Cantor’s Continuum Hypothesis: consequences in mathematics and its foundations

ALESSANDRO ANDRETTA
Università di Torino - E-mail: alessandro.andretta@unito.it

Sommario: Si illustra l’ipotesi del continuo, le sue applicazioni in matematica e le sue conseguenze sui fondamenti della matematica.

Abstract: We give an overview of the continuum hypothesis, of its impact on mathematics, and on the foundations of set theory.

1. Introduction

Georg Cantor’s name is inextricably connected with set theory and the continuum hypothesis. But while set theory (or rather the set-theoretic jargon) has become the standard framework in which mathematical objects are construed, the continuum hypothesis is still fairly unknown among mathematicians. The continuum hypothesis, CH for short, is the assertion that every infinite subset of the real line is either countable or else it is in bijection with the line itself; in other words: there is no type of infinity intermediate between that of the integers, and that of the real numbers. Georg Cantor first conjectured this fact in 1878, and spent the rest of his life in trying to prove it, an endeavour undertaken by many other valiant mathematicians. The situation changed dramatically in 1963, when Paul Cohen devised the method of forcing to prove that the negation of CH is consistent with ZFC, the commonly accepted axiomatic framework for set theory. In other words, CH cannot be proved from the axioms of ZFC. On the other hand Kurt Gödel had showed in 1938 that CH is consistent with ZFC, showing thus that there is no point in trying to refute CH. To summarize: the continuum hypothesis can neither be proved, nor disproved from ZFC.

Cantor’s continuum hypothesis is an easily stated problem, one that should tickle the curiosity of a mathematician. It is not a particularly recent question, one of those problems that haven’t had a chance to get enough exposure. In fact CH was the first among the twenty three problems posed by Hilbert at the International Congress of Mathematicians held in Paris in 1900, one hundred years have passed since Cantor’s death, and fifty five years have passed since Paul Cohen’s breakthrough (1). As observed in [Cho09], “Monastyrsky’s outstanding book [Mon97] gives highly informative and insightful expositions of the work of almost every Fields Medalist—but says almost nothing about forcing.” Another book that surveys a vast portion of twentieth century mathematics, but says almost nothing about the continuum hypothesis, set theory and, more generally, mathematical logic is [Die82]. A possible explanation for this phenomenon is that research on the continuum problem is connected

(1) Cohen announced his result in July 1963, and was awarded of the Fields Medal in 1966.
with nontrivial questions in mathematical logic, a feature that hinders the communication of the results.

The aim of the present paper is to try to correct, at least in part, this situation. We shall carefully examine the statement of the continuum hypothesis, showing what kind of results it entails in mathematics, and how it impinges on the foundations of mathematics.

While this is essentially a survey paper in mathematics, we will try to highlight Cantor’s contributions to set theory and the continuum problem. Yet this paper is not an historical survey of Cantor’s work—for this the reader is referred to [GKW12; Dau90] or to the original source [Can80], and to the papers in this volume by mathematicians that are much more versed in the history of set theory than the present author.

2. – Countable and uncountable sets

Consider a very large tea-set, so large that we cannot estimate the number of items: if every cup corresponds to a single plate and conversely, then we can infer that the number of cups is the same as the number of plates. The key idea of set theory is that this comparison method applies to all sets, finite or otherwise: two sets have the same size just in case there is a bijection between them. Before we move on, let us fix some notation.

We write $A \preceq B$ if there is an injective function $f: A \to B$, and if moreover $f$ is surjective then we say that $A$ and $B$ are equipotent, in symbols $A \cong B$. It is immediate to check that, on the universe of all sets, the relation $\preceq$ is a pre-order (i.e. reflexive and transitive) and that $\simeq$ is an equivalence relation. The Cantor-Schröder-Bernstein theorem (2) says that

$$A \simeq B \text{ just in case } A \preceq B \text{ and } B \preceq A;$$

in other words $\simeq$ is the equivalence relation induced by the pre-order $\preceq$. In naïve set theory the cardinality of a set $A$ is identified with $\{B \mid B \simeq A\}$, the equivalence class of $A$ with respect to $\simeq$, and hence one defines the natural number as follows: $0 = \{\emptyset\}$ is the equivalence class of the only set without elements, $1 = \{\{a\} \mid a\}$ is the family of all singletons, $2 = \{\{a, b\} \mid a \neq b\}$ is the family of all sets with exactly two distinct elements, and so on. The problem with this approach is that the $\prec$-equivalence class of a nonempty set is a proper class, a collection that is too large to be a set. The official definition of cardinality is deferred to Definition 4.2—for the time being we just present the construction of the natural numbers due to John von Neumann:

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \ldots$$

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

Note that $n < m \iff n \in m$ and by pigeonhole principle $n \preceq m \iff n \leq m$, so that $n \times m \equiv n = m$.

A set is finite if it is in bijection with some $n \in \mathbb{N}$ where $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of all natural numbers; otherwise it is infinite. (This is the definition of finiteness used by Cantor; another common definition of finiteness, due to Dedekind, says that a set $A$ is finite just in case $A \not\cong B$ for any $B$ proper subset of $A$. Assuming the axiom of choice these two definitions agree, but in the absence of this axiom, a set could be Dedekind-finite without being finite.)

A set is countable if it is finite or in bijection with $\mathbb{N}$; equivalently, if it is empty or else it is the surjective image of $\mathbb{N}$. The set $\mathbb{N}$ is equipotent with each of its infinite subsets, and it is also equipotent with $Z$ using the bijection $\mathbb{N} \to Z$, $2n \mapsto n$ and $2n + 1 \mapsto -(n + 1)$. The function $J: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $J(n, m) = (n + m)(n + m + 1)/2 + n$ is a bijection, so $\mathbb{N} \times \mathbb{N}$ is countable. As any rational number can be written as $n/m$ with $n, m \in Z$, $m \in \mathbb{N} \setminus \{0\}$ and $n, m$ co-prime, we have that $Q$ is in bijection with a subset of $Z \times \mathbb{N} \preceq \mathbb{N} \times \mathbb{N}$, and therefore $\mathbb{Q} \preceq \mathbb{N}$. By further applying the map $J$, Cantor was able to prove that the set of all algebraic numbers is countable. (Note that $J$ essentially the bijection devised by Cantor in 1878; moreover $J$ and $(n, m) \mapsto J(m, n)$ are the only known polynomial functions that are a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ [Smo91].)
The next goal is to show that $\mathbb{R}$ is not countable, but in order to prove this we first digress a bit.

Note that if $f: A \to B$ is injective and $\bar{a} \in A$, then $g: B \to A$,

$$g(b) = \begin{cases} f^{-1}(b) & \text{if } b \in \text{ran } f \\ \bar{a} & \text{otherwise} \end{cases}$$

is surjective and $g \circ f: A \to A$ is the identity. Thus if $\emptyset \neq A \not\subseteq B$, then $B$ surjects onto $A$. Recall that the power set of $A$

$$\mathcal{P}(A) = \{B \mid B \subseteq A \}$$

is equipotent to the set of all functions from $A$ to $2 = \{0, 1\}$

$$^3A_2 = \{ f \mid f: A \to 2 \}$$

via the bijection $\mathcal{P}(A) \to ^3A_2$, $B \mapsto \chi_B$, mapping $B \subseteq A$ to its characteristic function. The set $^3A_2$ is usually denoted in mathematics as $2^A$; the first notation is preferable to the second when $A$ is a natural number or an ordinal: $^32$ is the set of all $2^3 = 8$ functions from $3 = \{0, 1, 2\}$ to $2 = \{0, 1\}$.

