An Analysis of the Continuum Hypothesis

Andrew Powell[1]

1 Imperial College London

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.

Abstract

This paper analyses the Continuum Hypothesis, that the cardinality of a set of real numbers is either finite, countably infinite or the same as the cardinality of the set of all real numbers. It argues that the Continuum Hypothesis makes sense as a very strong choice principle that is maximally efficient as a principle for deciding whether a real number is in a set of real numbers, in the sense that it is uniform in deciding membership for every real number in a countable number of steps. The approach taken is to analyze the intended meaning of the Continuum Hypothesis rather than to analyze models of set theory in which the Continuum Hypothesis is true or false and to use those models to support or reject the Continuum Hypothesis.

Andrew Powell

Institute for Security Science and Technology, Imperial College, South Kensington Campus, London, SW7 2AZ. E-mail address: andrew.powell@imperial.ac.uk.

Keywords: Axiom of Choice, Continuum Hypothesis.

2000 Mathematics Subject Classification: 03E17.

1. Introduction

This short paper analyses the Continuum Hypothesis (CH), which states that the cardinality of a set of real numbers is either finite, countably infinite, or the same as the cardinality of the set of all real numbers. The approach taken is to analyze the intended meaning of CH rather than to analyze models of the real numbers in which CH is true or false and to use those models to support or reject CH. The latter approach has a complex and extensive literature (see Rittberg (2015); Schindler (2021) for accessible discussions), but will not be considered here since the set of subsets of all real numbers is the only model that counts as far as determining the truth value of CH is concerned. Historically the earliest approach to CH from Cantor's time has been to classify the topological complexity of sets, a subject known as *descriptive set theory* (see (Hausdorff (1957); Martin (1977); Kechris (1995)) for example), which remains a powerful stimulus to the foundations of real analysis and set theory to this day. But this approach has a huge literature and would require a survey of descriptive set theory, and will therefore not be covered here. A fourth approach is to find propositions equivalent to CH, which was originally due to Sierpiński (see Sierpiński (1934); Martin (1970); Moore (2017) and Streprans (2012) for a survey), in the hope that statements equivalent to CH or consequences of CH will be more obviously true or false than CH itself. This approach will also not be considered here.

The reason for the focus on meaning is that at a minimum it will be possible to understand the claim (or potentially claims) that CH represents. This is a "bottom-up" approach to understanding CH, which does not depend on whether some powerful axiom of set theory is true or not. The other approaches mentioned above (with the exception of propositions equivalent to CH) lead to axioms that are not provable from the standard axiomatization of the cumulative hierarchy of sets, Zermelo Fraenkel (ZF) set theory, see (Shoenfield 1977) for an intuitive motivation of ZF. Of course, since CH is also independent of ZF (see (Gödel 1940; Cohen 1963)), CH itself or its negation could be taken to be axioms of set theory. The question is: is CH or its negation a reasonable axiom to assert? It is this question that this paper tries to address.

The intended meaning of CH goes back to Cantor and Zermelo (see Dauben (1979); Hallett (1986); Kanamori (1996)) and is based on the view that *all infinite sets* are like the *set of natural numbers* at least to the extent that they are definite and can be enumerated (albeit in general by infinitary functions, *i.e.* functions which cannot be represented by a finite algorithm).[1] In addition to the focus on the meaning of CH and the use of infinitary methods, this paper combines algorithms and ideas from computability complexity theory with the theory of sets of real numbers.

This paper considers some principles that relate to CH and argues that CH is a very strong choice principle that is equivalent to the ability to decide membership of a set of real numbers uniformly (that is, which does not depend on the nature of the putative member of the set) in a countable number of steps. It is argued on the grounds of analogy with the natural numbers and the countable amount of information in each real number that CH is a reasonable principle to assert.

2. Preliminaries

In the following definitions, standard logic symbols are used as a means of notational compactness: $\vee$ for "or", $\wedge$ for "and", $\Rightarrow$ for "implies", $\exists$ for "there exists" and $\forall$ for "for all". Definitions are taken where possible from a standard text on set theory, Jech (2002).

