

LSE

THE LONDON SCHOOL
OF ECONOMICS AND
POLITICAL SCIENCE ■

LSE Research Online

George Barmpalias and Andrew Lewis-Pye **Computing halting probabilities from other halting probabilities**

Article (Accepted version)
(Refereed)

Original citation:

Barmpalias, George and Lewis-Pye, Andrew (2016) Computing halting probabilities from other halting probabilities. Theoretical Computer Science . ISSN 0304-3975

Reuse of this item is permitted through licensing under the Creative Commons:

© 2016 Elsevier
CC-BY-NC-ND4.0

This version available at: <http://eprints.lse.ac.uk/68332/>
Available in LSE Research Online: November 2016

LSE has developed LSE Research Online so that users may access research output of the School. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. You may freely distribute the URL (<http://eprints.lse.ac.uk>) of the LSE Research Online website.

Computing halting probabilities from other halting probabilities *

George Barmpalias

Andrew Lewis-Pye

October 4, 2016

Abstract. The halting probability of a Turing machine is the probability that the machine will halt if it starts with a random stream written on its one-way input tape. When the machine is universal, this probability is referred to as Chaitin's omega number, and is the most well known example of a real which is random in the sense of Martin-Löf. Although omega numbers depend on the underlying universal Turing machine, they are robust in the sense that they all have the same Turing degree, namely the degree of the halting problem. This means that, given two universal prefix-free machines U, V , the halting probability Ω_U of U computes the halting probability Ω_V of V . If this computation uses at most the first $n + g(n)$ bits of Ω_U for the computation of the first n bits of Ω_V , we say that Ω_U computes Ω_V with redundancy g .

In this paper we give precise bounds on the redundancy growth rate that is generally required for the computation of an omega number from another omega number. We show that for each $\epsilon > 1$, any pair of omega numbers compute each other with redundancy $\epsilon \log n$. On the other hand, this is not true for $\epsilon = 1$. In fact, we show that for each omega number Ω_U there exists another omega number which is not computable from Ω_U with redundancy $\log n$. This latter result improves an older result of Frank Stephan.

George Barmpalias

State Key Lab of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China.
School of Mathematics, Statistics and Operations Research, Victoria University of Wellington, New Zealand.
E-mail: barmpalias@gmail.com. *Web:* <http://barmpalias.net>

Andrew Lewis-Pye

Department of Mathematics, Columbia House, London School of Economics, Houghton Street, London, WC2A 2AE, United Kingdom.

E-mail: A.Lewis7@lse.ac.uk. *Web:* <http://aemlewis.co.uk>

*Barmpalias was supported by the 1000 Talents Program for Young Scholars from the Chinese Government, grant no. D1101130. Additional support was received by the Chinese Academy of Sciences (CAS) and the Institute of Software of the CAS. Lewis-Pye was supported by a Royal Society University Research Fellowship.

1 Introduction

Consider the following experiment, involving a Turing machine with a one-way input tape. We turn on the machine, and whenever it tries to read the next bit from the input, we give to it a random digit. What is the probability that the machine will halt at some point? This is an experiment that Chaitin considered in [Cha75]. In the case of a universal machine he called the probability Ω and showed that it is algorithmically random, in the sense of Martin-Löf [ML66]. Chaitin originally considered Ω for self-delimiting machines, i.e. machines that operate on instantaneous code, without any out-of-band markers or special symbols that frame the words in the input tape. The cumulative work of Solovay [Sol75], Calude, Hertling, Khossainov and Wang [CHKW01] and Kučera and Slaman [KS01], has shown Chaitin's omega numbers do not depend significantly on many parameters of the universal machine. In particular, the series of papers above showed that a left-c.e. real (i.e. one which is the limit of a computable increasing sequence of rational numbers) is the halting probability of a universal self-delimiting machine if and only if it is Martin-Löf random (a good presentation of this work is given in [DH10, Chapter 9]).