Clearly

$$A \not\subseteq B \Rightarrow \mathcal{P}(A) \not\subseteq \mathcal{P}(B)$$

and

$$A \not\times B \Rightarrow \mathcal{P}(A) \not\times \mathcal{P}(B).$$

The function $a \mapsto \{a\}$ shows that $A \not\subseteq \mathcal{P}(A)$, and hence $\mathcal{P}(A) \not\subseteq A$. The converse does not hold: if $F: A \to \mathcal{P}(A)$, the set $B = \{a \in A \mid a \not\in F(a)\}$ cannot be of the form $F(\bar{a})$ for any $\bar{a} \in A$. If fact, if $B = F(\bar{a})$ then $\bar{a} \in B \iff \bar{a} \not\in F(\bar{a}) = B$: a contradiction. We have therefore proved:

**Theorem 2.1 (Cantor).** For every set $A$, there is no surjection $A \to \mathcal{P}(A)$. ($^3$) In particular $\mathcal{P}(A) \not\subseteq A$ and hence $\mathcal{P}(A) \not\cong A$.

In particular, $\mathcal{P}(\mathbb{N})$ is uncountable. Let us show that $\mathbb{R} \not\cong \mathcal{P}(\mathbb{N})$ so that $\mathbb{R}$ is uncountable as well.

The set $\mathbb{R}$ can be construed as the set of all Dedekind sections, that is the set of all $\emptyset \neq x \subset \mathbb{Q}$ that are an initial segment of $\mathbb{Q}$ (that is to say: $q < p \in x \Rightarrow q \in x$) and have no maximum. It follows that $\mathbb{R} \not\subseteq \mathcal{P}(\mathbb{Q}) \times \mathcal{P}(\mathbb{N})$. The set $2^\mathbb{N}$ can be mapped injectively into $[0, 1] \subseteq \mathbb{R}$ by the function

$$C: 2^\mathbb{N} \to [0, 1], \quad s \mapsto \sum_{i=0}^{\infty} 2s(i) \cdot 3^{-i+1},$$

so $\mathcal{P}(\mathbb{N}) \not\subseteq \mathbb{R}$. By the Cantor-Schröder-Bernstein theorem it follows that $\mathbb{R} \not\cong \mathcal{P}(\mathbb{N})$.

**Remark 2.2.** -- ran $C \subseteq [0, 1]$ is the Cantor set, a well-known object studied in real analysis, topology, dynamical systems, etc. It is a closed, uncountable subset of the real line, of measure zero and empty interior. If $\mathbb{R} = \{0, 1\}$ is endowed with the discrete topology and $2^\mathbb{N}$ is given the product topology, then $C$ is a homeomorphism onto its image. For this reason $2^\mathbb{N}$ is known as the Cantor space.

Given three sets $A, B, C$, the function $\Phi: (A^B)^C \to A^{B \times C}$ sending each $\Phi(F): B \times C \to A$ defined as

$$\Phi(F)(b, c) = F(c)(b),$$

is a bijection. Keeping in mind that $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$, we have that

$$(1) \quad \mathbb{R} \times 2^\mathbb{N} \cong 2^{\mathbb{N} \times \mathbb{N}} \cong \mathbb{R}^\mathbb{N}.$$

In particular $\mathbb{R} \not\subseteq \mathbb{R} \times \mathbb{R} = \mathbb{C} \not\subseteq \mathbb{R}^\mathbb{N}$, so $\mathbb{C}$ is equipotent with $\mathbb{R}$.

Using these results one can easily verify that many sets encountered in mathematics are in bijection with $\mathbb{R}$.

**Example 2.3.** -- The set $\mathcal{C}(\mathbb{R}, \mathbb{R})$ of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$.

In fact a continuous function is completely determined by its behaviour on the rationals, so $\mathcal{C}(\mathbb{R}, \mathbb{R}) \not\subseteq \mathbb{R}^{\mathbb{Q}}$ from which we get $\mathcal{C}(\mathbb{R}, \mathbb{R}) \not\cong \mathbb{R}$.

**Example 2.4.** -- The set $\mathcal{H}$ of all entire functions.

Recall that an entire function is an $f: \mathbb{C} \to \mathbb{C}$ which is everywhere differentiable, and that every such $f$ can be written as a power series,
that is \( f(z) = \sum_{n \in \mathbb{N}} a_n z^n \) for suitable \( a_n \in \mathbb{C} \). Thus \( \mathcal{H} \not\subseteq \mathbb{C}^{\mathbb{N}} \times \mathbb{C} \). As \( \mathbb{C} \not\subseteq \mathcal{H} \) then \( \mathcal{H} \napprox \mathbb{C} \times \mathbb{R} \).

3. – The theory ZF

Naïve set theory, as usually presented in beginning math courses, is based on two principles: the axiom of extensionality and the principle of comprehension. The former states that two sets coincide just in case they have the same elements, while the latter asserts the existence of the set of all \( x \) that satisfy \( P(x) \), where \( P \) is a given property. This approach works fairly well if we just want to formalize simple concepts, but it quickly shows its inadequacy when more advanced notions are considered. For example, when we consider very large collections (such as the \( \propto \)-equivalence classes) we run into logical antinomies \(^{(5)}\), the most famous being

**Russell’s paradox.** By the principle of comprehension consider the set \( R = \{ x \mid x \notin x \} \) of all sets \( x \) that do not belong to themselves: does \( R \) belong to itself? One readily sees that \( R \in R \iff R \notin R \), a contradiction!

Secondly, several elementary questions on cardinalities are not easily solved with the tools of naïve set theory. For example:

**Question 3.1.** – Suppose \( A \) is uncountable. Is it true that \( A^\mathbb{N} \napprox A \)?

Another problem that cannot be easily solved using elementary methods is:

**Question 3.2.** – Suppose \( A \) is infinite. Is it true that \( A \times A \napprox A \)?

Cantor’s result summarized by equation (1) yields a positive answer to both Questions in specific cases: for example if \( A \napprox B^\mathbb{N} \) for some \( B \) (as in the case of \( A = \mathbb{R} \)) the answer to both questions is affirmative, and in view of Cantor’s bijection \( \mathbb{N} \npropto \mathbb{N} \times \mathbb{N} \), the answer to Question 3.1 is also affirmative when \( A \) is countable. These arguments, though, do not generalize to arbitrary sets.

In the first decades of the twentieth century, several distinct axiomatizations of set theory were introduced, aiming at avoiding the antinomies such as Russell’s paradox. The approach that was most successful is the theory Zermelo-Fraenkel ZF and its further extensions. Let us see how to formalize in ZF the notion of ordinal and cardinal numbers, two of the pivotal ideas introduced by Cantor.

The **ordinals** are sets \( x \) that are transitive \(^{(5)}\) (that is such that \( z \in y \in x \Rightarrow z \in x \)) on which the membership relation is a well-order—\( \text{the ordinals are denoted by lower-case Greek letters } \alpha, \beta, \ldots \). Ord is the class of all ordinals and the ordering on Ord is the member \( \subseteq \)-relation. The class Ord is well-ordered by \( \text{Thus natural numbers are ordinals, and so is the set } \mathbb{N} \), which in set theory is usually denoted by \( \omega \). It is possible to define on the class of ordinals the operations of addition, multiplication, and exponentiation, and check that they agree with the usual operations on the natural numbers. An ordinal is a **successor** if it is of the form \( x + 1 \equiv x \cup \{ x \} \); otherwise it is **limit**, if different from 0.

An ordinal \( x \) is a **cardinal** if it is not in bijection with some \( \beta \in x \), and Card is the class of cardinals. Every natural number is a cardinal, and so is \( \omega \). Not every ordinal is a cardinal: for example the ordinal \( \omega + 1 \) (that is: the set \( \omega \cup \{ \omega \} \)) is in bijection with \( \omega \) and hence it is not a cardinal. The **aleph** function \(^{(6)}\)

\[ \mathbb{N} : \text{Ord} \to \text{Card} \setminus \omega \]

enumerates all infinite cardinals. Thus \( \mathbb{N}_0 = \omega, \mathbb{N}_{x+1} \text{ is } (\mathbb{N}_x)^+ \text{ that is the smallest cardinal larger than } \mathbb{N}_x \), and if \( \lambda \) is limit, then \( \mathbb{N}_\lambda \) is the smallest cardinal larger than all \( \mathbb{N}_x \) with \( x < \lambda \). It is customary in set theory to write \( \omega_\alpha \) for \( \mathbb{N}_\alpha \). Let \( \kappa \in \text{Card} \) be an uncountable cardinal: we say \( \kappa \) is a **limit cardinal** if for any \( x < \kappa \) there is a cardinal \( \kappa' \) with \( x < \kappa' < \kappa \), otherwise it is a **successor cardinal**. Equivalently: a limit cardinal is of the form \( \mathbb{N}_\lambda \) with \( \lambda \) a limit ordinal, while a successor cardinal is of the form \( \mathbb{N}_{x+1} \).