Definition of linear ordering. A set X is *linearly ordered* by *linear ordering* $<$ if $(\forall x \in X)(\forall y \in X)((x < y) \vee (x = y) \vee (y < x))$, where $x \not< x$, $x < y \wedge y < z \Rightarrow x < z$ for all x, y, z (see Jech (2002) Definition 2.1).

Definition of well-ordering. A set X is *well-ordered* by *well-ordering* $<$, written $\langle X, < \rangle$, if X is linearly ordered by $<$ and for all non-empty $Y \subseteq X$ $(\exists z \in Y)(\forall y \in Y)((z < y) \vee (z = y))$ (see Jech (2002) Definition 2.3).

Definition of enumeration. An *enumeration* of a set X is a well-ordering of X.

Definition of ordinal. A well-ordered set $\langle X, < \rangle$ has an *order type* or *ordinal* which is a measure of order complexity that applies to any well-ordered set $\langle Y, \prec \rangle$ for which there is a one-to-one function f such that $f(X) = Y$ and $x < y$ if and only if $f(x) \prec f(y)$ (compare Jech (2002) Definition 2.2).[2]

Definition of a real number. We can identify a real number as a binary ω-sequence, written as $\langle f_i \rangle_{i<\omega}$, that is to say a function $f: \mathbb{N} \rightarrow \{0, 1\}$ where $\mathbb{N}$ is the set of all natural numbers and ω is the order type of the natural numbers in their standard strictly increasing ordering $0, 1, 2, \ldots$ (see Feferman (2009)).

Definition of lexicographical linear ordering. There is a natural *lexicographical* linear ordering on the real numbers given by $\langle x_i \rangle_{i<\omega} < \langle y_i \rangle_{i<\omega}$ if $(\exists k < \omega)[(\forall l < k)(x_l = y_l) \wedge (x_k < y_k)]$, $\langle x_i \rangle_{i<\omega} = \langle y_i \rangle_{i<\omega}$ if $(\forall l < \omega)(x_l = y_l)$ and $\langle y_i \rangle_{i<\omega} < \langle x_i \rangle_{i<\omega}$ otherwise (see Halmos (1974) Section 14).

Definition of a binary tree. A *set of real numbers* is identified with a binary tree, where a *binary tree* T comprises a set of *branches*, that is to say a set of binary ω-sequences (see Feferman (2009)). The *set of all real numbers* is denoted by $\mathbb{R}$.

Definition of a cardinal. A set X has a *cardinal* which is a measure of size that applies to any set Y such that there is a one-to-one function f such that $f(X) = Y$ (see Jech (2002) 3.1). We denote the cardinal of a countably infinite set, *i.e.* the cardinal of the set of natural numbers, as $\aleph_0$, which in fact is the smallest infinite cardinal. $\aleph_1$ is the least cardinal greater than $\aleph_0$, which is equivalent to saying that $\aleph_1$ is the least uncountable cardinal. The cardinal of a set X, often called its *cardinality*, is written $|X|$. The only theorem we assume is $2^{\aleph_0} \geq \aleph_1$ due to Cantor (see (Dauben 1979) for example).

Remark. For infinite cardinals, there is a many-to-one relation between ordinals and cardinals, and any ordinal can be mapped to a cardinal by ignoring the well-ordering of the ordinal. There is a least ordinal that *corresponds* to, *i.e.* maps one-to-one onto, any given cardinal. For example, the least ordinal that corresponds to $\aleph_0$ is called ω, and the least ordinal that corresponds to $\aleph_1$ is called ω_1.

Definition of a cardinal enumeration. A *cardinal enumeration* of a set X is an enumeration of X in a well-ordering of the least ordinal that corresponds to the cardinal of X.

Remark. A cardinal enumeration is used in Proposition 6 as Proposition 6 is not true for longer enumerations than a cardinal enumeration (which is the shortest of all enumerations of X).

