\alpha = L(\alpha) \cap \mathbf{ON}$ for all $\alpha < \beta$. We have two cases to consider.

β is a limit ordinal: Then $\beta = \cup\{\alpha : \alpha < \beta\}$ and $L(\beta) = \cup\{L(\alpha) : \alpha < \beta\}$, so we have that $\beta \cap \mathbf{ON} = \cap\{\alpha : \alpha < \beta\} \cup \mathbf{ON} = \beta$.

$\beta = \alpha + 1$: Then $L(\beta) = \mathcal{D}(L(\alpha))$. Let $\varphi(x)$ be the formula which states that x is an ordinal. Then $\varphi^{L(\alpha)}(x) \leftrightarrow \varphi(x)$ since $\varphi(x)$ contains any bounded quantifiers and $L(\alpha)$ is transitive (the latter by Lemma 12 (a)). Hence by Lemma 10 and our induction hypothesis,

$$\alpha = L(\alpha) \cap \mathbf{ON} = \{x \in L(\alpha) : \varphi(x)\} = \{x \in L(\alpha) : \varphi^{L(\alpha)}(x)\} \in \mathcal{D}(L(\alpha)).$$

By Lemma 11, $\alpha \subset L(\alpha) \subset \mathcal{D}(L(\alpha))$ and hence $\beta = \alpha + 1 = \alpha \cup \{\alpha\} \subset \mathcal{D}(L(\alpha)) = L(\beta)$. \square

Note that as an immediate consequence we have that $\mathbf{ON} \subset \mathbf{L}$.

Our theorem is thus ready to be stated and proven:

Theorem 4. *\mathbf{L} is a model of ZF + $\mathbf{V} = \mathbf{L}$.*

Proof. That \mathbf{L} models ZF was the result of Theorem 3. To prove that $(\mathbf{V} = \mathbf{L})^{\mathbf{L}}$, we must show

$$\forall x \in \mathbf{L} \exists \alpha \in \mathbf{L} ((x \in L(\alpha))^{\mathbf{L}}).$$

Fix $x \in \mathbf{L}$. Now fix α such that $x \in L(\alpha)$. Then $\alpha \in \mathbf{L}$ since $\mathbf{ON} \subset \mathbf{L}$ by Lemma 17, and $(x \in L(\alpha))^{\mathbf{L}}$ by Lemma 16. \square

Corollary 2. *If ZF is consistent, so is ZF in conjunction with $\mathbf{V} = \mathbf{L}$.*

One may ask why we simply do not add the Axiom of Constructibility to our existing list of axioms? The reason is that \mathbf{L} does not contain all interesting mathematical objects. Indeed, it does not even necessarily contain all subsets of ω ! So adding the Axiom of Constructibility would simply limit the usefulness of any model fulfilling our axioms greatly, due to the forcing technique of Cohen. Thus, we are satisfied with using the Axiom of Constructibility as a tool to make our lives easier, and as we have just proven, usage of this tool is entirely consistent with ZF.

Furthermore, we find a number of useful properties of \mathbf{L} as a consequence of the absoluteness of $L(\alpha)$, said properties turning out to be necessary for our work with AC and GCH. We state these theorems without delving deeper into their actual meaning, having contented ourselves to merely using them to justify later results. Note that the formula defining \mathbf{ON} is absolute. Also, if $\varphi(x)$ is a formula expressing that $x \in \mathbf{L}$, then $\mathbf{L} = \mathbf{L}^{\mathbf{M}}$ means $\forall x (\varphi(x) \leftrightarrow \varphi^{\mathbf{M}}(x))$.

Theorem 5. *If $\mathbf{M} \subset \mathbf{WF}$ is any transitive proper class which is a model of ZF - P, then $\mathbf{L} = \mathbf{L}^{\mathbf{M}}$. Furthermore, $\mathbf{L}^{\mathbf{M}} \subset \mathbf{M}$.*