\(^{(5)}\) Keep in mind that in ZF every object is a set; in other words: the elements of a set are also sets. 

\(^{(6)}\) \( \mathbb{N} \) is **aleph** the first letter of the Hebrew alphabet.
4. – Cardinality and the continuum problem

4.1 – The axiom of choice and cardinality

The theory ZF is not strong enough to efficiently handle the notion of cardinality. In order to solve this problem one adds the axiom of choice, obtaining thus the theory ZFC.

**Definition 4.1.** – The axiom of choice AC is the statement: for every nonempty family $A$ of nonempty sets, there is a choice function for $A$, that is to say a function $C$ with domain $A$ such that $C(x) \in x$ for every $x \in A$.

By the results of Gödel and Cohen, AC is independent of ZF, that is to say: working in ZF, it is neither possible to refute, nor to prove AC. The axiom of choice and Zorn’s Lemma (which is well known to be equivalent to AC) have countless consequences in many areas of mathematics. In many cases one can show that the theorems proved using choice are equivalent in ZF to AC. For example AC is equivalent to each of the following:

- for every surjective function $g : B \to A$ there is an injective function $f : A \to B$ such that $g \circ f$ is the identity on $A$;
- $A \not\preceq B$ or $B \not\preceq A$ for every pair of sets $A$ and $B$;
- every set is well-orderable, that is it is in bijection with an ordinal,
- if $A$ is infinite, then $A \cong A \times A$.(i)

Assuming AC every set is equipotent with an ordinal, and the least such ordinal is a cardinal.

**Definition 4.2 AC.** – The cardinality of $A$, in symbols $|A|$, is the unique $\kappa \in \text{Card}$ such that $A \cong \kappa$.

If $\kappa, \lambda \in \text{Card}$ then

- $\kappa + \lambda$ is the cardinality of $(\{0\} \times \kappa) \cup (\{1\} \times \lambda)$, the disjoint union of $\kappa$ and $\lambda$;
- $\kappa \cdot \lambda$ is the cardinality of $\kappa \times \lambda$;
- $\kappa^\lambda$ is the cardinality of $\mathcal{P}(\kappa)$.

These operations restricted to the naturals agree with the usual arithmetical operations. When $\kappa, \lambda \geq \omega$, then addition and multiplication are trivial, meaning that $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$, while if $2 \leq \kappa$ then $\kappa^\lambda > \lambda$ by Cantor’s Theorem 2.1.

**Remark 4.3.** – Since $(\{0\} \times \kappa) \cup (\{1\} \times \lambda)$ and $\kappa \times \lambda$ are well-orderable in ZF, the definitions of $\kappa + \lambda$ and $\kappa \cdot \lambda$ do not require AC. The situation for exponentiation is different: without some form of choice it is not possible to prove that $\aleph_2$ is well-orderable, so $2^{\aleph_0}$ would not be defined.

Replacing $\kappa \to \kappa^+$ with $\kappa \to 2^\kappa$ in the definition of the $\aleph$ function we obtain the beth function(6)

$$\beth : \text{Ord} \to \text{Card} \setminus \omega$$

defined as $\beth_0 = \omega$, $\beth_{\alpha+1} = 2^{\beth_\alpha}$ and $\beth_\lambda = \sup_{\beta<\lambda} \beth_\beta$ if $\lambda$ is limit. In some sense the $\beth$ function is more natural than the $\aleph$ function, as the size of most sets occurring in mathematics is of the form $\beth$. For example:

- countable infinite sets have size $\beth_0$,
- $\mathbb{R}$, $\mathbb{C}$, the family of Borel subsets of $\mathbb{R}$, a separable Banach space, … all have size $\beth_1 = 2^{\beth_0}$,
- $\mathbb{R}^\beta$, the family of Lebesgue measurable sets, the Stone–Čech compactification of the integers $\beta \mathbb{N}$, … all have size $\beth_2 = 2^{\beth_1} = 2^{2^{\beth_0}}$.

On the other hand, one would be hard pressed to find a concrete mathematical object of size $\aleph_1$ or $\aleph_2$. In fact even the definition of $\aleph_1$ is a bit contrived: it is the smallest kind of infinity above the countable. Kuratowski, extending previous work of Tarski, proved in 1951 a little known theorem with very concrete criterion as to when a set

**Definition 4.4.** – Let $(e_1, \ldots, e_n)$ denote the canonical basis of the vector space $\mathbb{R}^n$; a line parallel to $e_i$ is a set of the form $\{a + x e_i \mid x \in \mathbb{R}\}$, for some $a \in \mathbb{R}^n$. The set of all lines parallel to a non-zero vector $u$ is denoted by $\hat{u}$.

(i) Thus the answer to Question 3.2 is affirmative for an arbitrary infinite set $A$ if and only if AC holds.

(6) $\beth$ is beth, the second letter of the Hebrew alphabet.
With a minor abuse of notation, we extend this definition when \( R \) is replaced by some arbitrary set \( X \): a line parallel to \( e_i \) is a set of the form

\[
\{(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) \in X^n \mid x \in X\}
\]

for some \( a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in X \).

**Theorem 4.5 (Kuratowski).** For any \( n \) and any \( 2 \leq k \leq n + 2 \), the statement \(|X| \leq \aleph_n\) is equivalent to

\[
\exists A_1, \ldots, A_k (A_1 \cup \ldots \cup A_k = X^k)
\]

and

\[
\forall 1 \leq i \leq k \forall L \in \tilde{e}_i ([L \cap A_i] < \aleph_{n+2-k}).
\]

Therefore

- \( X \) is countable if its square can be partitioned into two parts so that every horizontal intersects the first part in a finite set, and every vertical line intersects the other part in a finite set;
- \( X \) has size \( \leq \aleph_1 \) if its square can be partitioned into two parts so that every horizontal intersects the first part in a countable set, and every vertical line intersects the other part in a countable set; or equivalently if its cube can be partitioned into three parts so that every line parallel to the coordinate axis intersects the relevant part in a finite set;
- and so on.

**4.2 – The continuum hypothesis**

Having shown that \(|R| > |N|\) and not having been able to exhibit a subset of \( R \) of intermediate cardinality, Georg Cantor conjectured that the cardinality of \( R \cong \mathcal{P}(N) \) was least possible:

\[
(2) \quad X \subseteq R \Rightarrow (X \not\subseteq N \text{ or } X \cong R).
\]

Every open interval is in bijection with \( R \), so an open subset of \( R \) is either empty, or else is in bijection with \( R \). Therefore every open set \( X \) satisfies (2).

Not every closed set is equipotent with \( R \), but Cantor proved that every closed set can be written as \( C \cup P \) where \( C \) is countable and \( P \) is closed with-out isolated points\(^{(9)}\); therefore a closed set is either countable or else it contains a homeomorphic copy of Cantor’s space. Therefore every closed set \( X \) satisfies (2). In other words: if \( X \) is open or closed, then it satisfies

\[
X \subseteq R \Rightarrow (X \not\subseteq N \text{ or } \exists f: 2^N \rightarrow X \text{ continuous embedding}).
\]

Not only (3) implies (2), it gives an explanation for its truth: a given subset of \( R \) is either small (i.e. countable) or else it is big (i.e. equipotent to \( R \)) for a topological reason. Property (3) has been verified for all Borel sets, but cannot hold for every set, as Felix Bernstein constructed an uncountable \( X \subseteq R \) that does not contain any copy of the Cantor set.