Definition of the number of bits of information. The *number of bits of information* in a real number is the length in bits of a binary sequence that cannot be compressed any further losslessly (see Vitanyi (2008) for example).[3] Here *lossless compression* (of a sequence of bits q to a sequence of bits p) means that p can be *encoded* from q where the length of p $|p| \leq |q|$ and q can be *decoded* from p, where the length of a binary sequence $|p|$ is the cardinal of the domain of p as function[4]. Lossless compression is *strict* if $|p| < |q|$. The *cardinal of the lossless compression of a sequence* p is denoted by $\rangle|p|\langle$, which is the greatest cardinal $c \leq |q|$ for all lossless compressions q of p. A set of binary sequences S can be *encoded* as a set of binary sequences T if every binary sequence in S can be mapped one-to-one to a binary sequence in T by a computable function e that is onto T, *i.e.* $e(S) = T$, and a binary sequence $s \in S$ is *encoded* as $e(s)$. S can be then *decoded* from T as $e^{-1}(T)$ and a binary sequence $t \in T$ can be *decoded* as $e^{-1}(t)$ if e^{-1} is a computable function. The *number of bits of information* in a set S of binary sequences can be defined as $|S| \times sup_{p \in S}(\rangle|p|\langle)$, where $\times$ is cardinal multiplication and $sup_{p \in S}(\rangle|p|\langle)$ is the least cardinal c such that $c \geq \rangle|p|\langle$ for all $p \in S$.[5]

Remark. The definition of number of bits in a set is a weak notion in the sense that the only limiting factor for lossless compression for infinite sets is that $|S| = |T|$ of infinite sets of binary sequences S and T provided that the members of S and T have length $< |S| (= |T|)$ because $c \times d = max(c, d)$ for cardinals c, d at least one of which is infinite, for $max(c, d)$ the maximum of c and d. However, since the argument in Proposition 2 only needs the cardinality restriction, stronger and more adequate notions of the number of bits will not be developed here. The suggested route for such a stronger notion is to code patterns and their number of repetitions as in the example below.

Example. Strict lossless compression on sets of sequences of bits exists, for example the set of all rational numbers expressed as infinite binary sequences. Any rational number corresponds to an initial finite sequence of bits[6], *init*, and a repetition of a finite binary sequence *seq* ω times; so we can losslessly compress a binary sequence representing a rational number by encoding *init*, *seq* and ω as a finite sequence of bits. We can represent the binary sequence $\langle 1, 0, 1 \rangle$ followed by $\langle 0, 1 \rangle$ repeated ω times as $\langle 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1 \rangle$, where 0 is used as an inter-bit marker for a sequence and an inter-bit 1 indicates a boundary to the next element of the code, whether to a finite sequence or to the code for the number of repetitions. For the number of repetitions, 1 indicates an infinite number of repetitions and 1 is the code for the ordinal exponential ω^1 (which $= \omega$ and should not be confused with ω_1, the first uncountable ordinal). Binary encodings of finite binary sequences and binary sequences that allow infinite repetitions for larger ordinals than ω using ordinal notations for infinite ordinals (see
(Rathjen 2006)) are clearly possible using the same encoding function (n 0s represent natural number n for example), but are not the subject of this paper.

Definition of a mathematical object. A mathematical object is taken to be a well-founded set definable in the cumulative hierarchy of pure sets, see (Shoenfield 1977) and (Jech 2002) 6.3. It is assumed in this paper that any mathematical object can be represented as a binary α-sequence for some ordinal α (which in general requires the Axiom of Choice).

3. Principles relating to the Continuum Hypothesis

We will start with CH itself written in logical notation:

$$\text{CH: } (\forall X \subseteq \mathbb{R})[(|X| \leq \aleph_0) \vee (|X| = |\mathbb{R}|)]$$

CH can also be formulated as $2^{\aleph_0} = \aleph_1$ because any uncountable set of real numbers, including any (set representing a) sequence of real numbers indexed by all countable ordinals (which has cardinality $\aleph_1$), must have the same cardinality as R.

CH can be expressed as follows as a statement about well-orderings of a set of real numbers (compare Koellner 2019, which allows well-orderings of order type $< \omega_2$):

$$\text{CH=: For all linear orderings of a set of real numbers, } X\text{, there is a well-ordering of } X \text{ of order type } \leq \omega_1.$$

