

AN ANALYSIS OF THE CONTINUUM HYPOTHESIS

ANDREW POWELL

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 a 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 CH is true or false and to use those models to support or reject the Continuum Hypothesis.

1. INTRODUCTION

This short paper analyses the Continuum Hypothesis (CH), 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 & Asperó (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 & Solovav (1970) 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 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. All of the other approaches mentioned above lead to axioms that are not provable from the standard axiomatization of the cumulative hierarchy of sets, Zermelo Fraenkel (ZF) set theory, see (Shoenfield

²⁰⁰⁰ Mathematics Subject Classification. 03E17.

Key words and phrases. Axiom of Choice, Continuum Hypothesis.

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

1977). 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* 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. Some Definitions

Definition. A set X is *linearly ordered* by *linear ordering* < if $(\forall x \in X)(\forall y \in X)(x < y \lor x = y \lor y > x)$, where $x \not\leq x, x < y \land y < z \rightarrow x < z$ for all x, y, z.

Definition. X is well-ordered by well-ordering < if it is linearly ordered by < and for all $Y \subseteq X$ ($\exists z \in Y$)($\forall y \in Y$)($z < y \lor z = y$).

Definition. Well-orders have an *order type* or *ordinal* which is the type of the isomorphism class of well-orderings <.

Definition. There is a natural *lexicographical* linear ordering on the real numbers given by $\langle x_{i < \omega} \rangle < \langle y_{i < \omega} \rangle$ if $(\exists k < \omega)[(\forall l < k)(x_l = y_l) \land (x_k < y_k)], \langle x_{i < \omega} \rangle = \langle y_{i < \omega} \rangle$ if $(\forall l < \omega)(x_l = y_l)$ and $\langle y_{i < \omega} \rangle < \langle x_{i < \omega} \rangle$ otherwise.

Definition. We can identify a real number as a binary ω -sequence, written as $\langle f_{i < \omega} \rangle$, that is to say a function $f : N \to 2$ where N is the type of the natural numbers, ω is the order type of the natural numbers in their standard strictly increasing ordering 0, 1, 2, ... and $2 := \{0, 1\}$.

Definition. A set of real numbers is identified with a binary tree, where a binary tree T comprises a set of branches or binary ω -sequences.

Definition. We denote the cardinality or size of a countable infinite set as \aleph_0 , and call \aleph_0 a *cardinal*, in fact 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 only theorem we assume is $2^{\aleph_0} \ge \aleph_1$ due to Cantor (see (Dauben 1979) for example).

¹The 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.

Definition. The number of bits of information in a real number is the length in bits of a binary sequence which cannot be compressed any further losslessly (see Li & Vitanyi (1997) for example). 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. 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 $e^{-1}(t)$. Since it is always possible to choose a short length code for a particular binary sequence, the encoding function should not be defined by cases but must act uniformly on each member of S.

Example. Lossless compression on sets of sequences of bits exist, for example the set of all rational numbers expressed as infinite binary sequences. Any rational number corresponds to an initial finite sequence, *init*, and a repetition of a finite binary sequence seq $0 \le \alpha \le \omega$ times; so we can losslessly compress a binary sequence representing a rational number by auto-encoding *init*, seq and α as a finite sequence of bits if α is sufficiently large. In case of rational numbers treated as binary ω -sequences, we take $\alpha = \omega$. For example, we can represent the binary sequence (1,0,1) followed by (0,1) repeated ω times as (1,0,0,0,1,1,0,0,1,1,1), 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 ω^1 (whereas natural number n would be represented by n 0s). Binary representations of finite binary sequences and of 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, but are not the subject of this paper.

3. Principles relating to the Continuum Hypothesis

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 $\langle \omega_2 \rangle$:

CH=: For all linear orderings of a set of real numbers, X, there is a well-ordering of X 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, $|X| \leq \aleph_1$. 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 . 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, 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 almost all 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 $\langle \omega \rangle$ bits), which would violate Cantor's theorem that $2^{\aleph_0} \geq \aleph_1$. 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:²

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 for sets of 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 minimum we can say that CH is a choice principle that is as at least as strong as AC. The fact that AC for sets in general follows from the Generalized Continuum Hypothesis is due to (Sierpiński 1947).

²It 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.

4. CH AS A UNIFORM INFINITE BINARY SEARCH

Definition. 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 & 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 $X_\omega = \emptyset$ if $x \notin X$.

