Electronic Notes in Theoretical Computer Science 66 No. 1 (2002)
URL: http://www.elsevier.nl/locate/entcs/volume66.html 17 pages

Trivial Reals

Rod G. Downey [1]

School of Mathematical and Computing Sciences
Victoria University of Wellington
New Zealand

Denis R. Hirschfeldt

Department of Mathematics
University of Chicago
U.S.A.

André Nies

Department of Computer Science
Auckland University
New Zealand

Frank Stephan [2]

Mathematical Institute
University of Heidelberg
Germany

Abstract

Solovay showed that there are noncomputable reals α such that $H(\alpha \upharpoonright n) \leqslant H(1^n) + O(1)$, where H is prefix-free Kolmogorov complexity. Such H-*trivial* reals are interesting due to the connection between algorithmic complexity and effective randomness. We give a new, easier construction of an H-trivial real. We also analyze various computability-theoretic properties of the H-trivial reals, showing for example that no H-trivial real can compute the halting problem (which means that our construction of an H-trivial computably enumerable set is a particularly easy, injury-free construction of an incomplete c.e. set). Finally, we relate the H-trivials to other classes of "highly nonrandom" reals that have been previously studied.

[1] Supported by the Marsden fund of New Zealand.
[2] Supported by the Heisenberg program of the Deutsche Forschungsgemeinschaft (DFG), grant no. Ste 967/1–1.

1 Introduction

Our concern is the relationship between the intrinsic computational complexity of a real and the intrinsic randomness of the real. In [11,12], together with LaForte, we looked at ways of understanding the intrinsic randomness of reals by measuring their relative initial segment complexity. (In this paper, "random" will always mean "1-random"; see Section 2 for basic definitions.) Thus, for instance, if α and β are reals (in $(0,1)$), given as binary sequences, then we can compare the complexities of α and β by studying notions of reducibility based on relative initial segment complexity. For example, we define $\alpha \leqslant_K \beta$ if $K(\alpha \restriction n) \leqslant K(\beta \restriction n) + O(1)$, where we will be denoting classical Kolmogorov complexity by K. For prefix-free Kolmogorov complexity H, we define $\alpha \leqslant_H \beta$ analogously.

The goal of the papers [11,12] was to look at the structure of reducibilities like the above, and interrelationships among them, as a way of addressing questions such as: How random is a real? Given two reals, which is more random? If we partition reals into equivalence classes of reals of the "same degrees of randomness", what does the resulting structure look like?

The classic example of a random real is the halting probability of a universal prefix-free machine M, Chaitin's $\Omega = \sum_{\sigma \in \mathrm{dom}(M)} 2^{-|\sigma|}$. It is well-known that Ω has the property that $\alpha \leqslant_H \Omega$ for all reals α.

A natural question to ask is the following: Given reals $\alpha \leqslant_Q \beta$ (for $Q \in \{H, K\}$), what can be said about the computational complexity of α and β measured relative to, say, Turing reducibility?

For example, if we restrict our attention to computably enumerable (c.e.) reals (ones whose left cuts are computably enumerable), then being H-complete like Ω implies that the real is Turing complete. A natural guess would be that for all reals, if $\alpha \leqslant_Q \beta$ then $\alpha \leqslant_T \beta$. However, this is not true in general.

The present paper is concerned with "trivial reals". These are reals whose complexity is "low" or trivial from the point of view of randomness, in the sense that such reals resemble computable reals like 1^ω.

Building on work of Loveland [29], Chaitin proved that if α is a real with $K(\alpha \restriction n) \leqslant K(1^n) + O(1)$ then α is computable. That is, if in terms of its Kolmogorov complexity, α looks like 1^ω, then it must be trivial computationally. What about the prefix-free version? Chaitin also proved that if a real α has the property that $H(\alpha \restriction n) \leqslant H(1^n) + O(1)$ then α is Δ^0_2. He asked if this could be improved to say that α must be computable.

It is a remarkable result that one *cannot* so improve this: Solovay [35] proved that there are Δ^0_2 noncomputable reals β such that $H(\beta \restriction n) \leqslant H(1^n) + O(1)$. Solovay's proof is in an unpublished manuscript, and is long and difficult. All known proofs of Solovay's theorem use variations of his technique.