**Definition 4.6.** The continuum hypothesis (CH) is the statement \( 2^{\aleph_0} = \aleph_1 \).

Note that CH subsumes that \( R \) is well-orderable (i.e. some form of AC). The statement that (2) holds for every \( X \) is known as the weak continuum hypothesis, in symbols wCH: clearly it can be stated without choice, it is a consequence of CH, and under choice is equivalent to CH, that is to say AC \( \Rightarrow (CH \leftrightarrow wCH) \).

It is neither possible to prove nor to refute CH from ZFC (see Section 7), and the problem of establishing the cardinality of \( R \) is known as the continuum problem.

The only result provable in ZFC is that \( 2^{\aleph_0} \geq \aleph_1 \). For example, it is consistent with ZFC that the value of \( 2^{\aleph_0} \) is \( \aleph_n \) for any given \( n > 0 \); or else that it is \( \aleph_{\omega+1}, \aleph_{\omega+2}, \ldots \) or even larger, for example \( \aleph_{\omega_1} \). By Corollary 6.4 of Section 6, \(|R|\) cannot take any value: for example \( 2^{\aleph_0} \neq \aleph_\omega \).

\(^{(9)}\) This result, known as the Cantor-Bendixson theorem, is at the basis of descriptive set theory, a thriving area of research with many applications to other areas of mathematics. Its proof is a landmark in set theory: not only it introduced the concept of ordinal to the world, but served as a template for many other important results, such as Felix Hausdorff’s analysis of scattered linear orders.
4.3 – Is the continuum problem a real math problem?

Some mathematicians have expressed doubts over the fact that the continuum problem is a true math problem, a question that is relevant for the rest of mathematics. For example the late Solomon Feferman was a proponent of the thesis that CH is not a definite math problem. Giving a reasonable account of his point of view (and arguing for a rebuttal) would take too much space—the present author finds Feferman’s attitude towards set-theoretic methods not so different from the reactions that mathematicians of the XVII century would have had when confronted with a continuous function that is nowhere differentiable.

Another rather common attitude is to use independence results to infer that, since undecidable, the continuum hypothesis is not mathematically interesting. Results that depend on CH aren’t true results; if a problem turns out to depend on CH then you’d better change problem [Fol99, page 17]. This seems a rather peculiar position, as if from the non-existence of a method for solving by radicals all equations of degree bigger than four, we should infer the lack of interest for algebraic equations of higher degree, and maybe even for algebra and number theory as well.

At this point the reader would like to see a consequence of CH (or its negation) in mathematics. An exhaustive treatment of the consequences of CH and similar arguments would require a book of its own; here we just limit ourselves to a (far from being exhaustive!) list of topics in which set-theoretic techniques have played an important role:

- The Stone–Čech compactification of the integers βN is the set of all ultrafilters on N. It is a very important object for functional analysis and operator algebras, and it is becoming increasingly more relevant for Ramsey theory, a very active research area of combinatorics [HS12]. The structure of βN is most sensitive to the set-theoretic assumptions that are added to ZFC. For example, using CH one can construct special elements of βN (Ramsey ultrafilters, P-points, etc.) that have several applications to various problems.

- Functional analysis has always been a playground for set theory. For example, Kaplansky’s problems on automatic continuity for Banach algebras depends on CH [DW87]. Results on Banach spaces use increasingly sophisticated techniques, such as the Proper Forcing Axiom, a powerful generalization of the Baire category theorem that implies that 2^ω = ℵ_2; for example Steve Todorčević used this axiom to prove very general theorems on non-separable Banach spaces [Tod06].

- In the last few years many important results in C^*-algebras and von Neumann algebras have been obtained by Ilijaš Farah and his collaborators [Far11; CF14; Far+14], using techniques from logic and set theory.

- The use of set-theoretic methods in algebra has focused, initially, on the structure of infinite modules, in particular under the work of Saharon Shelah—see [EM02]. Among the more recent applications we would like to point to the paper [Kra+05].

5. – The continuum hypothesis in mathematics

In this section we look at a few results that not only depend on CH, but are actually equivalent to it.

5.1 – Complex analysis.

If ℱ is a subset of ℬ, the family of entire functions, and z ∈ ℂ let ℱ_z ≜ \{f(z) | f ∈ ℱ\}. Clearly, if ℱ is countable, then so is ℱ_z. The converse is equivalent to the negation of CH [Erd64].

**Theorem 5.1.** – ¬CH holds iff for every ℱ ⊆ ℬ, if ℱ_z is countable, for all z ∈ ℂ, then ℱ is countable.

Theorem 5.1 and its proof yields some further information on entire functions. By Example 2.4 |ℬ| = 2^{ℵ_0}. Say that ℱ ⊆ ℬ is κ-small if |ℱ_z| < κ for all z ∈ ℂ. Direction ⇒ in Theorem 5.1 follows from the next result when κ = ω_1.

**Lemma 5.2.** – If κ < 2^{ℵ_0} and ℱ ⊆ ℬ is κ-small, then |ℱ| < κ.
COROLLARY 5.3. – If $\mathcal{F}_z$ is finite for all $z \in \mathbb{C}$, then $\mathcal{F}$ is finite and hence there is an $n$ such that $|\mathcal{F}_z| \leq n$ for every $z$.

Theorem 5.1 can be phrased as follows: CH implies that there is $\mathcal{F} \subseteq \mathcal{H}$ of size $2^{2^{\aleph_0}}$ that is $2^{2^{\aleph_0}}$-small. Erdős [Erd64] asked whether this implication can be reversed. The answer is negative: it is consistent with ZFC the existence of an $\mathcal{F}$ of size $2^{2^{\aleph_0}} > \aleph_1$ which is $2^{2^{\aleph_0}}$-small [KS17]. In that model the continuum is quite large $2^{2^{\aleph_0}} = \aleph_n$ and it is not known if a negative answer to Erdős’ problem can be obtained with a small continuum, such as $2^{\aleph_0} = \aleph_2$.

5.2 – Real analysis.

THEOREM 5.4 ([Dav74]). – CH is equivalent to each of the following statements:

a) For every $f: \mathbb{R}^2 \to \mathbb{R}$ there are $g_n, h_n: \mathbb{R} \to \mathbb{R}$ such that for every $(x,y) \in \mathbb{R}^2$ the set
\[
\{n \in \omega \mid g_n(x) \cdot h_n(y) \neq 0\}
\]
is finite and $f(x,y) = \sum_n g_n(x) \cdot h_n(y)$.

b) As in (a), but with $f(x,y) = e^{x y}$.

By Cantor’s results we know that $\mathbb{R} \sim \mathbb{R}^{k+1}$; moreover there is a continuous surjection $[0;1] \to [0;1]^2$ (Peano’s curve).

THEOREM 5.5 ([Mor87]). – For every $k \geq 1$, CH is equivalent to the existence of a surjection $(f_1, \ldots, f_k, f_{k+1}): \mathbb{R}^{k+1} \to \mathbb{R}$, where $f_i: \mathbb{R} \to \mathbb{R}$ and $1 \leq i \leq k+1$, such that for any $x \in \mathbb{R}$ at least one among the $f_i$ is derivable in $x$.

In particular, CH $\iff \exists (f_1, f_2): \mathbb{R} \to \mathbb{R}^2$ surjective such that either $f_1(x)$ exists or else $f_2(x)$ exists for every $x \in \mathbb{R}$.

If $f_1, f_2$ are as in Theorem 5.5, define $g_j(x_1, x_2) = f_j(x_1)$ with $j = 1, 2$ and $g_3(x_1, x_2) = x_2$, so that $(g_1, g_2, g_3): \mathbb{R}^2 \to \mathbb{R}^3$ is surjective and differentiable with exceptions, in the following sense.

DEFINITION 5.6. – If $n, k \geq 1$, the function $(f_1, \ldots, f_{k+n}): \mathbb{R}^n \to \mathbb{R}^{k+n}$ where $f_j: \mathbb{R}^n \to \mathbb{R}$, is differentiable with exceptions if for any $a \in \mathbb{R}^n$ at least $n + k - 1$ among the $f_j$ are differentiable in $a$.