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

Proof. We can allow $x \in X$ to be represented by a binary sequence of countably infinite length $\omega_1 > \beta \ge \omega$ rather than by a binary ω -sequence. Then we can adapt the infinite binary search algorithm outlined in the definition above by setting $X_{\lambda} = \bigcap_{i < \lambda} X_i$ for limit ordinal λ , choosing $a_i \in X_i$, setting $F(i) = a_i$ and $F(\gamma) = \emptyset$ and $X_{\gamma} = \emptyset$ for $i < \gamma < \omega_1$ if $i < \beta$ and $x = a_i$, otherwise setting $F(\beta) = x$ and $F(\gamma) = \emptyset$ and $X_{\gamma} = \emptyset$ for $\beta < \gamma < \omega_1$. 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 and Kunen (1980) for a comprehensive account of ways of understanding forcing). 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. $\bigcap_{i < \omega_1} X_i = \emptyset$ 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 $\bigcap_{i < \omega} G_i = \emptyset$ 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 $n \ge m$ 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 $G_{i \ge n} = \emptyset$. 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

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 $X \subseteq N$, 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, N - X, takes $< \omega$ steps. Replacing N by R, \aleph_0 by \aleph_1 and "finitely" by "countably many" we get: to decide whether $x \in X$ for $X \subseteq R$ requires no more than countably many steps and to find x by enumeration of X when interleaved one-to-one with an enumeration of X when interleaved one-to-one with an enumeration of X when interleaved one-to-one with an enumeration of R - X takes $< \omega_1$ steps.

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

Proof. If CH, then since X and X - R can be linearly ordered by the lexicographical ordering, they can be enumerated in $\leq \omega_1$ steps by a well-order. Since either $x \in X$ or $x \in R - X$ 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 $x \in R - X$ then x can be found by an enumeration of R - X in $< \omega_1$ steps by assumption. If X is empty, 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 R - X is empty, X can be enumerated in $\leq \omega_1$ steps by the same argument; otherwise both X and 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 7. While an analogy is a weak argument, there is 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 one 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, 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 a 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 counterintuitive 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 enumeration with the countability of computation of the number of steps to check membership of a set of real numbers by enumeration.

References

- Burgess, J. P. (1977), Forcing, in J. Barwise, ed., 'Handbook of Mathematical Logic', Vol. 90 of Studies in Logic and the Foundations of Mathematics, North-Holland, chapter B.4, pp. 403–452.
- Cohen, P. J. (1963), 'The Independence of the Continuum Hypothesis', Proceedings of the National Academy of Sciences of the United States of America 50(6), 1143– 1148.
- Dauben, J. W. (1979), Georg Cantor: His Mathematics and his Philosophy of the Infinite, Princeton University Press.
- 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.
- Hausdorff, F. (1957), *Set Theory*, Chelsea, Translated by J.R. Aumann et al from Grundzüge der Mengenlehre, Veit, Leipzig, third edition 1937.
- Horowitz, E. & Sahni, S. (1978), The Fundamentals of Algorithms, Computer Software Engineering Series, Computer Science Press.
- Kanamori, A. (1996), 'The Mathematical Development of Set Theory from Cantor to Cohen', Bulletin of Symbolic Logic 2(1), 1–71.
- Kechris, A. S. (1995), Classical Descriptive Set Theory, Springer: Berlin.
- Kleene, S. C. (1938), 'On notation for ordinal numbers', Journal of Symbolic Logic 3(4), 150–155.
- Koellner, P. (2019), The Continuum Hypothesis, in E. N. Zalta, ed., 'The Stanford Encyclopedia of Philosophy', Spring 2019 edn, Metaphysics Research Lab, Stanford University.
- Kripke, S. A. (1965), Semantical Analysis of Intuitionistic Logic I, in J. N. Crossley & M. A. E. Dummett, eds, 'Formal Systems and Recursive Functions', Vol. 40 of 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. & Vitanyi, P. (1997), An Introduction to Kolmogorov Complexity and Its Applications, Springer: Berlin.
- Martin, D. A. (1977), Descriptive set theory: Projective sets, in J. Barwise, ed., 'Handbook of Mathematical Logic', Vol. 90 of Studies in Logic and the Foundations of Mathematics, North-Holland: Amsterdam, chapter C.8, pp. 783–818.
- Martin, D. A. & Solovay, R. M. (1970), 'Internal Cohen Extensions', Annals of Mathematical Logic 2(2), 143–178.
- 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', Archive of the History of the Exact Sciences 69(125-151).
- Schindler, R. & Asperó, D. (2021), 'Martin's Maximum++ implies Woodin's axiom', Annals of Mathematics 192(3), 793–835.
- Shoenfield, J. R. (1977), Axioms of Set Theory, in J. Barwise, ed., 'Handbook of Mathematical Logic', Vol. 89 of Studies in Logic and the Foundations of Mathematics, North-Holland, Amsterdam, pp. 321–344.
- Sierpiński, W. F. (1934), Hypothèse du Continu, Vol. 4 of Monografje Matematyczne, Seminarjum Matematyczne Uniwersytetu Warszawskiego.
- Sierpiński, W. F. (1947), 'L'hypothèse généralisée du continu et l'axiome du choix', Fundamenta Mathematicae 34(1-5).
- Stillwell, J. (2002), 'The Continuum Problem', The American Mathematical Monthly 109(3), 286–297.
- Streprans, J. (2012), History of the Continuum in the 20th Century, in 'Sets and Extensions in the Twentieth Century', Vol. 6 of Handbook of the History of Logic, Elsevier, pp. 73–144.