There are many other results that witness the robustness of the halting probability and the similarity between different omega numbers. Solovay [Sol75], for example, showed that omega numbers are, in a specific sense, equally and maximally hard to approximate, compared to other left-c.e. reals. Calude and Nies observed in [CN97] that omega numbers are computable from each other, with computable bounds on the use of the oracle (i.e. computable bounds on the number of bits of the oracle tape required on each argument). On the other hand, a number of incompatibility results are known which distinguish the halting probabilities of different machines. Figueira, Stephan, and Wu [FSW06] showed, for example, that for each universal machine U with halting probability Ω_U there exists a universal machine V with halting probability Ω_V such that Ω_U and Ω_V have incomparable truth-table degrees. Frank Stephan (see [BDG10, Section 6] for a proof) showed that for each universal machine U there exists a universal machine V such that Ω_U cannot compute the first n bits of Ω_V using only the first $n + \mathbf{O}(1)$ bits of Ω_U as an oracle. Tadaki [Tad09] gave a very interesting quantitative characterization of the equivalence between the initial segments of Ω and the sets A_n of the strings of length n in the domain of the universal prefix-free machine.

Downey, Hirschfeldt Miller and Nies showed [DHMN05] that the Turing degree of Ω is not robust when the halting probability is relativized to an infinite oracle, even when two oracles differ at only a finite number of bits. Such strong negative results do not only apply to relativized versions of halting probabilities, but also to probabilities that concern more complicated properties of a universal machine than mere halting. This was demonstrated by Barmpalias and Dowe in [BD12], who studied the probability that a machine remains universal even when random bits are prefixed in the input tape. This is known as the *universality probability*, and it was shown that for different universal Turing machines the universality probabilities can have different Turing degrees. These negative results suggest that the apparent robustness of Ω stems from the fact that it is the probability of a relatively simple property, namely halting, which is Σ_1^0 . Indeed, there is only one Σ_1^0 Turing degree which contains Martin-Löf random numbers, namely the degree of the halting problem, but the same is not true for classes of higher arithmetical complexity.

In this paper we study the similarity of omega numbers in terms of the length of the initial segment of an omega number Ω_0 that is needed in order to compute the first n bits of another omega number Ω_1 .

Definition 1.1 (Redundancy). *If a real β computes a real α , and for each n the computation of the first n bits of α uses at most the first $\lfloor n + g(n) \rfloor$ bits of the oracle β , we say that β computes α with redundancy g .*

Our main result is a sharp estimation of the redundancy growth rate that is generally required for the computation of one omega number from another, in terms of logarithms. Throughout this paper we shall write $\log(n)$ in order to denote $\log_2(n)$, i.e. we always work base 2. It will also be convenient to agree to the convention that $\log(0) = 0$.

Definition 1.2. For $\epsilon \in \mathbb{R}$ with $\epsilon \geq 1$, we define $h_\epsilon(n) = \epsilon \cdot \log(n)$, and $h_\epsilon^*(n) = \log(n) + \epsilon \cdot \log \log(n)$.

Theorem 1.3. If $\epsilon > 1$ then every omega number is computable from any other omega number with redundancy h_ϵ . If $\epsilon = 1$ then given any omega number Ω there exists another omega number which is not computable from Ω with redundancy h_ϵ .

Our result extends an older result of Frank Stephan (see [BDG10, Section 6] for a proof) which says that two omega numbers do not always compute each other with constant redundancy. Our proof of Theorem 1.3 involves effective measure-theoretic tools like the effective Borel-Cantelli lemmas, effective martingales and other notions from algorithmic randomness. We review these notions in Section 2 and present our main argument in Section 3.1.

2 Preliminaries

Recall that the series $\sum_n n^{-\epsilon}$ converges if and only if $\epsilon > 1$. Recall also the Cauchy condensation series convergence criterion (e.g. see [B06]).

Lemma 2.1 (Condensation). *If $f : \mathbb{N} \rightarrow \mathbb{R}^+$ is nonincreasing, then the series $\sum_n f(n)$ converges if and only if the series $\sum_n (2^n \cdot f(2^n))$ converges.*

From these well known facts the following lemma immediately follows.

Lemma 2.2 (Convergence and divergence). *The sums $\sum_n 2^{-h_\epsilon(n)}$ and $\sum_n 2^{-h_\epsilon^*(n)}$ are finite if and only if $\epsilon > 1$.*

Background on algorithmic randomness that is relevant to our argument can be found in [DH10, Chapter 6]. This monograph also contains a presentation of the work in [Sol75]. We shall identify reals with their infinite binary expansions (the fact that dyadic rationals have two expansions will not cause issues). We shall generally work with reals in $[0, 1]$, so that the decimal point may be neglected and reals can be thought of simply as infinite binary sequences, i.e. elements of Cantor space. It will be convenient to adopt the (slightly unusual) convention that the bits of a real α are indexed from 1 rather than zero, so that $\alpha = \alpha(1)\alpha(2)\alpha(3)\dots$, rather than $\alpha(0)\alpha(1)\alpha(2)\dots$.