In other words: for all $a \in \mathbb{R}^n$ there is $j^*$ such that $1 \leq j^* \leq k + n$ so that $\frac{\partial f_j}{\partial x_i}(a)$ exists for all $j \neq j^*$ and all $1 \leq i \leq n$.

THEOREM 5.7 ([CMS84]). – For all $k \geq 1$, $2^{2^{\aleph_0}} \leq \aleph_n$ is equivalent to the existence of a surjection $(f_1, \ldots, f_{k+n}): \mathbb{R}^n \to \mathbb{R}^{k+n}$ that is differentiable with exceptions.

Thus $2^{2^{\aleph_0}} \leq \aleph_2$ if and only if there is a surjection $(f_1, f_2, f_3): \mathbb{R}^2 \to \mathbb{R}^3$ such that for any $(a, b) \in \mathbb{R}^2$, all derivatives $\frac{\partial f_j}{\partial x_i}(a, b)$ exist, with at most one exception.

5.3 – Euclidean spaces

For the next two results, recall that $(e_1, \ldots, e_n)$ is the canonical basis of the vector space $\mathbb{R}^n$ (Definition 4.4.)

THEOREM 5.8 ([Sie56]). – CH is equivalent to each of the following statements:

a) There are $A_1, A_2$ such that $\mathbb{R}^2 = A_1 \cup A_2$ and every horizontal line intersects $A_1$ in a countable set, and every vertical line intersects $A_2$ in a countable set.

b) There are $A_1, A_2, A_3$ such that $\mathbb{R}^3 = A_1 \cup A_2 \cup A_3$ and every line parallel to $e_i$ has finite intersection with $A_i$ ($i = 1, 2, 3$).

Theorem 5.8 is due to Sierpinski, but was proved in different decades: part (a) is from 1919 while part (b) is from 1951. It is the ancestor of Kuratowski’s Theorem 4.5, of whom is an immediate consequence—see [Sim91] for more on the history of this result.

THEOREM 5.9. – $2^{2^{\aleph_0}} \leq \aleph_n$ is equivalent to the existence of $A_1, \ldots, A_{n+2} = \mathbb{R}^{n+2}$ such that every line parallel to $e_i$ has finite intersection with $A_i$.

More generally, for every $k \leq n$, $2^{2^{\aleph_0}} \leq \aleph_n$ is equivalent to

$$\exists A_1, \ldots, A_{n+2-k}[A_1 \cup \ldots \cup A_{n+2-k} = \mathbb{R}^{n+2-k}$$

and

$$\forall L \in \mathbb{E} \exists a \in L \cap A_i < \aleph_k]$$

240
There is no need to work in high dimension to have a statement equivalent to $2^{\kappa_0} \leq \aleph_n$.

**Theorem 5.10 (Davies).** $- 2^{\kappa_0} \leq \aleph_n$ if and only if there are $A_0 \cup \ldots \cup A_{n+2} = \mathbb{R}^2$ and $0 \leq \theta_0 < \ldots < \theta_{n+2} < \pi$ such that every line with direction $\theta_i$ has finite intersection with $A_i$.

The following result in [EJM94] generalize Theorems 5.9 and 5.10.

**Theorem 5.11.** Let $\text{AffGr}_1(\mathbb{R}^k)$ be the affine Grassmannian manifold, that is the set of all lines of $\mathbb{R}^k$. Let $\lambda$ be a limit ordinal or 0 and let $n \in \omega$ be such that $\lambda + n > 0$. The following are equivalent:

a) $2^{\kappa_0} \leq \aleph_{\lambda+n} $;

b) For every $k, m \geq 2$ and every partition $L_1 \cup \ldots \cup L_m = \text{AffGr}_1(\mathbb{R}^k)$, there is a partition $A_1 \cup \ldots \cup A_m = \mathbb{R}^k$ such that $|L \cap A_i| \leq \aleph_{\lambda+n+1}$ for all $L \in \mathcal{L}$.

c) There are $k \geq 2$ and $n + 2 \geq m \geq 2$, there are $u_1, \ldots, u_m$ pairwise non-collinear vectors of $\mathbb{R}^k$ and a partition $\mathbb{R}^n = A_1 \cup \ldots \cup A_m$ such that $|L \cap A_i| \leq \aleph_{\lambda+n-1}$ for all $L \in \mathcal{L}$.

**Remark 5.12.** In Theorem 5.11 we adopted the following convention:

- if $s > 0$, then $|A| \leq \aleph_{-s}$ means that $A$ is finite, and
- if $\lambda$ is limit and $s > n$ then $|A| \leq \aleph_{\lambda+n-s}$ means that $|A| < \aleph_{\lambda+n}$.

**Theorem 5.13.** For every $k \geq 1$, CH holds if and only if there is a partition $\{D_n \mid n \in \omega\}$ of $\mathbb{R}^k$ such that for every $n \in \omega$ the set $D_n$ has distinct distances, that is to say: if $P_0, P_1, P_2, P_3 \in D_n$ are distinct, then $\{|d(P_i, P_j)| \mid 0 \leq i < j \leq 3\}$ has size 6.

In Theorem 5.13 the case $k = 1$ is from [EK43], the case $k = 2$ is from [Dav72], the general case $k \geq 3$ is from [Kum87].

Fix a point $C \in \mathbb{R}^2$: a **cloud with center** $C$ is a subset of $\mathbb{R}^2$ that has finite intersection with every line through $C$; a **star with center** $C$ is a subset of $\mathbb{R}^2$ that intersects every half-line from $C$ in a finite segment; a **spray with center** $C$ is a subset of $\mathbb{R}^2$ that has finite intersection with every circle centred in $C$.

Note that given a cloud $X$ with center $C$ one can construct a star $Y \supset X$ with the same center-- for each half-line $r$ passing through $C$ take the segment determined by the points that are furthest apart. It is easy to check that $\mathbb{R}^2$ cannot be covered with two stars (and hence by two clouds) or by two sprays; nor it can be covered by three stars (and hence by three clouds) whose centers are collinear.

In [GL01] it was asked whether the plane can be covered by three stars.

The next two theorems are due to Péter Komjáth [Kom01], James Schmerl [Sch03; Sch10] and Ra-miro de la Vega [Veg09].

**Theorem 5.14**

a) CH if and only if $\mathbb{R}^2$ is covered by three clouds.

b) $2^{\kappa_0} \leq \aleph_n$ if and only if $\mathbb{R}^2$ is covered by $n + 2$ clouds.

**Theorem 5.15**

a) $\mathbb{R}^2$ is covered by three sprays whose centers are not collinear;

b) CH if and only if $\mathbb{R}^2$ is covered by three sprays whose centers are collinear.

In [Kom01] it is announced that it is consistent with ZFC $-\text{CH}$ that the plane cannot be covered with three stars.

5.4 – Algebra.

The next two results are essentially contained in [EK43].

**Theorem 5.16.** Let $V$ be a vector space over $\mathbb{Q}$ such that $V \neq \mathbb{R}$.

$2^{\aleph_0} \leq \kappa^+$ if and only if there is a partition $V = \bigcup_{\kappa \in \mathcal{K}} A_\kappa$ such that there are no distinct vectors belonging to the same $A_\kappa$ such that $a + b = c + d$.

Letting $\kappa = \aleph_0$ we have that CH holds just in case there is a partition $V = \bigcup_{\kappa \in \mathcal{K}} A_\kappa$ such that there are no distinct vectors $a, b, c, d$ belonging to the same piece $A_\kappa$ such that $a + b = c + d$. 

CANTOR’S CONTINUUM HYPOTHESIS: CONSEQUENCES IN MATHEMATICS AND ITS FOUNDATIONS 241
Theorem 5.17. \( -2^{\aleph_0} \leq \kappa^+ \) if and only if \( \mathbb{R} \setminus \{0\} \) is the union of \( \kappa \) many \( \mathcal{Q} \)-independent sets. In particular \( \text{CH} \) if and only if \( \mathbb{R} \setminus \{0\} \) is the union of countably many \( \mathcal{Q} \)-independent sets.

If we look at algebraic independence we obtain a similar result.