Proposition 1. *CH= is equivalent to CH.*

Proof. Assume CH=. Since any set of real numbers can be well-ordered with order type $\leq \omega_1$, the cardinality of X, $|X|$, is $\leq \aleph_1$. The set of all real numbers, R, has cardinality $\aleph_1$ because it is uncountable by Cantor's theorem that $2^{\aleph_0} \geq \aleph_1$. It follows that every subset of the real numbers is countable or has the cardinality of R, which is CH. Conversely, assume CH. Then take any set of real numbers, X. By CH, if X is countable then it has cardinality $\leq \aleph_0$ and if X is uncountable it has cardinality $\aleph_1$ because by CH there is only one uncountable cardinality of any set of real numbers and that must be $\aleph_1$. Well-order X by applying the Axiom of Choice (AC), that is $x_\alpha := f(X - \bigcup_{\beta<\alpha}\{x_\beta\})$, where $0 \leq \alpha < \|X\|$ for choice function f that chooses a member of each set in a non-empty set of sets, where $\|X\| = |X|$ for finite X, $\|X\| = \gamma$ for $\omega \leq \gamma < \omega_1$ if X is countably infinite and $\|X\| = \omega_1$ if X is uncountable. The linear ordering of X is not used, but can be added as a premiss. Thus, CH follows. □

Proposition 2. *Each real number contains $\leq \omega$ bits of information, with almost all real numbers having exactly ω bits of information. All objects with a countable number of bits have $\leq \omega$ bits of information.*

Proof. Each real number contains $\leq \omega$ bits of information, with some (in fact all but countably infinitely many) real numbers having exactly ω bits of information, as otherwise there would be a lossless compression, *i.e.* a one-to-one and onto function, from the set of all real numbers to the set of natural numbers (where each natural number contains $< \aleph_0$ bits),[7] which would violate Cantor's theorem that $2^{\aleph_0} \geq \aleph_1 > \aleph_0$. Let us assume that x is an object with a countable number of bits of information. Then either x has a finite number of bits of information or x has countably infinitely many bits of information. In the first case, x can be encoded as a natural number and therefore as a real number. In the second case, there is a lossless compression of a binary α-sequence representation of x for $\omega \leq \alpha < \omega_1$ to a binary ω-sequence representation of x by definition of countability. Since a real number is identified with a binary ω-sequence, x is a real number. Seen in this way, a real number can be identified with a mathematical object with a countable number of bits. □

We can generalize CH as follows:

CH*: For all linear orderings of a set of mathematical objects which contain a countable number of bits of information, X, there is a well-ordering of X of order type $\leq \omega_1$.

Proposition 3. *CH* is equivalent to CH.*

Proof. This follows from Proposition 1 and Proposition 2. □

Remark. We hold CH* in reserve until the next section, but it will come in useful when we examine arguments for CH. We can compare CH with AC. AC says that there is a choice function that for a set of non-empty sets chooses a member of each set and collects them in a set. As we have seen in Proposition 1, repeated application of AC will generate a well-ordering of a non-empty set (known as the *well-ordering principle*). In particular, we have:[8]

Consequence of AC: For all linear orderings of a set of real numbers, X, there is a well-ordering of X.

Remark. Both AC and the well-ordering principle as applied to real numbers are a consequence of CH, because CH says that each member of a set of real numbers, X, can be indexed with a countable ordinal, which means that there is a method for choosing a member of any subset of X by taking the member with the least ordinal index (see Stillwell (2002)). At a minimum, we can say that CH is a choice principle that is as at least as strong as AC when applied to sets of real numbers. The fact that AC for sets in general follows from the Generalized Continuum Hypothesis is due to (Sierpiński 1947).

4. CH as a Uniform Infinite Binary Search

Definition of binary search. According to principle CH*, CH translates the countability of the number of bits in any member x of a linear ordering of a set of real numbers X to the countability of a (single) enumeration up to and including x in a well-ordering of X. One problem is that this form of CH does not correspond in logical form to a standard search algorithm such as *binary search*, which is a very efficient way to decide membership of a set of real numbers (linear in the length of the real numbers and logarithmic in the size of the set of real numbers, see Horowitz and Sahni 1978 for example for the finite case of binary search). Binary search of a set of real numbers, X, is the process where, given a real number to be searched for, x, a linear ordering $<$ of X is continually divided into two contiguous linear sub-orderings $A_{i+1} = \langle y \in X_i : y \leq a_i \rangle$ and $B_{i+1} = \langle y \in X_i : y > a_i \rangle$ for some $a_i \in X_i$ where $X_0 := X$ and $X_{i+1} := A_{i+1}$ if $x \leq a_i$ and $X_{i+1} := B_{i+1}$ if $x > a_i$ and i is a natural number index of the subdivision process. The process will stop if $x = a_i$ for some $i < \omega$, otherwise in the limit we have $X_\omega = \{x\}$ if $x \in X$ and $X_\omega = \varnothing$ if $x \notin X$.