Proof. We first show that $\mathbf{ON} \subset \mathbf{M}$: Fix $\alpha \in \mathbf{ON}$. As $\mathbf{M} \not\subset R(\alpha)$, there is an $x \in \mathbf{M}$ with $\text{rank}(x) \geq \alpha$ (as \mathbf{M} is a proper class). But the formula defining the rank function is absolute for \mathbf{M} (being defined by recursion on x), so $\text{rank}(x) \in \mathbf{M}$ and so $\alpha \in \mathbf{M}$ as \mathbf{M} is transitive. Then by absoluteness of $L(\alpha)$ and \mathbf{ON} ,

$$\mathbf{L}^{\mathbf{M}} = \{x \in \mathbf{M} : (\exists \alpha (x \in L(\alpha)))^{\mathbf{M}}\} = \bigcup \{L(\alpha) : \alpha \in \mathbf{ON}\} = \mathbf{L},$$

and hence $\mathbf{L} = \mathbf{L}^{\mathbf{M}} \subset \mathbf{M}$. \square

In the interest of formality, observe that there is a finite conjunction ϕ of axioms of ZF - P such that the notions of ordinal, rank, and $L(\alpha)$ are all absolute for transitive models of ϕ . We may then rewrite Theorem 5 as the affirmation that for each class \mathbf{M} , the statement

$$\mathbf{M} \text{ is a transitive proper class} \wedge \phi^{\mathbf{M}} \rightarrow \mathbf{L} \subset \mathbf{M}$$

is provable.

Definition 48. $o(M) = M \cap \mathbf{ON}$ for any set M .

Lemma 18. *If M is any transitive set, $o(M) \in \mathbf{ON}$, and is the first ordinal not in M .*

Proof. That $o(M) \in \mathbf{ON}$ follows from the definition, along with properties of the ordinal numbers and the fact that M is transitive. Now assume for some α that $\alpha \in \mathbf{ON}$, $\alpha \notin M$, $\alpha < o(M)$. As α , $o(M) \in \mathbf{ON}$, we have that $\alpha < o(M) \Rightarrow \alpha \in o(M)$. Then by definition of $o(M)$, it follows that $\alpha \in M$. But this contradicts our assertion previously that $\alpha \notin M$. \square

Theorem 6. *There is a finite conjunction ψ of axioms of $ZF - P$ such that*

$$\forall M (M \text{ transitive} \wedge \psi^M \rightarrow (L(o(M)) = \mathbf{L}^M \subset M)).$$

Proof sketch. ψ is a conjunction of the ϕ discussed above before definition 48, with enough axioms to prove that there is no largest ordinal. If M is transitive and ψ^M , then $o(M)$ is a limit ordinal, so $L(o(M)) = \bigcup_{\alpha \in M \cap \mathbf{ON}} L(\alpha)$. But then

$$\mathbf{L}^M = \{x \in M : (\exists \alpha (x \in L(\alpha)))^M\} = \bigcup_{\alpha \in M \cap \mathbf{ON}} L(\alpha)$$

by absoluteness of $L(\alpha)$, so $L(o(M)) = \mathbf{L}^M \subset M$. □

Theorem 7. *There is a finite conjunction χ of axioms of $ZF - P + \mathbf{V} = \mathbf{L}$ such that*

(a) *If \mathbf{M} is a transitive proper class and $\chi^{\mathbf{M}}$, then $\mathbf{M} = \mathbf{L}$.*

(b) $\forall M (M \text{ transitive} \wedge \chi^M \rightarrow M = L(o(M)))$.

Proof. χ is just the ψ of Theorem 6, conjuncted with $\mathbf{V} = \mathbf{L}$. So if \mathbf{M} is transitive and $\chi^{\mathbf{M}}$, then $(\forall x (x \in \mathbf{L})^{\mathbf{M}})$. Part (a) now follows from Theorem 5, and part (b) from Theorem 6. □

AC and GCH in \mathbf{L}

By the end of this section, we will have proven that \mathbf{L} , in addition to modelling ZF, also is a model of AC and GCH, thus fulfilling what we set out to do in our introduction to this paper.

We begin with AC. The idea here is to inductively define well-orders of $L(\alpha)$. Once this is done, AC follows almost immediately from the definition.

Definition 49. By recursion on $\alpha \in \mathbf{ON}$, define well-orders $\triangleleft_\alpha = \triangleleft(\alpha)$ of $L(\alpha)$ as follows.

$\triangleleft_0 = 0$.