A real is Martin-Löf random if it avoids all effective statistical tests. This notion was introduced by Martin-Löf in [ML66]. We will make use of an essentially equivalent notion of statistical test due to Solovay [Sol75]: a Solovay test is a computable sequence of finite strings (σ_i) (each σ_i often being identified with the set of infinite binary sequences extending it, meaning that it may be regarded as a basic open subset of Cantor space) such that $\sum_i 2^{-|\sigma_i|}$ is bounded. We say that a real avoids this test if there are only finitely many i such that σ_i is a prefix of the binary expansion of the real. Solovay showed that a real is Martin-Löf random if and only if it avoids all Solovay tests. An equivalent definition of Martin-Löf randomness can be given in terms of betting strategies, which are often expressed as martingales. We shall think of martingales as functions $f : 2^{<\omega} \rightarrow \mathbb{R}^{\geq 0}$ with the property $f(\sigma 0) + f(\sigma 1) = 2 \cdot f(\sigma)$. A martingale f is computably enumerable (c.e.) if the values $f(\sigma)$ can be computably and uniformly approximated by rationals from

below, i.e. there exists a computable function $f^*(\sigma, i)$ taking rational values, which is nondecreasing in the second argument, and such that for all σ , $\lim_{i \rightarrow \infty} f^*(\sigma, i) = f(\sigma)$. We say that f succeeds on a real X if $\lim_n f(\alpha \upharpoonright_n) = \infty$. It is well known that a real X is Martin-Löf random if and only if no c.e. martingale succeeds on X . We let $\alpha \upharpoonright_n$ denote the first n bits of α . Given a real α , suppose that there exists a partial computable function p such that $p(\alpha \upharpoonright_n) \downarrow$ for infinitely many n , and such that whenever $p(\alpha \upharpoonright_n) \downarrow$ we have $p(\alpha \upharpoonright_n) = \alpha(n+1)$, i.e. p correctly predicts the next bit of α (recall our labelling convention above). In this case it is not hard to see that there exists a c.e. martingale which succeeds on α , so that α cannot be Martin-Löf random. This fact will be used in the proof of Theorem 1.3. A real is weakly 1-random if it is not a member of any null Π_1^0 class.

Finally, we state the effective Borell-Cantelli lemmas that are often used in order to derive statistical properties of algorithmically random numbers. Recall the basic fact from analysis that, given a sequence (b_i) of positive integers, we have:

$$\prod_i (1 - 2^{-b_i}) > 0 \iff \sum_i 2^{-b_i} < \infty. \quad (2.0.1)$$

This is a direct consequence of the fact that $\log(1+x) = x + \mathbf{O}(x^2)$ in a neighborhood of zero.

Given a finite set B of natural numbers, a string σ of length $|B|$ (i.e. the cardinality of B) and a real β , we may say that β meets σ on B if the following holds for all $n < |B|$: if m_n is the n th element of B we have $\beta(m_n) = \sigma(n)$. The same definition applies for the case when β is a string of length at least the largest element of B . Note that if the B_i are disjoint sets (and fixing the uniform probability measure), the events ‘ β meets σ_i on B_i ’ are independent. We can therefore state the effective Borel-Cantelli lemmas as follows.

Lemma 2.3 (Effective Borel-Cantelli lemmas). *Let (B_i) be a collection of pairwise disjoint sets, let $b_i = |B_i|$ for each i and suppose that (σ_i) is a sequence of strings with $|\sigma_i| = |B_i|$.*

1. *If $\sum_i 2^{-b_i} < \infty$ then the reals that meet σ_i on B_i for only finitely many i form a class of measure 1.*
2. *If $\sum_i 2^{-b_i} = \infty$ then the reals that meet σ_i on B_i for only finitely many i form a class of measure 0.*

Suppose the sequence (B_i) is computable. Then in the first case every Martin-Löf random real meets σ_i on B_i for only finitely many i , and in the second case every weakly 1-random real meets σ_i on B_i for infinitely many i .