In Section 3 we will give a new, short and easy proof of a strengthening of

Solovay's result that such noncomputable "H-trivial reals" exist. To state an extension of this result, we need another triviality notion.

Answering a question of Kučera and of van Lambalgen, Kučera and Terwijn [22] constructed a set X which is low for random. Here we say that X is low for random (also known as Martin-Löf-low) iff the collection of sets random relative to X is exactly the collection of random sets. It is possible to modify the construction given in Section 3 to show that there exist noncomputable computably enumerable sets that are both H-trivial and low for random.

H-triviality is surely a remarkable phenomenon. The remainder of the present paper is devoted to exploring this concept.

We prove that no H-trivial set can be Turing complete, and indeed every H-trivial set has array non-computable (anc) degree, where a degree is anc if it contains one of the array non-computable sets of Downey, Jockusch and Stob [13,14] (see Section 6 for a definition). This means that the construction of a noncomputable H-trivial real provides a very simple (one line, essentially) injury-free solution to Post's problem.

In an unpublished report, Zambella [40] proved that there is a computable function f such that for each c there are at most $f(c)$ many reals α with

$$H(\alpha \upharpoonright n) \leqslant H(1^n) + c.$$

No proof of Zambella's theorem has appeared in print. We will give a proof of this result.

The reducibility $\leqslant_H$ is a preordering and hence we can form a degree structure from it, the H-degrees. The resulting degree structure on the c.e. reals has as its join operation ordinary addition. That is, $[\alpha] \vee [\beta] = [\alpha + \beta]$, where $[\alpha]$ is the H-degree of α. The H-trivial reals form the least H-degree.

The notion of triviality seems intimately related to weak truth table reducibility. Recall that $A \leqslant_{wtt} B$ iff there is a Turing procedure Φ and a computable function φ such that $\Phi^B = A$ and for all x the maximum number queried of B on input x is bounded by $\varphi(x)$. We prove that the H-trivial reals form an ideal in the *wtt*-degrees.

Related to the topic of H-triviality is work of Kummer [24]. Kummer investigated "Kummer trivial" computably enumerable sets. In terms of classical (non-prefix free) Kolmogorov complexity, we know that if A is a computably enumerable set then $K(A \upharpoonright n) \leqslant 2\log n + O(1)$ for all n. Kummer constructed computably enumerable sets A and constants c such that, infinitely often, $K(A \upharpoonright n) \geqslant 2\log n - c$. He called such sets *complex*. Kummer also showed that the computably enumerable degrees exhibit a gap phenomenon. Namely, either a degree $\mathbf{a}$ contains a complex set A, or all c.e. $A \in \mathbf{a}$ are "Kummer trivial" in the sense that $K(A \upharpoonright n) \leqslant (1+\epsilon)\log n + O(1)$ for all $\epsilon > 0$. (By Chaitin's work, if $K(A \upharpoonright n) \leqslant \log n + O(1)$ then A is computable, so this result is sharp.) Kummer proved that the degrees containing such complicated sets are exactly the anc degrees. We prove that (i) not every array-noncomputable computably enumerable set is H-trivial, and (ii) there exist Turing degrees containing only Kummer trivial sets which contain no H-trivial sets. The result (ii) implies that being Kummer trivial does not make a set H-trivial.

2 Basic Definitions

Our notation is standard, except that we follow the tradition of using H for prefix-free complexity and K for non-prefix-free complexity. Our computability-theoretic notation follows Soare [33].

We work with reals between 0 and 1, identifying a real with its binary expansion, and hence with the set of natural numbers whose characteristic function is the same as that expansion. A real α is c.e. if its left cut is c.e. as a set, or equivalently, if α is the limit of a computable increasing sequence of rationals.

We work with machines with input and output alphabets $\{0,1\}$. A machine M is *prefix-free* (or *self-delimiting*) if, for all finite binary strings σ and $\tau \subsetneq \tau'$, we have $M^\sigma(\tau)\downarrow \Rightarrow M^\sigma(\tau')\uparrow$, where M^σ means that M uses σ as an oracle. It is *universal* if for each prefix-free machine N there is a constant c such that, for all binary strings σ and τ, if $N^\sigma(\tau)\downarrow$ then $M^\sigma(\mu)\downarrow = N^\sigma(\tau)$ for some μ with $|\mu| \leqslant |\tau| + c$. We call c the *coding constant* of N.