If α is a limit,

$$\triangleleft_\alpha = \{\langle x, y \rangle \in L(\alpha) \times L(\alpha) : \rho(x) < \rho(y) \vee (\rho(x) = \rho(y)) \wedge \langle x, y \rangle \in \triangleleft(\rho(x) + 1)\}.$$

Given \triangleleft_α , let \triangleleft_α^n be the induced lexicographic order on $L(\alpha)^n$:

$$s \triangleleft_\alpha^n t \leftrightarrow \exists k < n (s \upharpoonright k = t \upharpoonright k \wedge s(k) \triangleleft_\alpha t(k)).$$

If $X \in L(\alpha + 1) = \mathcal{D}(L(\alpha))$, let n_X be the least n such that

$$\exists s \in L(\alpha)^n \exists R \in \text{Df}(L(\alpha), n + 1)(X = \{x \in L(\alpha) : s \frown \langle x \rangle \in R\}).$$

Let s_X be the $\triangleleft_\alpha^{n_X}$ -least $s \in L(\alpha)^{n_X}$ such that

$$\exists R \in \text{Df}(L(\alpha), n_X + 1)(X = \{x \in L(\alpha) : s_X \frown \langle x \rangle \in R\}).$$

and let m_X be the least $m \in \omega$ such that

$$X = \{x \in L(\alpha) : s_X \frown \langle x \rangle \in \text{En}(m, L(\alpha), n_X)\}.$$

For $X, Y \in L(\alpha + 1)$, define $X \triangleleft_{\alpha+1} Y$ if

- (a) $X, Y \in L(\alpha) \wedge X \triangleleft_\alpha Y$, or
- (b) $X \in L(\alpha) \wedge Y \notin L(\alpha)$, or
- (c) $X, Y \notin L(\alpha) \wedge ((n_X < n_Y) \vee (n_X = n_Y \wedge s_X \triangleleft_\alpha^{n_X} s_Y) \vee (n_X = n_Y \wedge s_X = s_Y \wedge m_X < m_Y))$.

We leave the tedious yet straightforward task of verifying that \triangleleft_α is a well-order on $L(\alpha)$ to the intrepid reader. Showing that AC holds in \mathbf{L} is now literally a one-line proof.

Lemma 19. $V = L \rightarrow AC$.

Proof. If $x \in \mathbf{L}$, then $x \subset L(\alpha)$ for some α , and the well-order \triangleleft_α well-orders x . □

Thus the completion of our grand mission is at hand; all that remains is to prove GCF holds in \mathbf{L} . This is slightly more complicated than demonstrating AC. A theorem will give the result needed to conclude GCF, with a little help from a lemma.

Lemma 20. For all $\alpha \geq \omega$, $|L(\alpha)| = |\alpha|$.

Proof. By Lemma 17, $\alpha \subset L(\alpha)$, and as a consequence $|\alpha| \leq |L(\alpha)|$. We prove $|\alpha| = |L(\alpha)|$ by transfinite induction on α . Assume $\alpha \geq \omega$ and $\forall \beta < \alpha (\beta \geq \omega \rightarrow |L(\beta)| = |\beta|)$. Then $\forall \beta < \alpha (|L(\beta)| \leq |\alpha|)$ (since $|L(n)| = |R(n)| < \omega$ for $n < \omega$).

If α is a limit, then $L(\alpha) = \cup_{\beta < \alpha} L(\beta)$ is a union of sets of cardinality $\leq |\alpha|$, and so by AC has cardinality $|\alpha|$.

If $\alpha = \beta + 1$, then $|L(\beta)| = |\beta| = |\alpha|$, and $L(\alpha) = \mathcal{D}(L(\beta))$, so by Lemma 11 (d) $|L(\alpha)| = |\alpha|$. \square

Theorem 8. *If $\mathbf{V} = \mathbf{L}$, then for all infinite ordinals α , $\mathcal{P}(L(\alpha)) \subset L(\alpha^+)$.*

Proof. Let χ be a finite conjunction of axioms of $\text{ZF} + \mathbf{V} = \mathbf{L}$ such that

$$\forall M (M \text{ transitive} \wedge \chi^M \rightarrow M = L(o(M))).$$

Theorem 7 allows this. Now assume $\mathbf{V} = \mathbf{L}$, and fix $A \in \mathcal{P}(L(\alpha))$. Let $X = L(\alpha) \cup \{A\}$. Then $|X| = |\alpha|$ by Lemma 20: This lemma uses AC, but as we have just seen, $\mathbf{V} = \mathbf{L} \rightarrow \text{AC}$.