The first clause is essentially just Solovay’s characterization of Martin-Löf randomness in terms of Solovay tests that we discussed above. For the sake of completeness we include a short proof of the second clause. Let $m_n = \max \cup_{i \leq n} B_i$. For a given n , the number of subsets of $\{0, \dots, m_n\}$, regarded as strings of length $m_n + 1$, which do not meet σ_i on B_i for any $i \leq n$ is:

$$2^{m_n+1 - \sum_{i \leq n} b_i} \cdot \prod_{i=0}^n (2^{b_i} - 1). \quad (2.0.2)$$

Since there are 2^{m_n+1} subsets of $\{0, \dots, m_n\}$, the measure of reals that do not meet any of the sets B_i , $i \leq n$ is exactly the expression in (2.0.2) divided by 2^{m_n+1} , i.e.

$$2^{-\sum_{i \leq n} b_i} \cdot \prod_{i=0}^n (2^{b_i} - 1) = \prod_{i=0}^n (1 - 2^{-b_i}).$$

By (2.0.1), the above quantity tends to zero if and only if the sum $\sum_i 2^{-b_i}$ diverges. For each finite set D , the sum $\sum_{i \notin D} 2^{-b_i}$ still diverges. So the argument above suffices to show that the reals which meet some B_i

with $i \notin D$ are of measure 1. Taking the intersection over all finite D , we get a countable intersection of sets of measure 1, which is therefore of measure 1. The effective version of the second clause follows since for each n , the set of reals which meet σ_i on B_i for at most n many i , forms a null Π_1^0 class.

The Borel-Cantelli lemmas were used by Chaitin in [Cha87] in order to establish the existence of certain blocks of zeros in the binary expansion of Ω . For example, it was shown that if g is computable and $\sum_n 2^{-g(n)}$ diverges, then for infinitely many n there exists a block of $n + g(n)$ zeros between digits 2^n and 2^{n+1} of the binary expansion of Ω .

3 Upper bounds on the oracle use in computations from omega numbers

We prove Theorem 1.3, along with some slightly more general statements. In Section 3.2 we consider the more general question of characterising the computable functions that are upper bounds on the oracle use in computations of one halting probability from another one.

3.1 Proof of Theorem 1.3

We start with the first part of Theorem 1.3, which relies on the approximation properties of omega numbers. The limits of increasing computable sequences of rational numbers are known as left computably enumerable (left-c.e.) reals, and can be viewed as the halting probabilities of (not necessarily universal) prefix-free machines.

Lemma 3.1 (Sufficient redundancy). *Suppose that g is a computable function such that $\sum_i 2^{-g(i)}$ converges. Given any two omega numbers, each is computable from the other with redundancy g .*

Proof. Let g be as in the statement, let Ω be an omega number and let α be a left-c.e. real. It suffices to show that α is computable from Ω with redundancy g . Let $(\alpha_s), (\Omega_s)$ be computable nondecreasing dyadic rational approximations that converge to α, Ω respectively. Recall that a Solovay test is a computable sequence of basic open intervals (σ_i) such that $\sum_i 2^{-|\sigma_i|}$ is bounded above. Since Ω is Martin-Löf random, it has only finitely many initial segments in any Solovay test (σ_i) . We construct a Solovay test as follows, along with a c.e. set I . At each stage $s + 1$ we consider the least $n \leq s$ such that $\alpha_s(n) \neq \alpha_{s+1}(n)$, if such exists. If such an n exists, we define $\sigma_s = \Omega_{s+1} \upharpoonright_{[n+g(n)]}$ and enumerate s into I . First let us verify that the set of strings $\sigma_s, s \in I$ is a Solovay test. Note that for every n , the number of stages s such that n is the least number with the property that $\alpha_s(n) \neq \alpha_{s+1}(n)$, is bounded above by the number of times that $\alpha_s(n)$ can change from 0 to 1 in the monotone approximation to α . Hence this number is bounded above by 2^{n-1} . So we have:

$$\sum_{s \in I} 2^{-|\sigma_s|} \leq \sum_n 2^n \cdot 2^{-g(n)-n} = \sum_n 2^{-g(n)} < \infty.$$

Since Ω is Martin-Löf random, there exists some s_0 such that for $s > s_0$ in I , σ_s is not an initial segment of Ω . This means that whenever our construction enumerates s in I because we find some least n with $\alpha_s(n) \neq \alpha_{s+1}(n)$, there exists some later stage where the approximation to $\Omega \upharpoonright_{[n+g(n)]}$ changes. So with oracle $\Omega \upharpoonright_{s+g(s)}$ we can uniformly compute $\alpha(n)$, and α is computable from Ω with redundancy g . \square

The reader may note that the above proof establishes a slightly more general statement, regarding the computation of any left-c.e. real from an omega number. The second part of Theorem 1.3 is also established slightly more generally than stated, as the following lemma indicates. For this proof recall that, by Demuth [Dem75], the sum of a Martin-Löf random left-c.e. real and any other left-c.e. real is Martin-Löf random. Since the halting probabilities of universal prefix-free machines are exactly the Martin-Löf random left-c.e. reals, it follows that the sum of an omega number and any left-c.e. real is an omega number.