Proposition 4. *We can write binary search in the form* $(\forall X \subseteq \mathrm{R})(\forall x \in X)(\exists F : \omega_1 \to X)(\exists \beta < \aleph_1)(F(\beta) = x)$ *for* R *the set of all real numbers and F is a function. CH is the stronger statement* $(\forall X \subseteq \mathrm{R})(\exists F : \omega_1 \to X)(\forall x \in X)(\exists \beta < \omega_1)(F(\beta) = x)$*, as in CH F does not depend on* x.[9]

Proof. We can allow $x \in X$ to be represented by a binary sequence of countably infinite length $\omega_1 > \beta \geq \omega$ rather than by a binary ω-sequence. Then we can adapt the infinite binary search algorithm outlined in the definition of binary search above by recursively choosing $a_i \in X_i$, setting $X_{i+1} := A_{\gamma+1}$ if $x \leq a_i$ and $X_{i+1} := B_{i+1}$ for ordinal $i < \beta$, $X_\lambda = \bigcap_{i<\lambda} X_i$ for limit ordinal λ, and setting $F(i) = a_i$ and $F(\gamma) = \varnothing$ for $i \neq \gamma < \omega_1$ if $i < \beta$ and $x = a_i$, otherwise setting $F(\beta) = x$ and $F(\gamma) = \varnothing$ for $\beta \neq \gamma < \omega_1$ (since $x \in X$, so the search will never fail). The statement of CH is a formalization of CH as a search algorithm. □

Remark. CH can thus be thought of as a *uniformization* condition on individual countable binary searches for $x \in X$ to produce a single countable search that can find every $x \in X$. Besides having a different logical form to binary search, it is possible that an enumeration of a set C of size $2^{\aleph_0}$ is such that every countable ordinal label for a real number is re-used $2^{\aleph_0}$ times or otherwise that almost all ordinal labels used for members of a well-ordering are $\geq \omega_1$. There is nothing in Zermelo Fraenkel set theory that prevents a mapping $2^{\aleph_0} \to \aleph_1$ from being many-to-one. In fact Cohen in Cohen (1963) showed that it is possible to force a mapping from $2^{\aleph_0} \to \aleph_1$ to be many-to-one in a countably infinite model of set theory by adding a countably infinite set of computably decidable conditions using a knowledge-based semantics (see Burgess (1977) for an accessible treatment, Kunen (1980) for a comprehensive account of ways of understanding forcing and Jech (2002) for reference). The knowledge-based semantics was set out in Kripke (1965) from Cohen (1963) and is based on the view that knowledge forms a tree (a partial ordering) of cumulative conditions where a condition and its negation will appear in separate branches.

Corollary 5. $\bigcap_{i<\omega_1} X_i = \varnothing$ *and* $\bigcap_{i<\beta} X_i = \{x\}$ *for any given countably infinite ordinal* β *and given* $x \in X$ *for uncountable set of real numbers X and* X_i *and* β *are as defined in Proposition 4, while* $\bigcap_{i<\omega} G_i = \varnothing$ *and* $\bigcap_{i<n} G_i = \{x\}$ *for G a non-empty set of finite binary sequences such that* $x \in G$ *has length m and* $n \geq m$ *for some natural number n,* $G_0 = G$ *and* G_{i+1} *represents a subdivision of* G_i.

Proof. The first part is a restatement of Proposition 4, while G can be searched using finite binary search once it has been ordered lexicographically. The construction of G_i follows X_i for finite ordinals with $G_0 = G$ and $G_{i \geq n} = \varnothing$. $n = m$ can be achieved if the midpoint, $mid_i = (s_i + f_i)/2$ in binary, of $G_i := [s_i, f_i]$, the set of all finite binary sequences between and including s_i and f_i, is chosen as a_i (which always exists for sets of binary sequences), where mid_i does not have to be member of G. Note that all binary sequences start with ordinal index 0.□

Remark. Corollary 5 shows that there may be an analogy between the cardinality of the set of all finite binary sequences, which is $\aleph_0$, and the finiteness of individual binary sequences and the cardinality of an uncountable set of real numbers and the countability of each real number. A similar analogy appears in the next section.