We need two results which are not included in this paper (please see the final section for a note about this). By the Löwenheim-Skolem theorem (allowing us to find a model of any infinite cardinality) and the Mostowski Collapsing Theorem there then exists a unique transitive M such that $|M| = |\alpha|$, $X \subset M$, and $\chi^M \leftrightarrow \chi^{\mathbf{V}}$, the latter as a result from applying Corollary 1 with $\mathbf{Z} = \mathbf{V}$ (note that it follows that $A \in M$). However, $\chi^{\mathbf{V}}$ is true by $\mathbf{V} = \mathbf{L}$, so χ^M holds, and therefore $M = L(o(M))$. As $|M| = |\alpha|$, $|o(M)| < \alpha^+$. So,

$$A \in L(o(M)) \subset L(\alpha^+).$$

\square

Our desired result now follows.

Corollary 3. $\mathbf{V} = \mathbf{L} \rightarrow \text{AC} + \text{GCH}$.

Proof. That AC holds is the result of Lemma 19. Now by Theorem 8, for each cardinal $\kappa \geq \omega$, $\mathcal{P}(\kappa) \subset \mathcal{P}(L(\kappa)) \subset L(\kappa^+)$, and so $2^\kappa \leq |L(\kappa^+)| = \kappa^+$ by Lemma 20. \square

Theorem 9. *If ZF is consistent, then $\text{ZF} + \text{AC} + \text{GCH}$ is also consistent.*

Proof. If ZF is consistent, ZF has a model, call it \mathbf{V} . In \mathbf{V} we have constructed a subclass \mathbf{L} , which according to Theorem 4 is a model of $\text{ZF} + \mathbf{V} = \mathbf{L}$. Then by Corollary 3 it follows that \mathbf{L} is a model of $\text{ZF} + \text{AC} + \text{GCH}$. \square

At the end of all things: Excluded results

So, after a great deal of work, we have proven that \mathbf{L} satisfies all our nine basic axioms, as well as AC and GCH.

But \mathbf{L} has other properties, not the least of which is that it satisfies several important combinatorial principles. Indeed, this paper has skirted the topic of infinitary combinatorics (which would likely require an entire paper on its own to properly explore), but it can be shown that \mathbf{L} implies the combinatorial principles \diamond and \diamond^+ . It is also possible to construct \mathbf{L} combinatorically (owing, just as the construction of \mathbf{L} , to Gödel).

On an unrelated note, with a bit of work, the following interesting corollary can also be shown:

Corollary 4. *If ZF is consistent, then $ZF + AC + GCH +$ "There exists no weakly inaccessible cardinal" is also consistent.*

Similarly, many results regarding ordinals and cardinals have been left out. The astute reader will no doubt also have noticed the lack of definition of what a class is. Those with some experience with working in ZFC will recognize the difficulty in actually defining a class, while those without such experience will simply have to be content with our assurances that this was done in order not to delve too deeply into philosophical quandaries.

We also opted not to include the statement of the Löwenheim-Skolem Theorems (in truth just one theorem, though it is typically divided into a downward and upward version), as well as the Mostowski Collapsing Theorem, even though we needed them to show GCH.

The Löwenheim-Skolem Theorem is a fundament of model theory and is certainly worth looking up for the interested reader: It states that if we have an infinite model, we can find another model of any infinite cardinality, greater or lesser in cardinality than the one we already have (provided that the first-order language we are working with is countable).

The Mostowski Collapsing Theorem states (simplified for our purposes) that given a set A and an extensional relation R on A , there is a unique isomorphism between $\langle A, R \rangle$ and a transitive set M with \in as its relation.

References

- [1] Kurt Gödel. *The consistency of the axiom of choice and of the generalized continuum-hypothesis with the axioms of set theory*. Annals of Mathematics Studies Volume 3, Princeton University Press, 1940.
- [2] Kurt Gödel. The consistency of the axiom of choice and of the generalized continuum-hypothesis. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1077160/>, Proceedings of the National Academy of Sciences in the United States of America, Volume 12 1938, pages 556 - 557. [Online].
- [3] Kenneth Kunen. *Set Theory: An introduction to independence proofs*. North Holland Publishing Company, 1980.