Lemma 3.2 (Insufficient redundancy). *Let g be a computable nondecreasing function and let (t_i) be a computable increasing sequence such that $t_i + g(t_i) < t_{i+1}$ for all sufficiently large i and:*

$$\sum_i 2^{-g(t_i)} = \infty \quad \text{and} \quad \sum_i 2^{t_i - t_{i+1}} < \infty. \quad (3.1.1)$$

Then given any omega number Ω there exists another omega number which is not computable from Ω with redundancy g .

Proof. We will show that for some constant c the following number has the required property:

$$\beta = \Omega + \sum_{i>c} 2^{-(t_i + \lfloor g(t_i) \rfloor + 1)}. \quad (3.1.2)$$

First, note that β as defined above is an omega number, since it is the sum of an omega number and a computable real. Consider the intervals of positions $I_k = [t_k, t_k + \lfloor g(t_k) \rfloor]$ and $J_k = [t_k + \lfloor g(t_k) \rfloor + 2, t_{k+1} + \lfloor g(t_k) \rfloor + 1]$. Given a real number X , we are interested in those k such that:

- (a)_k the binary digits of X at all positions in the interval I_k are 1.
- (b)_k some digit of X in the interval J_k is zero.

The properties (a)_k and (b)_k are effective, in the sense that the set of reals satisfying them is a finite union of basic open sets, which are uniformly computable in k . Note that, since $t_k + g(t_k) < t_{k+1}$ for all sufficiently large k , the properties (a)_k are independent¹ for all sufficiently large k . Since g is nondecreasing, the same is true of the properties (b)_k. The measure of reals that meet property (a)_k is $2^{-\lfloor g(t_k) \rfloor - 1}$. Also, the measure of reals that do not meet property (b)_k is $2^{t_k - t_{k+1}}$. Hence, by the effective Borel-Cantelli lemma:

For any Martin-Löf random real there exist infinitely many k such that (a)_k holds and finitely many k such that (b)_k does not hold. (3.1.3)

Now, given Ω , let c be a number such that for all $k \geq c$, $t_k + g(t_k) < t_{k+1}$ and the property (b)_k is met by Ω . Let β be defined as in (3.1.2) for that value of c . Define $d_k = t_k + \lfloor g(t_k) \rfloor + 1$. Let us say that k is *valid* if it is larger than c and (a)_k holds for Ω . Then the following holds:

$$\text{If } k \text{ is valid then } \Omega(d_k) = 1 \iff \beta(t_k) = 0. \quad (3.1.4)$$

In order to see this, note first that satisfaction of (b)_{k'} for all $k' \geq k$ (where $k > c$) means that β agrees with $\Omega + 2^{-d_k}$ on all digits in the interval

$$[t_{k-1} + \lfloor g(t_{k-1}) \rfloor + 2, t_k + \lfloor g(t_k) \rfloor + 1).$$

¹as events in the probability space of all reals, where the event corresponding to the property is the set of all reals that satisfy this property.

First suppose that $\Omega(d_k) = 0$. In this case, adding 2^{-d_k} to Ω (as one term in the sum $\sum_{i>c} 2^{-(t_i+\lfloor g(t_i)\rfloor+1)}$) will cause it to change at position d_k but leave it unchanged at position t_k , meaning that $\beta(t_k) = 1$. Suppose, on the other hand that $\Omega(d_k) = 1$. Let j be the greatest $\leq d_k$ such that $\Omega(j) = 0$, so that $j \in [t_{k-1} + \lfloor g(t_{k-1}) \rfloor + 2, t_k - 1]$ because $(a)_k$ is satisfied as well as $(b)_{k-1}$. The addition of 2^{-d_k} to Ω will cause the digit at position j to become 1, while making the digit at position t_k into a 0. Thus $\beta(t_k) = 0$ in this case.