The prefix-free complexity $H(\tau)$ of a binary string τ is the length of the shortest binary string σ such that $M(\sigma)\downarrow = \tau$ for a fixed universal prefix-free machine M. (The choice of M does not affect the prefix-free complexity, up to a constant additive factor.) For a natural number n, we write $H(n)$ for $H(1^n)$. A real α is *random*, or more precisely, 1-random, if $H(\alpha \upharpoonright n) \geqslant n - O(1)$.

An important tool in building prefix-free machines is the Kraft-Chaitin Theorem.

Theorem 2.1 (Kraft-Chaitin) *From a c.e. sequence of pairs $(\langle n_i, \sigma_i\rangle)_{i\in\omega}$ (known as* axioms*) such that $\sum_{i\in\omega} 2^{-n_i} \leqslant 1$, we can effectively obtain a prefix-free machine M such that for each i there is a τ_i of length n_i with $M(\tau_i)\downarrow = \sigma_i$, and $M(\mu)\uparrow$ unless $\mu = \tau_i$ for some i.*

3 A short proof of Solovay's theorem

We now give our simple proof of Solovay's theorem that H-trivial reals exist. This was proved by Solovay in his 1974 manuscript [35]. The proof there is complicated and only constructs a Δ^0_2 real.

Theorem 3.1 (after Solovay [35]) *There is a noncomputable c.e. set A such that $H(A \upharpoonright n) \leqslant H(n) + O(1)$.*

Remark 3.2 While the proof below is easy, it is slightly hard to see why it works. So, by way of motivation, suppose that we were to asked to "prove" that the set $B = \{0^n : n \in \omega\}$ has the same complexity as $\omega = \{1^n : n \in \omega\}$. A complicated way to do this would be for us to build our own prefix-free machine M whose only job is to compute initial segments of B. The idea would be that if the universal machine U converges to 1^n on input σ then $M(\sigma)\downarrow= 0^n$. Notice that, in fact, using Kraft-Chaitin it would be enough to build M *implicitly*, enumerating the length axiom (or "requirement") $\langle |\sigma|, 0^n\rangle$. We are guaranteed that $\sum_{\tau\in\mathrm{dom}(M)} 2^{-|\tau|} \leqslant \sum_{\sigma\in\mathrm{dom}(U)} 2^{-|\sigma|} \leqslant 1$, and hence Kraft-Chaitin applies.

Note also that we could, for convenience and as we do in the main construction, use a string of length $|\sigma|+1$, in which case we would ensure that $\sum_{\tau\in\mathrm{dom}(M)} 2^{-|\tau|} < 1/2$.

Proof of Theorem 3.1. The idea is the following. We will build a noncomputable c.e. set A in place of the B described in the remark and, as above, we will slavishly follow U on n in the sense that whenever U enumerates, at stage s, a shorter σ with $U(\sigma) = n$, then we will enumerate a requirement $\langle |\sigma|+1, A_s \upharpoonright n\rangle$ for our machine M. To make A noncomputable, we will also sometimes make $A_s \upharpoonright n \neq A_{s+1} \upharpoonright n$. Then for each j with $n \leqslant j \leqslant s$, for the currently shortest string σ_j computing j, we will also need to enumerate an axiom $\langle |\sigma_j|, A_{s+1} \upharpoonright j\rangle$ for M. This construction works by making this extra measure added to the domain of M small.

We are ready to define A:

$$A = \{\langle e,n\rangle : \exists s\,(W_{e,s} \cap A_s = \emptyset \wedge \langle e,n\rangle \in W_{e,s} \wedge \sum_{\langle e,n\rangle \leqslant j \leqslant s} 2^{-H(j)[s]} < 2^{-(e+2)})\},$$

where $W_{e,s}$ is the stage s approximation to the eth c.e. set and $H(j)[s]$ is the stage s approximation to the H-complexity of j.