5. A Choice-Based Argument for CH

Definition of an interleaved enumeration. An enumeration of non-empty set X is interleaved one-to-one with an enumeration of a non-empty set Y if one member of X is chosen followed by a member of Y and the operation repeated until all members of X and Y have been chosen, the enumeration no longer alternating if $|X| < |Y|$ or $|Y| < |X|$.

Remark. The choice-based argument for CH below is based on an *analogy* between $\aleph_0$ and $\aleph_1$. That is, we know that to decide whether $x \in X$ for $X \subseteq \mathrm{N}$, where N is the set of natural numbers, requires no more than finitely many steps, and to find x by enumeration of X when interleaved one-to-one with an enumeration of the complement of X, $\mathrm{N} - X$, requires $< \omega$ steps. Replacing N by R, $\aleph_0$ by $\aleph_1$ and "finitely" by "countably many" we get: to decide whether $x \in X$ for $X \subseteq \mathrm{R}$ requires no more than countably many steps and to find x by enumeration of X when interleaved one-to-one with an enumeration of $\mathrm{R} - X$ requires $< \omega_1$ steps.

In order to translate "requires" into mathematical language, we restrict enumerations to cardinal enumerations.

Proposition 6. *CH is equivalent to the statement that any cardinal enumeration of any* $X \subseteq \mathrm{R}$ *to find any* $x \in \mathrm{R}$ *when interleaved one-to-one with an enumeration of* $\mathrm{R} - X$*, takes* $< \omega_1$ *steps.*

Proof. If CH, then since X and $\mathrm{R} - X$ can be linearly ordered by the lexicographical ordering, they can be enumerated in $\leq \omega_1$ steps as a single cardinal enumeration of R. Since either $x \in X$ or $x \in \mathrm{R} - X$ then x will be enumerated in $< \omega_1$ steps. Conversely, if $x \in X$ then x can be found by an enumeration of X in $< \omega_1$ steps by assumption, and if $x \in \mathrm{R} - X$ then x can be found by an enumeration of $\mathrm{R} - X$ in $< \omega_1$ steps by assumption. If X is empty, $\mathrm{R} - X$ can be enumerated in $\leq \omega_1$ steps since all $x \in R$ can be enumerated in $< \omega_1$ steps by assumption; if $\mathrm{R} - X$ is empty, X can be enumerated in $\leq \omega_1$ steps by the same argument; otherwise both X and $\mathrm{R} - X$ can be enumerated in $\leq \omega_1$ steps, again by the same argument. Since X is an arbitrary set of real numbers which is assumed to be linearly ordered, we have shown that X is well-ordered (by enumeration) with an order type $\leq \omega_1$. CH follows. □

Remark. While an analogy is a weak argument, there is a reason why the analogy may hold. That is, if CH is false then it follows that there would be *no* uniform method (such as enumeration) for deciding whether any $x \in X$ in countably many steps. Thus CH is *false* would imply that these countable decision computations of $x \in X$ could not be well-ordered in a way that any such computation is accessible in countably many steps, or, more starkly, that *almost all countable decision computations of* $x \in X$ *require uncountably many steps to complete if the set of decision computations is well-ordered* Given that CH is a strong choice function, and CH* applies to all mathematical objects with a countable number of bits of information, it is plausible to believe that a choice function could be selected to minimize the total number of steps in the uniform method (*i.e.* to $\leq \omega_1$ steps) and to avoid having almost all countable content being decided in uncountably many steps.

To emphasize this point consider the following principle:

CH*-: For all linear orderings of a set of mathematical objects which contain a *strictly increasing* countable number of bits of information, X, there is a well-ordering of X of order type $\leq \omega_1$.