If Ω computes β with redundancy g , then for each k , computing $\beta(t_k)$ uses at most the first $\lfloor t_k + g(t_k) \rfloor$ bits of Ω . Then (3.1.4) establishes that for the special case where k is valid, the first $\lfloor t_k + g(t_k) \rfloor$ bits of Ω are enough to decide $\Omega(t_k + \lfloor g(t_k) \rfloor + 1)$. This shows that there is a partial computable prediction rule for the digits of Ω . In other words, there is a c.e. martingale that succeeds on Ω , contradicting the fact that Ω is Martin-Löf random. \square

It remains to show that a sequence (t_i) as in the hypothesis of Lemma 3.2 exists for the function $\log(n)$.

Lemma 3.3 (Existence of partition). *If $g(n) = \log(n)$, there exists a computable increasing sequence (t_i) such that $t_i + g(t_i) < t_{i+1}$ for all sufficiently large i and such that (3.1.1) holds.*

Proof. For $k \geq 1$ define:

$$t_k = \sum_{i=1}^k (\log(i) + 2 \log \log(i)).$$

Then $t_{k+1} - t_k = \log(k+1) + 2 \log \log(k+1)$ so the second clause of (3.1.1) holds by Lemma 2.2. Next we show that for all sufficiently large k , $t_k + g(t_k) < t_{k+1}$. Since $\log(i) + 2 \cdot \log \log(i) \leq 2 \cdot \log(i)$ we have:

$$t_k \leq 2 \cdot \sum_{i \leq k} \log(i) = 2 \cdot \log((k)!) \leq 2k \cdot \log(k).$$

Hence:

$$g(t_k) \leq g(2k \cdot \log(k)) = 1 + \log(k) + \log \log(k). \quad (3.1.5)$$

For all sufficiently large k the last expression is bounded above by $\log(k+1) + 2 \cdot \log \log(k+1)$. Hence $g(t_k) < t_{k+1} - t_k$ for all sufficiently large k , as promised. Moreover, by (3.1.5) and Lemma 2.2, the first clause of (3.1.1) holds for the sequence (t_i) , which concludes the proof of this lemma. \square

These lemmas conclude the proof of Theorem 1.3.

3.2 Computable functions as upper bounds of oracle use of omega

Theorem 1.3 gives a rather precise picture of the rate of growth of the oracle use in computations of one halting probability from another. It is reasonable to ask if we can obtain a more general characterisation of the upper bounds on the oracle use in such computations. Lemma 3.1, for example, suggests that this might be possible. Any computable function g such that $\sum_i 2^{-g(i)}$ converges is such an upper bound. Could this condition characterise these upper bounds? In other words, is it true that if $\sum_i 2^{-g(i)}$ diverges then there are two omega numbers such that one is not computable from the other with redundancy g ? If for all computable g such that $\sum_i 2^{-g(i)}$ diverges, there existed a sequence (t_i) satisfying the conditions described in Lemma 3.2, a positive answer would follow. The following proposition establishes that this is not the case, even if g is assumed to be monotone.

Proposition 3.4. *There exists a nondecreasing computable function g such that $\sum_i 2^{-g(i)} = \infty$ and the following holds for all increasing sequences of positive integers (t_i) :*

$$\sum_i 2^{-g(t_i)} = \infty \Rightarrow \sum_i 2^{t_i - t_{i+1}} = \infty. \quad (3.2.1)$$

For the proof of Proposition 3.4, we construct g of the form $\log(f(n))$. Let $m_i = 2^{2^i}$ and define $f(n) = m_1$ for m_1 many values of n (i.e. the interval $[1, m_1]$), then $f(n) = m_2$ for the next m_2 values of n , and so on. This determines f and g , so it remains to show that g has the desired property. Define the intervals $I_n = \{i \mid f(i) = m_n\}$ and note that by the definition of f we have $|I_n| = m_n$. Moreover, these intervals are a partition of \mathbb{N} . In order to understand the intuition behind the definition of f , imagine momentarily that the sequence (m_i) has not yet been specified, and let f be defined as above with respect to some sequence (m_i) which is yet to be determined. Through various considerations we shall arrive at the specific definition of (m_i) given previously, along with a proof that this particular choice confers the desired properties on f . Since $g(n) = \log(f(n))$, if $f(n) = m$, this will contribute $1/m$ to the sum $\sum_n 2^{-g(n)}$. So those values of n for which $f(n) = m_1$ contribute (in total) 1 to the sum $\sum_n 2^{-g(n)}$. Then those values of n for which $f(n) = m_2$ contribute the same amount again, and so on. This ensures that $\sum_n 2^{-g(n)}$ is infinite, for any choice of (m_i) . So it remains to specify (m_i) so that (3.2.1) is met.