Theorem 5.18 [Zol06]. \( -2^{\aleph_0} \leq \kappa^+ \) if and only if the set of all transcendental numbers can be covered by \( \kappa \) many algebraically independent sets. In particular \( \text{CH} \) if and only if the set of all transcendental numbers is the union of countably many algebraically independent sets.

A set \( X \) is union of a chain of subsets of size \( \kappa \) if \( X = \bigcup C \) where \( C \) is a family of subsets of \( X \), each of size \( \kappa \), which is linearly ordered under inclusion.

Theorem 5.19. \(|X| \leq \kappa \) if and only if \( X \) is the union of a chain of subsets of size \( \kappa \). Thus \( \text{CH} \) if and only if \( \mathbb{R} \) is the union of a chain of countable subsets.

In contrast with the previous results, Theorem 5.19 is a fact in infinite combinatorics, one that does not use anything of the algebraic (or analytic, or geometric) structure of \( \mathbb{R} \).

It can be restated replacing \( \mathbb{R} \) with any algebraic structure \( X \) equipotent to it, and requiring that the subsets be substructures of \( X \). For example \( \text{CH} \) is equivalent to the statement that \( C \) is union of a chain of countable (algebraically closed) fields.

6. – Cardinal arithmetic

If \( \omega \) is partitioned into finitely many pieces, then at least one piece is infinite, since the union of finitely many finite sets is finite. Similarly, if \( \omega_1 \) is partitioned into countably many pieces, then at least one piece is of size \( \aleph_1 \), since the countable union of countable sets is countable\(^{(10)}\). These pigeon-hole-type results can be extended to larger cardinals.

Theorem 6.1 [AC]. – If \( \kappa^+ = \bigcup_{\lambda < \kappa} A_\lambda \) then \( |A_\lambda| = \kappa^+ \) for some \( \lambda < \kappa \).

The previous result suggests the following

Definition 6.2. – Let \( \kappa \) be an infinite cardinal. We say that \( \kappa \) is regular if for all \( \lambda < \kappa \) and all partitions \( \kappa = \bigcup_{\lambda < \kappa} A_\lambda \) there is \( \lambda < \lambda \) such that \( |A_\lambda| = \kappa \). Otherwise we say that \( \kappa \) is singular.

Theorem 6.1 says that \( \kappa^+ \) is regular, while \( \aleph_\omega \) is singular, since \( \aleph_\omega = \bigcup_{\alpha < \omega} \aleph_\alpha \). Similarly \( \aleph_\omega \) is singular since \( \aleph_\omega = \bigcup_{\alpha < \omega} \aleph_\alpha \). On the other hand if \( \aleph_\omega = \bigcup_{\alpha < \omega} \aleph_\alpha \), then \( |A_\lambda| = \aleph_\omega \) for some \( \alpha \).

To see this, suppose each \( A_\alpha \) has size \( \aleph_\omega \); as \( \aleph_\omega < \omega_1 \), the regularity of \( \omega_1 \) yields that \( \bigcup_{\alpha < \omega} \aleph_\alpha \neq \omega_1 \) so \( \bigcup_{\alpha < \omega} \aleph_\alpha = \aleph_\omega < \omega_1 \), and hence \( |\bigcup_{\alpha < \omega} A_\alpha| = \aleph_\omega \cdot \aleph_\omega = \aleph_\omega < \aleph_\omega \). In other words: although \( \aleph_\omega \) can be written as \( \bigcup_{\lambda < \omega} A_\lambda \) with \( \lambda < \aleph_\omega \) and \( |A_\lambda| < \aleph_\omega \) for each \( \lambda \), the size of \( \lambda \) must be at least \( \omega_1 \). In order to explain this phenomenon, we need to introduce a new notion.

The cofinality of an infinite cardinal \( \kappa \), in symbols \( \text{cof}(\kappa) \), is the smallest ordinal \( \lambda \) such that there is a cofinal function \( f: \lambda \to \kappa \), that is such that the values \( \{ f(\alpha) | \alpha < \lambda \} \) are unbounded in \( \kappa \). Since the identity function on \( \kappa \) is cofinal, one has that \( \text{cof}(\kappa) \leq \kappa \). The ordinal \( \text{cof}(\kappa) \) is actually a cardinal, and moreover the function \( f: \text{cof}(\kappa) \to \kappa \) witnessing cofinality can always be taken to be increasing, so that \( \text{cof}(\text{cof}(\kappa)) = \text{cof}(\kappa) \). It can be shown that \( \text{cof}(\kappa) \) is the least cardinal \( \lambda \) such that \( \kappa = \bigcup_{\lambda < \kappa} A_\lambda \) with \( |A_\lambda| < \kappa \). In other words: \( \kappa \) is a regular cardinal if and only if \( \text{cof}(\kappa) = \kappa \).

Julius König in 1908 proved the following result.

Theorem 6.3. – \( \kappa^{\text{cof}(\kappa)} > \kappa \).

As \( \text{cof}(\kappa) \leq \kappa \), Theorem 6.3 implies that \( 2^\kappa = \kappa^+ > \kappa \), so the concept of cofinality allows us to strengthen Cantor’s Theorem 2.1. Moreover, if \( \kappa \) is an infinite cardinal of countable cofinality then \( \kappa^{\text{cof}(\kappa)} > \kappa \), showing that the answer to Question 3.1 is negative\(^{(11)}\).

If the cofinality of \( 2^\kappa \) were less or equal to \( \kappa \), then putting \( 2^\kappa \) in place of \( \kappa \) in Theorem 6.3 we would have

\(^{(10)}\) Actually, this innocent looking theorem requires a weak form of the axiom of choice.

\(^{(11)}\) Question 3.1 appears in a well-known Algebra textbook.
that \( 2^\kappa < (2^\kappa)^{\text{cf}(2^\kappa)} = 2^\kappa \cdot 2^\kappa = 2^\kappa \), a contradiction. We have therefore proved:

**Corollary 6.4.** \( \text{cf}(2^\kappa) > \kappa \).

It follows that \( \text{cf}(2^\kappa) \) is uncountable, and hence \( 2^{\aleph_0} \neq \aleph_1 \) for any countable limit ordinal \( \lambda \). All other values for \( 2^{\aleph_0} \), the ones not ruled out by König’s Theorem 6.3 are acceptable: it has been shown that \( 2^{\aleph_0} \) can be \( \aleph_1, \aleph_2, \ldots \), or \( \aleph_{\omega+1}, \aleph_{\omega+2}, \ldots \) or a singular cardinal of uncountable cofinality, such as \( \aleph_{\omega_1} \).

But even if we knew the value \( 2^{\aleph_0} \) there would still be the problem of computing \( 2^\kappa \) for \( \kappa > \omega \); even assuming CH we have no clue as to what \( 2^\kappa \) might be, other than it must be a cardinal of cofinality \( \geq \aleph_2 \).

In analogy with CH Hausdorff introduced the following definition.

**Definition 6.5.** The **generalized continuum hypothesis** (GCH) is the statement \( \forall \kappa \in \text{Ord} \Rightarrow 2^{\aleph_0} = \aleph_{\kappa+1} \). Equivalently: \( \aleph_\kappa = \beth_\kappa \) for all \( \kappa \).

In analogy with the weakening of CH to \( \text{wCH} \), we could state a weak version of the generalized continuum hypothesis

\[ \forall \kappa \in \text{Ord} \forall X \subseteq \mathcal{P}(\aleph_\kappa)(X \nsubseteq \aleph_\kappa \text{ or } X \sim \mathcal{P}(\aleph_\kappa)), \]

but this statement implies the axiom of choice, so it is indeed equivalent to the GCH.

As we shall see in the next section, GCH is consistent with ZFC, and it is a dramatic simplification of cardinal arithmetic. In particular GCH implies that \( 2^\kappa \) is always a regular cardinal.

If we do not assume GCH, what can we say on the exponential function \( \kappa \mapsto 2^\kappa \)? We know that it is monotone (\( \kappa \leq \lambda \Rightarrow 2^\kappa \leq 2^\lambda \)) and that König’s Theorem holds (\( \text{cf}(2^\kappa) > \kappa \)).