Clearly A is c.e.. Since $\sum_{j\geqslant m} 2^{-H(j)}$ goes to zero as m increases, if W_e is infinite then $A^{[e]} \cap W_e^{[e]} \neq \emptyset$. It is easy to see that this implies that A is noncomputable. Finally, the extra measure put into the domain of M, beyond one half of that which enters the domain of U, is bounded by $\sum_e 2^{-(e+2)}$ (corresponding to at most one initial segment change for each e), whence

$$\sum_{\sigma\in\mathrm{dom}(M)} 2^{-|\sigma|} < \sum_{\sigma\in\mathrm{dom}(U)} 2^{-(|\sigma|+1)} + \sum_e 2^{-(e+2)} \leqslant \frac{1}{2} + \frac{1}{2} = 1.$$

Thus M is a prefix-free machine, and hence $H(A \upharpoonright n) \leqslant H(n) + O(1)$. □

We remark that the above proof can be modified to prove a stronger result, which appears to be due to Muchnik, namely that there exists a noncomputable c.e. set A that is super-H-trivial, in the sense that H-complexity relativized to A is the same as H-complexity, up to an additive constant. Such an A is both H-trivial and low for random.

Clearly the proof also admits many variations. For instance, we can make A promptly simple, or below any nonzero computably enumerable degree. We cannot control the jump or make A Turing complete, since, as we will see, all H-trivials are Turing incomplete, and in fact, low_2. We do not know if the H-trivials coincide with the low for random sets. An interesting test case is whether all H-trivials are of low Turing degree, since all low for random sets are of low Turing degree (by combining results of Kučera and Terwijn [22] and Nies [31]).

4 Turing degrees of H-trivials

In this section we give a proof that every H-trivial c.e. real is Turing incomplete. This proof can be modified to show that every H-trivial real α is Turing incomplete, and in fact not high (i.e., $\alpha' <_T \emptyset'$). A more complicated modification shows that α must be array computable, and hence low_2 (i.e., $\alpha'' \equiv_T \emptyset''$).

Theorem 4.1 *Every H-trivial c.e. real is Turing incomplete.*

Proof. Since for every c.e. real there is a wtt-equivalent c.e. set, it is enough to prove the theorem for c.e. sets.

Suppose that A is H-trivial, c.e., and complete. For convenience, assume that $0 \notin A$, so that, thought of as a real, $A \leqslant 1/2$. Let e be such that $\Phi_e^A = K$, where K is the halting problem, and let d be such that $\forall n\ (H(A \upharpoonright n) \leqslant H(n) + d)$.

We build a c.e. set B and a prefix-free machine M (via the Kraft-Chaitin Theorem). By the Recursion Theorem, we can assume that we know i such that $\Phi_i^K = B$ and the coding constant b of M. Let $\Gamma = \Phi_i \circ \Phi_e$, so that $\Gamma^A = B$, and let $c = b + d$, so that $\forall n\ (H(A \upharpoonright n) \leqslant H_M(n) + c)$. Let $k = 2^{c+2}$.

We adopt the usual conventions on the use γ of Γ. All values appended by $[s]$ will be taken at the end of the stage. We also assume that we have slowed down our construction enough so that $\forall s\ \forall n \leqslant s\ (H(A \upharpoonright n)[s] \leqslant H_M(n)[s] + c)$ and $\forall s\ \forall n \leqslant s\ (\Gamma^A(n)[s]\downarrow)$.

We will have the following global variables: natural numbers $m_0, \ldots, m_{k-1}$, which are always kept in increasing order; reals *Used* and *Trash*; and sets of natural numbers $\mathit{Current}_j$ for $j \leqslant k$ and *Successful*. In each procedure below, q will always be a local variable.

Let us first define the procedure Increase:

(i) Let $s + 1$ be the current stage.

(ii) Choose a fresh large n and enumerate $\langle n, 2^{-\gamma^A(m_{k-1})[s]}\rangle$ as an axiom for M. Add $2^{-\gamma^A(m_{k-1})[s]}$ to *Used*.