Remark. CH*- is a consequence of AC since any strictly increasing linear order with a countable infinity of information can be mapped to a strictly increasing linear order of countable ordinals. CH* is stronger than CH*- because it is possible that at an uncountable limit ordinal the increasing number of bits becomes uncountable. Thus with CH* there is no natural way to map the countable content of real numbers to ordinals. The choice function in AC may provide such a mapping. In fact, we can say that CH* is really a claim that CH* is the same as CH*-. That is to say, not in thes sense of logical equivalence, but that CH* not only has a choice function to well-order any set of mathematical objects with a countably infinite number of bits of information, but that same choice function can also re-order the objects in an increasing countable number of bits. Thus CH is a natural strong choice principle (based on CH* and CH*-).

6. Conclusions

This paper concludes that CH is a very strong choice principle that is maximally efficient as a principle for deciding whether a real number is in a set of real numbers, in the sense that it is uniform in deciding membership for every real number in a countable number of steps. Moreover, if CH is false it follows that almost all membership decisions that require countably many bits of information are decided by enumeration in uncountably many steps. That this last assertion is counter-intuitive leads to CH being a reasonable principle to adopt. This is supported by the fact that CH reflects the analogy between the finiteness of computation of the number of steps to check membership of a set of natural numbers by (cardinal) enumeration with the countability of computation of the number of steps to check membership of a set of real numbers by (cardinal) enumeration.

Footnotes

[1] The number of enumerations (well-orderings) of any infinite set is uncountable, and thus the notion of an arbitrary enumeration of an infinite set cannot be specified in a finite way. Any enumeration of an uncountable set cannot be performed by a finitely computable function with finite inputs, because only a countable infinity of outputs will result, see Kleene (1938) for characterization of the first non-computable ordinal as a countable ordinal.

[2] This definition is a variant of the standard definition of an ordinal as an isomorphism class of a specific well-ordering. In formal set theory, since classes are larger than sets, it is usual to identify an ordinal with a specific well-ordered set, see Jech (2002) for example.

[3] is a text on algorithmic complexity, while the definition given here addresses the complexity of sequences and sets of sequences. The treatment of information here is also distinct from Shannon information, see Shannon (1948); Stone (2022), which concerns information used in a communication system.

[4] That is, $|p| = |S|$ for $p : S \to \{0, 1\}$ where $S \subseteq \mathbb{N}$. This definition can be extended to larger well-ordered sets than $\mathbb{N}$.

[5] There is a better definition of *number of bits of information* in a set S of binary sequences as the least number of bits in a binary sequence comprising a concatenation of all binary sequences $p \in S$ using the same compression algorithm for any set S of binary sequences. But it is harder to use than the definition in the main text because there is a length minimization operation over all possible concatenations of sequences of members of S, even if it can result in shorter lossless compressions.

[6] The initial sequence can contain repeated sub-sequences of bits, but has finite length.

[7] In terms of the definition of number of bits in a set we would have for set of all real numbers $\mathbb{R}$, $\aleph_0 \times 2^{\aleph_0} = \aleph_0 \times \aleph_0$, *i.e.* $2^{\aleph_0} = \aleph_0$, if all real numbers has finite information content as represented by the set of natural numbers $\mathbb{N}$, which contradicts Cantor's theorem.

[8] It should not be thought that the function that maps a linear ordering to a well-ordering will preserve the linear ordering. The choice function that operates on $b > a$ after a is chosen will in general select a different linear order of the set to form a well-ordering.

[9] The F used in binary search in the proof will have only one non-empty entry, while F used in CH is an enumeration of X of length $\leq \omega_1$.

References

- Burgess, J. P. (1977). “Forcing”. In: Handbook of Mathematical Logic. Ed. by J. Barwise. Vol. 90. Studies in Logic and the Foundations of Mathematics. North- Holland. Chap. B.4, pp. 403–452.
- Cohen, P. J. (1963). “The Independence of the Continuum Hypothesis”. In: Proceedings of the National Academy of Sciences of the United States of America 50.6, pp. 1143–1148.
- Dauben, J. W. (1979). Georg Cantor: His Mathematics and his Philosophy of the Infinite. Princeton University Press.
- Feferman, S. (2009). “Conceptions of the Continuum”. In: Intellectica The Mathematical Continuum. New Conceptions, New Challenges.61. Ed. by M. de Clas, pp. 168–190.
- Gödel, K. (1940). The Consistency of the Axiom of Choice and of the Generalized Continuum-Hypothesis with the Axioms of Set Theory. Annals of Mathematics Studies. Princeton University Press.
- Hallett, M. (1986). Cantorian Set Theory and Limitation of Size. Oxford Logic Guides. Clarendon Press.
- Halmos, P. R. (1974). Naive Set Theory. Undergraduate Texts in Mathematics. Springer-Verlag.
- Hausdorff, F. (1957). Set Theory. Translated by J.R. Aumann et. al. from Grundzüge der Mengenlehre, Veit, Leipzig, third edition 1937: Chelsea.