Are there other rules, provable in ZFC, that govern the exponential function? The answer is negative if we only consider regular cardinals: if \( F \) is any map on regular cardinals such that \( \kappa \leq \lambda \Rightarrow F(\kappa) \leq F(\lambda) \), and \( \text{cf}(F(\kappa)) > \kappa \), then we may assume that \( 2^\kappa = F(\kappa) \) for all regular cardinals \( \kappa \). But what about \( 2^\kappa \) when \( \kappa \) is a singular cardinal? The general consensus among set theorists was that a similar independence result should be established for singular cardinals as well, but in 1974 Jack Silver showed that this expectation had to be abandoned.

**Theorem 6.6.** If \( 2^{\aleph_0} = \aleph_{\alpha+1} \) for every \( \alpha < \omega_1 \), then \( 2^{\aleph_1} = \aleph_{\omega+1} \).

In other words: GCH cannot fail first at \( \aleph_1 \). Silver’s result is actually much more general, in particular it holds if \( \aleph_{\omega_1} \) is replaced by a singular cardinal of uncountable cofinality. What about singular cardinals of countable cofinality? For example, if \( 2^{\aleph_0} = \aleph_{n+1} \) for all \( n < \omega_1 \), is it true that \( 2^{\aleph_1} = \aleph_{\omega+1} \)? Menachem Magidor in 1978 showed that the answer is negative: it is consistent that GCH fails for the first time at \( \aleph_\omega \), e.g. \( 2^{\aleph_\omega} = \aleph_{\omega+1} \) for all \( n \) and \( 2^{\aleph_\omega} = \aleph_{\omega+2} \). The value \( 2^{\aleph_\omega} \) can be made larger than \( \aleph_{\omega+2} \), but not arbitrarily large. In fact, in 1989 Saharon Shelah proved the following result.

**Theorem 6.7.** If \( 2^{\aleph_\omega} = \aleph_n \) for all \( n \), then \( 2^{\aleph_\omega} < \min(\aleph_\omega, \aleph_{\aleph_\omega}) \).

The interested reader should consult [Jec03]. What has emerged after the last three decades of work in set theory is that there are highly non-trivial, new laws that rule the arithmetic of singular cardinals. This is hardly the end of the story, in fact it looks like it is only the beginning.

### 7. Independence of the continuum hypothesis and new perspectives

In this section we try to give some ideas of the independence phenomenon, and the current work in the foundations of set theory. The material is considerably more advanced than what we have discussed so far, and at times we will assume a passing acquaintance with some of the concept currently investigated in set theory, such as large cardinals and determinacy (\( \omega^2 \)).

#### 7.1 An overview of the universe of all sets.

Recall that in axiomatic set theory, the elements of a set are again sets. The (proper) class of all sets is

---

\( \omega^2 \) See also Giorgio Venturi and Matteo Viale’s contribution “New axioms in set theory” in this volume.
denoted by $V$, after von Neumann. It is stratified in a hierarchy of sets

$$V = \bigcup_{x \in \text{Ord}} V_x$$

where $V_0 = \emptyset$, $V_x = \bigcup_{\beta < x} V_\beta$ for $x$ a limit ordinal, and $V_{x+1} = \mathcal{P}(V_x)$. The $V_x$s are transitive, increasing (that is: $x < \beta \Rightarrow V_x \subset V_\beta$), and can be seen as an approximation to the whole universe. We pause for a few examples.

**Example 7.1**

a) $V_x \cap \text{Ord} = x$ and moreover if $x$ is limit, then it is closed under ordered pairs. In fact if $x, y \in V_x$, then $x, y \in V_\beta$ for some $\beta < x$, and since, following Kuratowski, the ordered pair $(x, y)$ is $\{\{x\}, \{x, y\}\}$, we have that $(x, y) \in V_{x+2} \subseteq V_x$.

b) The set $V_\omega$ is the collection of all **hereditarily finite** sets, that is those sets that are finite, and whose elements are finite, and whose elements of the elements are finite, and so on. Equivalently, $V_\omega$ is the smallest collection of sets having $\emptyset$ as an element, and closed under finite unions and the operation taking singletons. It is not hard to see that $V_\omega$ is countable. By part (a) $\mathbb{N} = \omega$ is a subset of $V_\omega$. In fact it is possible to construe $\mathbb{Z}$ and $\mathbb{Q}$ and as subsets of $V_\omega$. To see this identify $\mathbb{Z}$ with the union of the two sets $\{1\} \times \omega$ and $\{0\} \times (\omega \setminus \{0\})$, the first set in being identified with $\mathbb{N}$ and the second with the set of negative integers. Similarly $\mathbb{Q}$ can be construed as the collection of all pairs $(n, m)$ with $n, m \in \mathbb{Z}$ relatively prime and $m > 0$.

c) The set $V_{\omega+1}$ is equivalent with $\mathbb{R}$, and since a real number can be identified with the set of rationals strictly smaller than itself, one can assume that $\mathbb{R} \subseteq V_{\omega+1}$.

There is another way to stratify the universe of all sets. The **transitive closure** $\text{TC}(x)$ of a set $x$ is the smallest transitive set containing $x$. Let $H_x$ be the set of all $x$ such that $\text{TC}(x)$ has size $< \kappa$. Then

$$V = \bigcup_{x \in \text{Card}} H_x.$$ 

Note that $V_\omega = H_\omega$, that $V_{\omega+1} \subseteq H_\omega$, and that $|H_\omega| = 2^{\omega_0}$.

The vast majority of mathematical objects encountered in mathematics belongs to (or better: can be identified with an isomorphic copy of itself belonging to) $V_{\omega+\eta}$, for some $\eta \in \omega$, so one might wonder what is the point of studying arbitrary $V_\omega$s and $H_\omega$s, and, more generally, sets of arbitrary cardinality. One of the main discoveries in set theory in the last fifty years has been the positive, and somehow ubiquitous influence of large cardinals on just about every aspect of set theory (13). In particular, the existence of large cardinals yields a very detailed analysis of the structure of definable (e.g. Borel, projective, ...) sets of reals. The interested reader can find some basic information on these matters in [And03a; And03b] and in the author’s chapter in [HLT15].

7.2 – **Gödel’s constructibility and Cohen’s forcing.**

As we have said before, the continuum hypothesis is independent from ZFC, that is to say: starting from ZFC it is not possible to prove or refute $\text{CH}$. Recall that an axiomatic theory $\mathcal{T}$ is said to be **consistent** if it is free from contradictions, and it is **effectively axiomatizable** if the axioms of $\mathcal{T}$ form a list that can be checked in an automatic manner. Gödel’s Second Incompleteness Theorem asserts that an effectively axiomatizable, sufficiently powerful theory $\mathcal{T}$ (such as ZFC) cannot prove its own consistency, unless $\mathcal{T}$ is itself inconsistent. In 1938 Gödel showed that if ZFC is consistent then also ZFC + $\text{CH}$ is consistent, and in 1963 Cohen showed that if ZFC is consistent then also ZFC + $\neg \text{CH}$ is consistent.

7.2.1 – **The constructible universe.**

Given a set $M$, a subset $X \subseteq M$ is said to be **definable in $M$ with parameters** if there is a formula $\varphi(v_0, v_1, \ldots, v_n)$ and elements $p_1, \ldots, p_n \in M$ such that $X$ is the set of all elements $x$ of $M$ that satisfy $\varphi$ using the parameters $p_1, \ldots, p_n$, in symbols

$$x \in X \iff (M, \in) \models \varphi(x, p_1, \ldots, p_n).$$

(13) Gödel was probably the first logician to suggest that ZFC should be strengthened by positing the existence of large cardinals.
The collection of all $X$ as above is denoted by $\text{Def}(M)$, and it is a collection of subsets closed under unions, intersections, and complements; in other words $\text{Def}(M)$ is a Boolean algebra. Let us pause for some examples.

**Example 7.2**

(i) If $|M|=\kappa \geq \omega_1$, then $|\text{Def}(M)|=\kappa$, since any $X \in \text{Def}(M)$ is determined by a formula $\varphi$ (of which there are countably many) together with an $n$-tuple of elements of $M$, for some $n$.