Given any increasing sequence (t_n) such that $\sum_n 2^{-g(t_n)} = \infty$, we wish to show that $\sum_n 2^{t_n - t_{n+1}} = \infty$. For each n , consider the set $J_n(t) = \{i \mid t_i \in I_n\}$, (where the suffix (t) indicates the dependence on (t_i)). Since $|I_n| = m_n$ we have:

$$\sum_i 2^{-g(t_i)} = \sum_i \frac{1}{f(t_i)} = \sum_n \frac{|J_n(t)|}{m_n} = \sum_n \frac{|J_n(t)|}{|I_n|}.$$

Since we are given that $\sum_i 2^{-g(t_i)} = \infty$, it follows that there are infinitely many n with $|J_n(t)| > |I_n| \cdot 2^{-n}$. Let $D(t)$ be the set of such n , where once again the suffix (t) indicates the dependence on (t_i) , i.e. $D(t) = \{n \mid |J_n(t)| > |I_n| \cdot 2^{-n}\}$. We aim to show that, so long as we specify the sequence (m_i) appropriately:

$$\text{if } n \in D(t) \quad \text{then} \quad \sum_{i \in J_n(t)} 2^{t_i - t_{i+1}} \geq 2^{-2}. \quad (3.2.2)$$

Since $\sum_i 2^{-g(t_i)} = \infty$ implies that $D(t)$ is infinite, this suffices to give the result because:

$$\sum_i 2^{t_i - t_{i+1}} \geq \sum_{n \in D(t)} \left(\sum_{i \in J_n(t)} 2^{t_i - t_{i+1}} \right). \quad (3.2.3)$$

The rough idea is that, for an adversary who wishes to keep the sum in (3.2.2) small, the optimal approach is to ensure that the terms t_i , $i \in J_n(t)$ are spaced evenly in I_n . This rough idea is formalised in the following lemma.

Lemma 3.5 (Minimizing the sums). *Let I be an interval, $k > 1$, and suppose that t_i , $1 \leq i \leq k + 1$ is an increasing sequence of numbers in I . Then $\sum_{1 \leq i \leq k} 2^{-(t_{i+1} - t_i)} \geq k \cdot 2^{-\lceil |I|/k \rceil} \geq k \cdot 2^{-|I|/k - 1}$.*

Proof. The second inequality above is obvious, so we only need to prove the first one. Let us consider the t_i as movable markers. We can assume that the first marker t_1 is placed on the first element of the interval I , and that t_{k+1} is placed on the last element of the interval, since otherwise they can be moved there reducing the sum $\sum_{1 \leq i \leq k} 2^{-(t_{i+1} - t_i)}$. Let $c_i = t_{i+1} - t_i$ and let $m = t_{k+1} - t_1$, so that $\sum_{i=1}^k c_i = m$. Consider \prod_k^m , which

is the set of all sequences a_1, a_2, \dots, a_k such that every $a_i \in \mathbb{N}^+$, and $\sum_{i=1}^k a_i = m$. The result follows if we can establish that amongst all sequences in Π_k^m , the minimum value of $\sum_i 2^{-a_i}$ is attained whenever $a_i \in \{\lfloor m/k \rfloor, \lceil m/k \rceil\}$ for all i . We show this by induction on $m \geq k$. For $m = k$ the result follows easily, since we must have $a_i = 1$ for all i . Suppose the result holds for m . Let $\hat{\Pi}_k^m$ be all those sequences in Π_k^m such that $a_i \in \{\lfloor m/k \rfloor, \lceil m/k \rceil\}$ for all i . It is clear that for all sequences in $\hat{\Pi}_k^m$ the sum $\sum_i 2^{-a_i}$ is the same (and similarly for $\hat{\Pi}_k^{m+1}$). Now suppose there exist two sequences (a_i) and (b_i) in Π_k^{m+1} such that $(a_i) \in \hat{\Pi}_k^{m+1}$, $(b_i) \notin \hat{\Pi}_k^{m+1}$ and for which $\sum_i 2^{-b_i} < \sum_i 2^{-a_i}$. Let c be such that b_c is largest, and let d be such that a_d is largest. Then we have $b_c \geq a_d$. Let (a_i^*) be the element of $\hat{\Pi}_k^m$ obtained by replacing a_d by $a_d - 1$. Let (b_i^*) be the element of Π_k^m obtained by replacing b_c by $b_c - 1$. Then we have $\sum_i 2^{-b_i^*} < \sum_i 2^{-a_i^*}$, contradicting the induction hypothesis. \square