- Horowitz, E. and S. Sahni (1978). The Fundamentals of Algorithms. Computer Software Engineering Series. Computer Science Press.
- Jech, T. (2002). Set Theory: The Third Millenium Edition, Revised and Expanded. Springer.
- Kanamori, A. (1996). “The Mathematical Development of Set Theory from Cantor to Cohen”. In: Bulletin of Symbolic Logic 2.1, pp. 1–71.
- Kechris, A. S. (1995). Classical Descriptive Set Theory. Springer: Berlin.

  Kleene, S. C. (Dec. 1938). “On Notation for Ordinal Numbers”. In: Journal of Symbolic Logic 3.4, pp. 150–155.
- Koellner, Peter (2019). “The Continuum Hypothesis”. In: The Stanford Encyclopedia of Philosophy. Ed. by Edward N. Zalta. Spring 2019. Metaphysics Research Lab, Stanford University.
- Kripke, S. A. (1965). “Semantical Analysis of Intuitionistic Logic I”. In: Formal Systems and Recursive Functions. Ed. by J. N. Crossley and M. A. E. Dummett. Vol. 40. Studies in Logic and the Foundations of Mathematics. North-Holland, pp. 92–130.
- Kunen, K. (1980). Set Theory: An Introduction to the Independence Proofs. North- Holland.
- Li, M. and P. Vitanyi (2008). An Introduction to Kolmogorov Complexity and Its Applications. Third Edition. Springer: Berlin.
- Martin, D. A. (1977). “Descriptive set theory: Projective sets”. In: Handbook of Mathematical Logic. Ed. by J. Barwise. Vol. 90. Studies in Logic and the Foundations of Mathematics. North-Holland: Amsterdam. Chap. C.8, pp. 783–818.
- Martin, D. A. and R. M. Solovay (1970). “Internal Cohen Extensions”. In: Annals of Mathematical Logic 2.2, pp. 143–178.
- Moore, J. T. (2017). “What makes the continuum @2”. In: Foundations of Mathematics. Ed. by A. E. Caicedo and J. Cummings. American Mathematical Society, pp. 259–288.
- Rathjen, M. (2006). “The art of ordinal analysis”. In: Proceedings of the International Congress of Mathematicians. European Mathematical Society, pp. 45–69.
- Rittberg, C. (2015). “How Woodin changed his mind: new thoughts on the Continuum Hypothesis”. In: Archive of the History of the Exact Sciences 69.125-151. Schindler, R. and D. Asperó (May 2021). “Martin’s Maximum++ implies Woodin’s axiom”. In: Annals of Mathematics 192.3, pp. 793–835.
- Shannon, C. E. (1948). “A Mathematical Theory of Communication”. In: The Bell System Technical Journal 27, pp. 379–423.

  Shoenfield, J. R. (1977). “Axioms of Set Theory”. In: Handbook of Mathematical
- Logic. Ed. by J. Barwise. Vol. 89. Studies in Logic and the Foundations of Mathematics. Amsterdam: North-Holland, pp. 321–344.
- Sierpiński, W. F. (1934). Hypothèse du Continu. Vol. 4. Monografje Matematyczne. Seminarjum Matematyczne Uniwersytetu Warszawskiego.

  – (1947). “L’hypothèse généralisée du continu et l’axiome du choix”. In: Fundamenta Mathematicae 34.1-5.
- Stillwell, J. (Mar. 2002). “The Continuum Problem”. In: The American Mathematical Monthly 109.3, pp. 286–297.
- Stone, J. V. (2022). Information Theory: A Tutorial Introduction. Sebtel Press.
- Steprans, J. (2012). “History of the Continuum in the 20th Century”. In: Sets and Extensions in the Twentieth Century.

Vol. 6. Handbook of the History of Logic. Elsevier, pp. 73–144.