(iii) If during stage $s+1$ some number enters A below $\gamma^A(m_{k-1})[s]$ then remove $2^{-\gamma^A(m_{k-1})[s]}$ from *Used* and add it to *Trash*. In this case, return 0.

(iv) Enumerate n into $\mathit{Current}_k$, conclude stage $s+1$, and return $2^{-\gamma^A(m_{k-1})[s]}$.

Let us now define the procedure Load(j):

(i) If $j = k$ then return INCREASE.

(ii) Let $q = 0$ and let $s+1$ be the current stage.

(iii) While $q < 2^{-\gamma^A(m_{j-1})}[s]$ (or $q < 1/2$ if $j = 0$):
 (a) Call LOAD$(j+1)$ and add the returned value to q.
 (b) End the current stage t.
 (c) If $\gamma^A(m_{j-1})[t] \neq \gamma^A(m_{j-1})[s]$ then remove q from *Used* and add it to *Trash*. In this case, empty $Current_{j+1}$ and return 0.

(iv) Enumerate m_j into B and choose a fresh large value for each m_i, $i \geqslant j$.

(v) If, during the current stage $t+1$, some number enters A below $\gamma^A(m_{j-1})[t]$ then remove q from *Used* and add it to *Trash*. In this case, empty $Current_{j+1}$ and return 0.

(vi) Enumerate every number in $Current_{j+1}$ into $Current_j$, empty $Current_{j+1}$, conclude stage $t+1$, and return q.

Our main procedure is as follows:

(i) Let $Used = Trash = 0$ and let each $Current_j$ be empty. Choose values for $m_0, \dots, m_{k-1}$.

(ii) Call LOAD(0)

(iii) Let $Successful = Current_0$.

It is easy to check that the total amount of the axioms for M is equal to $Used + Trash$, that $Used \leqslant 1/2$, and that $Trash \leqslant A \leqslant 1/2$. (To see that $Trash \leqslant A$, notice that, for each $n \in A$, the amount that is put into *Trash* as a consequence of n entering A at stage s is at most the amount corresponding to the elements of $Current_j$ for the least j such that $n < \gamma^A(m_j)[s]$, and that this amount is bounded by $2^{-\gamma^A(m_j)[s]}$.)

Furthermore, the main procedure must terminate. This can be argued by reverse induction. First of all, LOAD(k) always returns. Now assume that LOAD$(j+1)$ always returns. Then the only way LOAD(j) can get stuck is if the values returned by successive calls to LOAD$(j+1)$ go to 0. But that would mean that $\lim_s \gamma^A(m_j)[s] = \infty$, contradicting the choice of Γ. Thus, by induction, LOAD(0) always returns, and by the same argument as above, the values returned by successive calls to this routine do not go to 0. This means that the main procedure eventually terminates.

It is now easy to check that $Used = \sum_{n \in Successful} 2^{-H_M(n)} = 1/2$. We claim that for each $n \in Successful$, if s is least such that $H_M(n)[s+1] = H_M(n)$ then $A \upharpoonright n$ assumes at least k many values after stage s. If this is true then we have a contradiction, since $\sum_{n \in Successful} k 2^{-(H_M(n)+c)} = k 2^{-c} \sum_{n \in Successful} 2^{-H_M(n)} = 2^{c+2} 2^{-c}(1/2) > 1$.

To verify the claim, let $n \in Successful$. At some stage $s+1$ we enumerate $\langle n, 2^{-\gamma^A(m_{k-1})[s]} \rangle$ as an axiom for M. Notice that $H_M(n)[s+1] = H_M(n)$, since we never enumerate another axiom involving n.

For each $j < k$, let $t_j + 1$ be the stage at which n enters $Current_j$ and let

$l_j = \gamma^A(m_j)[s]$. Since m_j enters A stage t_j+1, we have $A[t_j+1] \upharpoonright l_j \neq A[s] \upharpoonright l_j$. On the other hand, $A[t_j+1] \upharpoonright l_{j-1} = A[s] \upharpoonright l_{j-1}$, since otherwise n could not enter $Current_j$.

So we have $A[t_{k-1}] \upharpoonright n \neq \cdots \neq A[t_0] \upharpoonright n$, as desired. □

One final limitation is the following.