(ii) Among the definable subsets of $V_{\omega_1}$ we have:
- all recursive (i.e., computable) subsets of $\mathbb{N}$,
- the sets $\mathbb{Z}$, $\mathbb{Q}$ (Example 7.1(b)) and all computable real numbers (Example 7.1(c)).

Thus by part (i) above, $\text{Def}(V_{\omega_1})$ is countable so it is a proper subset of $V_{\omega_1+1}$. Gödel’s constructible universe is obtained by modifying the definition of the hierarchy $(V_\alpha \mid \alpha \in \text{Ord})$: rather than using the operation $\mathcal{P}$ of taking all subsets we use the operation $\text{Def}$ of taking only the definable subsets. The **constructible universe** is the transitive class

$$L = \bigcup_{\alpha \in \text{Ord}} L_\alpha$$

where $L_0 = \emptyset$, $L_{\omega+1} = \text{Def}(L_\omega)$, and $L_\lambda = \bigcup_{\beta < \lambda} L_\beta$ for $\lambda$ a limit ordinal. The definition of the map $\alpha \mapsto L_\alpha$ can be carried out in $\mathsf{ZFC}$, and it can be shown that every axiom of $\mathsf{ZF}$ holds when restricted to $L$. In fact, working in $\mathsf{ZF}$, it is possible to show that the axiom of choice holds in the constructible universe, so that every theorem of $\mathsf{ZFC}$ is true inside $L$. The inhabitants of $L$ can also develop their definition of the constructible hierarchy; if $L$ thinks that a certain set $M$ is the $\alpha$-th level of the constructible hierarchy, then indeed $M = L_\alpha$. Using this fact one can prove that $L$ satisfies the statement that every set is constructible, that is the statement $\forall x \exists \alpha (x \in L_\alpha)$ holds true in $L$. We abbreviate this statement as $V = L$. As the axioms of $\mathsf{ZFC}$ are true in $L$, this implies that the existence of a non-constructible set cannot be proved in $\mathsf{ZFC}$. Moreover from $V = L$ one can prove the GCH, and more. From all this we obtain that

if $\mathsf{ZF}$ is consistent, then so is $\mathsf{ZFC} + \text{GCH}$. The axiom $V = L$ yields a very detailed, highly uniform description of the universe of all sets, and solves most of the set-theoretic problems one might encounter, yet is generally rejected by the set theorists as a viable axiom. The reason for this rejection is threefold. Firstly, requiring that every set be obtained by taking only definable subsets seems an unduly restriction; in fact Gödel himself thought that this was a most convincing argument that $V$ cannot be equal to $L$. Secondly, the picture of projective sets of the reals emerging from $V = L$ is very distant from the results that we can prove in $\mathsf{ZFC}$ on Borel or analytic sets. Thirdly, and more importantly, the constructible universe is too small to accommodate large cardinals, a topic that has become increasingly important for set theory in the last few decades.

### 7.2.2 The method of forcing

After Gödel’s landmark result that $\text{GCH}$ is consistent with $\mathsf{ZFC}$, the question of Cantor’s continuum hypothesis being provable from $\mathsf{ZFC}$ became even more prominent. Since $\text{GCH}$ follows from the statement that $V = L$, any proof of the consistency of $\neg\text{CH}$ would entail that $V = L$ is unprovable from $\mathsf{ZFC}$. By its very nature, $L$ is minimal among the transitive proper classes $M$ that satisfy the axioms of $\mathsf{ZFC}$, and this implies that the quest for a construction in $\mathsf{ZFC}$ of such an $M$ satisfying $\neg\text{CH}$, is doomed to failure. The way out of this conundrum is to give up either on $M$ being a proper class, or else on $M$ being transitive. The first option is adopted in the expositions Cohen’s method of forcing: starting with a countable transitive model of (a large enough fragment of) $\mathsf{ZFC}$, one develops a larger countable transitive model in which $\text{CH}$ fails. Forcing is a great method to obtain new independence results, but with a fairly steep learning curve. There is another approach to obtain independence proofs, completely equivalent to forcing, but somewhat simpler to explain; it was developed by Dana Scott and Robert Solovay in the mid 60s, on wake of Cohen’s results, and it is called the **Boolean valued models** method. In introductory courses in logic one gives the formal definition of

the structure $M$ satisfies the formula $\varphi(x_1, \ldots, x_n)$ when we assign $u_1, \ldots, u_n \in M$ to the variables $x_1, \ldots, x_n$
in symbols: \( M \models \varphi(u_1, \ldots, u_n) \). Thus given \( \varphi, M \)
and \( u_1, \ldots, u_n \in M \), one assigns values 1 or 0 to
\( \varphi(u_1, \ldots, u_n) \) just as in case \( M \models \varphi(u_1, \ldots, u_n) \) or not.
The key idea of Boolean valued models is to redefine the set \( \{0, 1\} \) replacing the set \( \{0, 1\} \)
with a complete Boolean algebra \( B \). One then constructs a \( B \)-valued model \( [\mathcal{V}]_B \)
by interpreting each statement \( \varphi(u_1, \ldots, u_n) \) in
the language of set theory as \( [\varphi(u_1, \ldots, u_n)]_B \) in \( B \),
where \( \varphi \) is a well-formed formula in the language of set theory.

The system of \( \mathcal{V} \) is complete if suprema and infima
exist for any set.

7.3 – Woodin’s work on the foundations of set theory.

After the deluge of independence results that followed from the
invention of forcing, for many years it seemed that no solution for
the continuum problem was possible. In the mid nineties W. Hugh Woodin
started a thorough investigation of the structure
(\( H_{\omega_2}, \in \)). Recall that \( H_{\omega_1} \), the set of all hereditarily
finite sets, is equivalent to the realm of arithmetic
((\( \mathbb{N}, +, \times \)), while \( H_{\omega_1} \), the set of all hereditarily
countable sets, is equivalent to the structure
\( (\mathbb{N} \cup \mathcal{P}(\mathbb{N}), +, \times, \in) \). Woodin has argued that
any correct axiomatization of \( H_{\omega_1} \)

is given by the axiom of projective determinacy, much
like Peano’s arithmetic is the correct axiomatization of
((\( \mathbb{N}, +, \times \)). Furthermore he has singled out an
axiomatization of \( (H_{\omega_1}, \in) \), showed that it is canonical, and
that it implies \( 2^{\aleph_1} = \aleph_2 \). Unfortunately this approach
does not seem to generalize to larger \( H_{\kappa} \).
The reader interested in this topic is referred to the papers
[Wood91; Wood92] or to the formidable [Wood99].

In the last ten years Woodin started a massive program
to generalize Gödel’s L in order to accommodate
all large cardinals. This idea has been one of the
main goals of set theory for the last fifty years
(the so-called inner model program) but progress in
this area has been quite slow, hitting some roadblocks
at the beginning of this century. Woodin has
isolated the main obstruction, and although he has
still not been able to remove it, he has proved some
very general theorems showing that in some sense
this is the only block. If Woodin’s approach will be
successful, it would yield a transitive proper class,
called Ultimate-L, which is sufficiently L-like to
guarantee that the generalized continuum hypothesis
holds in it. In other words: Ultimate-L should
give a very concrete conception of the notion of set,
similar to the conception of natural numbers
that we are accustomed to. A complete account of
these matters has not been completely written down,
but the reader can consult [Rid15], or [Wood17] for a
general overview of the program. Regardless of the
final outcome of these investigations, we agree with
Woodin’s remarks expressed in [Wood91b]:

So, is the Continuum Hypothesis solvable?
Perhaps I am not completely confident the “solution” I have sketched is the solution, but it is
for me convincing evidence that there is a so-

---

\(^{(14)}\) A Boolean algebra is complete if suprema and infima
exist for any set.
lution. Thus, I now believe the Continuum Hypothesis is solvable, which is a fundamental change in my view of set theory... The universe of sets is a large place. We have just barely begun to understand it.

References