Since $|I_n| = m_n$ and $|J_n(t)| \geq 2^{-n} \cdot |I_n|$ for each $n \in D(t)$, by Lemma 3.5 we have that for each $n \in D(t)$,

$$\sum_{i \in J_n(t)} 2^{t_i - t_{i+1}} \geq (|J_n| - 1) \cdot 2^{-|I_n|/|J_n(t)| - 1} \geq (2^{-n} \cdot m_n - 1) \cdot 2^{-2^n - 1} \geq (m_n - 1) \cdot 2^{-2^n - n - 1}. \quad (3.2.4)$$

So if we define $m_n = 2^{2^n + n}$ (as previously), we get the required inequality (3.2.2). We summarize the argument. We already noted that for any choice of m_i , the corresponding function g satisfies $\sum_n 2^{-g(n)} = \infty$. Now fix $m_i = 2^{2^i + i}$ and assume that $\sum_i 2^{-g(t_i)} = \infty$ for some increasing sequence (t_i) . By Lemma 3.5 we get (3.2.4). So by (3.2.3) we have that $\sum_i 2^{t_i - t_{i+1}} = \infty$ which concludes the proof.

4 Concluding remarks

We have characterised the redundancy growth rate which is generally required in computations of halting probabilities from other halting probabilities, in terms of the functions $h_\epsilon(n)$. It would be pleasing to obtain a more general characterisation of the required redundancy in such computations, in terms of arbitrary computable nondecreasing functions g such that $\sum_n 2^{-g(n)}$ converges. Although our analysis applies to this generalised goal with respect to the upper bounds that we obtain (Lemma 3.1), Proposition 3.4 indicates that our lower bound analysis (Lemma 3.2) may not be sufficient for such a generalisation.

References

- [B06] Daniel D. Bonar and Michael J. Khoury Jr. . *Real Infinite Series*. Classroom resource materials. Mathematical Association of America, USA, 2006.
- [BD12] George Barmpalias and David L. Dowe. Universality probability of a prefix-free machine. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 370(1971):3488–3511, 2012.
- [BDG10] George Barmpalias, Rodney Downey, and Noam Greenberg. Working with strong reducibilities above totally ω -c.e. and array computable degrees. *Transactions of the American Mathematical Society*, 362(2):777–813, 2010.
- [Cha75] Gregory J. Chaitin. A theory of program size formally identical to information theory. *J. Assoc. Comput. Mach.*, 22:329–340, 1975.

- [Cha87] Gregory J. Chaitin. Incompleteness theorems for random reals. *Advances in Applied Mathematics*, 8:119–146, 1987.
- [CHKW01] Christian. Calude, Peter. Hertling, Bakhadyr Khossainov, and Yongge Wang. Recursively enumerable reals and Chaitin Ω numbers. *Theoret. Comput. Sci.*, 255(1-2):125–149, 2001.
- [CN97] Cristian Calude and André Nies. Chaitin Ω numbers and strong reducibilities. *J.UCS*, 3(11):1162–1166, 1997.
- [Dem75] Oswald Demuth. On constructive pseudonumbers. *Comment. Math. Univ. Carolin.*, 16(2):315–331, 1975. In Russian.
- [DH10] Rod G. Downey and Denis Hirshfeldt. *Algorithmic Randomness and Complexity*. Springer, 2010.
- [DHMN05] Rod Downey, Denis R. Hirschfeldt, Joseph S. Miller, and André Nies. Relativizing Chaitin’s halting probability. *J. Math. Log.*, 5(2):167–192, 2005.
- [FSW06] Santiago Figueira, Frank Stephan, and Guohua Wu. Randomness and universal machines. *J. Complexity*, 22(6):738–751, 2006.
- [KS01] Antonín Kučera and Theodore Slaman. Randomness and recursive enumerability. *SIAM J. Comput.*, 31(1):199–211, 2001.
- [ML66] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.
- [Sol75] Robert Solovay. Handwritten manuscript related to Chaitin’s work. IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 215 pages, 1975.
- [Tad09] Kohtaro Tadaki. Chaitin Ω numbers and halting problems. In *Proceedings of the 5th Conference on Computability in Europe: Mathematical Theory and Computational Practice*, CiE ’09, pages 447–456, Berlin, Heidelberg, 2009. Springer-Verlag.