Theorem 4.2 *The Turing degrees of H-trivial reals are bounded by a c.e. degree strictly below* $\mathbf{0}'$.

Proof. Nies (unpublished) has shown that every H-trivial real is Turing reducible to an H-trivial c.e. set, so it is enough to prove the theorem for the degrees of H-trivial c.e. sets. Notice that the statement "$H(W_i \upharpoonright n) \leqslant H(1^n)+c$ for all n" is Π^0_2 in the parameters i, c. Thus the collection of indices of H-trivial c.e. sets is Σ^0_3. We can enumerate a piecewise c.e. set A where the $\langle i, c\rangle$-th column is equal to W_i iff W_i is H-trivial with constant c, and finite otherwise. By Theorem 6.3, the H-trivials are closed under join, so such a set has the property that $\oplus_{m\leqslant n} A^{(m)}$ is Turing incomplete for all m. Hence, the result follows from the strong form of the thickness lemma (e.g., Soare [33], Ch. VIII, Theorems 2.3 and 2.6). □

In unpublished work, Nies has shown that the degrees of H-trivial c.e. sets are bounded below $\mathbf{0}'$ by a low$_2$ c.e. set. This is much more difficult to prove.

5 Zambella's Theorem

In this section we will give proofs of some unpublished material of Zambella. Our proofs are different and we establish some intermediate results of independent interest.

Definition 5.1 Given a prefix free machine D, we define the *Zambella measure* with respect to D as

$$Z_D(\sigma) = \mu(D^{-1}(\sigma)).$$

That is, $Z_D(\sigma)$ is the probability that D outputs σ. If D is the fixed universal machine we will write $Z(\sigma)$ for $Z_D(\sigma)$.

Theorem 5.2 $Z_D(\sigma) = O(2^{-H(\sigma)})$.

We make a few comments before proving this theorem. A measure of complexity is any function $F : 2^{<\omega} \to \omega$ such that $\sum_\sigma 2^{-F(\sigma)} < 1$ and $\{\langle \sigma, k\rangle : F(\sigma) \leqslant k\}$ is c.e.. Chaitin [5] introduced this concept and showed that H-complexity is a minimal measure of complexity in the sense that, for any measure of complexity F, we have $H(\sigma) \leqslant F(\sigma) + O(1)$. Notice that $-\log_2 Z(\sigma)$ is a measure of complexity, and hence, by the minimality of H among measures of complexity, we know that $2^{-H(\sigma)} \leqslant Z(\sigma)$. Therefore, by

Theorem 5.2, we know that for some constant d,

$$2^{-H(\sigma)} \leqslant Z(\sigma) \leqslant d2^{-H(\sigma)}.$$

Therefore, we can often replace usage of H by Z. As an illustration, for reals α and β, we have the following result.

Theorem 5.3 *$\alpha \leqslant_H \beta$ iff there is a constant c such that for all n,*

$$cZ(\beta \upharpoonright n) \geqslant Z(\alpha \upharpoonright n).$$

Proof. Suppose that $\alpha \leqslant_H \beta$. Then there is a constant d such that for all n, $H(\alpha \upharpoonright n) \leqslant H(\beta \upharpoonright n) + d$. This happens iff there is a constant d' such that for all n,

$$2^{-H(\alpha \upharpoonright n)} \geqslant d' 2^{-H(\beta \upharpoonright n)}.$$

This happens iff for some c and all n, $Z(\alpha \upharpoonright n) \geqslant cZ(\beta \upharpoonright n)$. The other direction is similar. □

Remark 5.4 For any σ, $Z(\sigma)$ is random.

To see that the remark is true we use the Kraft-Chaitin Theorem to build a machine M and show that $\Omega \leqslant_S Z(\sigma)$, where $\leqslant_S$ is Solovay reducibility (see [12] for a definition and discussion of Solovay reducibility). At stage s, if we see $U(\nu)\downarrow$, where U is the universal machine, we declare that $M(\nu) = \sigma$. Then for some $c = c_M$, there is a ν' with $U(\nu') = \sigma$ and furthermore $|\nu| \leqslant |\nu'| + c$. Thus whenever we add $2^{-|\nu|}$ to Ω, we add $2^{-(|\nu|+c)}$ to $Z(\sigma)$, and hence $\Omega \leqslant_S Z(\sigma)$, which implies $Z(\sigma)$ is random.

We now turn to the proof of Theorem 5.2. The idea of the proof is the following: We will use the Kraft-Chaitin Theorem to define a prefix-free machine M as follows. Whenever we see $Z_D(\sigma) \geqslant 2^{2r-n}$, where n is the current H-complexity of σ, we will enumerate an axiom $\langle n - r + 1, \sigma\rangle$ (saying that some string of length $n - r + 1$ is mapped to σ by M). For large enough r we will get to contradict the minimality of H. In detail, at stage s, we do the following.

For each $\sigma, n, r < s$, if

- σ, n, s is not yet attended to,
- $n > 2r \geqslant 2$,
- $H(\sigma)[s] = n$, and
- $Z_D(\sigma) \geqslant 2^{2r-n}$, then attend to σ, r, n by enumerating an axiom $\langle n-r+1, \sigma\rangle$.

Notice that for any fixed σ, r, we put in axioms $\langle n-r+1, \sigma\rangle$ for descending values of n. Let $h_{\sigma,r}$ be the last value put in. We add at most

$$\sum_{n=0}^{\infty} 2^{-(h_{\sigma,r}-r+1+n)} = 2^{-h_{\sigma,r}+r}$$

to the measure of the domain of M.

When we put in the last axiom $\langle h_{\sigma,r}-r+1, \sigma\rangle$, we see that $Z_D(\sigma) \geqslant 2^{2r-h_{\sigma,r}}$. Since D is prefix-free, for this fixed r we can conclude that

$$\sum_{\sigma} 2^{2r-h_{\sigma,r}} \leqslant 1.$$

Therefore,

$$2^r \sum_{\sigma} 2^{-h_{\sigma,r}+r} \leqslant 1.$$

Hence, for r we can add at most 2^{-r} to the measure of the domain of M. Thus, as $r \geqslant 1$, we can apply the Kraft-Chaitin Theorem to conclude that M exists.

Let c be such that

$$H(\sigma) \leqslant H_M(\sigma) + c.$$

Let $d = 2^{2(c+2)}$. Then we claim that

$$Z_D(\sigma) \leqslant d2^{-H(\sigma)}.$$

To see this, let $r = c+2$. If $Z_D(\sigma) > 2^{2r-H(\sigma)}$, then eventually we put in an axiom $\langle H(\sigma)-r+1, \sigma\rangle$, and hence $H_M(\sigma) \leqslant H(\sigma)-(c+1)$, a contradiction. This concludes the proof of Theorem 5.2.

This result allows us to get a analog of the result of Chaitin for the number of descriptions of a string.

Corollary 5.5 *There is a constant d such that for all c and all σ,*

$$|\{\nu : D(\nu) = \sigma \ \wedge \ |\nu| \leqslant H(\sigma) + c\}| \leqslant d2^c.$$

Proof. Trivially,

$$\mu(\{\nu : D(\nu) = \sigma \wedge |\nu| \leqslant H(\sigma) + c\}) \geqslant \\ 2^{-(H(\sigma)+c)} \cdot |\{\nu : D(\nu) = \sigma \wedge |\nu| \leqslant H(\sigma) + c\}|.$$

But also, $\mu(\{\nu : D(\nu) = \sigma \ \wedge \ |\nu| \leqslant H(\sigma)+c\}) \leqslant d \cdot 2^{-H(\sigma)}$, by Theorem 5.3. Thus,

$$d2^{-H(\sigma)} \geqslant 2^{-c}2^{-H(\sigma)}|\{\nu : D(\nu) = \sigma \ \wedge \ |\nu| \leqslant H(\sigma) + c\}|.$$

Hence, $d2^c \geqslant |\{\nu : D(\nu) = \sigma \ \wedge \ |\nu| \leqslant H(\sigma) + c\}|$. □

We can now conclude that there are few H-trivials.

Theorem 5.6 *The set $S_d = \{\sigma : H(\sigma) < H(|\sigma|) + d\}$ has at most $O(2^d)$ many strings of length n.*

Proof. Given a universal prefix-free machine U, there is another machine V with the following property: V has for each n a program of length m (on which it converges) whenever the sum of all $2^{-|p|}$ such that $U(p)$ is defined and has length n is at least 2^{1-m}; furthermore V has for every n and every length m at most one program of length m. As U is universal, it follows that there is a constant c such that the following holds: If the sum of all $2^{-|p|}$ such that $U(p)$ is defined and has length n is at least 2^{c-m}, then there is a program q of length m with $U(q) = n$.

Let $m = H(n)$ and n be any length. There are less than 2^{d+c+1} many programs p of length $m + d$ or less such that $U(p)$ has length n, as otherwise the sum $2^{-|p|}$ over these programs would be at least 2^{c+1-m}, which would cause the existence of a program of length $m-1$ for n, a contradiction to $H(n) = m$. So the set $S_d = \{\sigma : H(\sigma) < H(|\sigma|) + d\}$ has at most 2^{d+c+1} many strings of length n, where c is independent of n and d. □

Corollary 5.7 (i) (Zambella [40]) *For a fixed d, there are at most $O(2^d)$ many reals α with*

$$H(\alpha \restriction n) \leqslant H(1^n) + d$$

for all n.

(ii) (Chaitin [5]) *If a real is H-trivial, then it is Δ^0_2.*

Proof. Consider the Δ^0_2 tree $T_d = \{\sigma : \forall \nu \subseteq \sigma(\nu \in S_d)\}$. This tree has width $O(2^d)$, and hence it has at most $O(2^d)$ many infinite paths. For each such path X, we can choose $\sigma \in T_d$ such that X is the only path above σ. Hence such X is Δ^0_2. □

6 Triviality and wtt-reducibility

Recall that $A \leqslant_{wtt} B$ iff there is a procedure Φ with computable use φ such that $\Phi^B = A$. As we have seen in the earlier papers mentioned in the introduction, *wtt*-reducibility seems to have a lot to do with randomness considerations. Triviality is no exception.

Theorem 6.1 *Suppose that $\alpha \leq_{wtt} \beta$ and β is H-trivial. Then α is H-trivial.*

Proof. For each computable $\varphi : \mathbb{N} \mapsto \mathbb{N}$,

$$H(\varphi(n)) \leqslant H(n) + O(1).$$

(To see this consider the prefix-free machine M such that for all σ, if $U(\sigma) = n$ then $M(\sigma) = \varphi(U(\sigma))$, where U is a universal prefix-free machine.)

Now suppose that $\alpha = \Phi^\beta$ with computable use φ and that β is H-trivial. We have

$$H(\alpha \restriction n) \leqslant H(\beta \restriction \varphi(n)) + O(1) \leqslant H(\varphi(n)) + O(1) \leqslant H(n) + O(1),$$

by the above. □

We now show that the H-trivials are closed under $\oplus$, and hence form an ideal in the *wtt*-degrees. We begin by showing that the H-trivials are closed under addition.

Theorem 6.2 *If α and β are H-trivial then so is $\alpha + \beta$.*

Proof. Assume that α, β are two H-trivial reals. Then there is a constant c such that $H(\alpha \upharpoonright n)$ and $H(\beta \upharpoonright n)$ are both below $H(n) + c$ for every n. By Theorem 5.6 there is a constant d such that for each n there are at most d strings $\tau \in \{0,1\}^n$ satisfying $H(\tau) \leqslant H(n) + c$. Let e be the shortest program for n. One can assign to $\alpha \upharpoonright n$ and $\beta \upharpoonright n$ numbers $i, j \leqslant d$ such that they are the i-th and the j-th string of length n enumerated by a program of length up to $|e| + c$.

Let U be a universal prefix-free machine. We build a prefix-free machine V witnessing the H-triviality of $\alpha + \beta$. Representing i, j by strings of the fixed length d and taking $b \in \{0,1\}$, $V(eijb)$ is defined by first simulating $U(e)$ until an output n is produced and then continuing the simulation in order to find the i-th and j-th string α and β of length n such that both are generated by a program of size up to $n + c$. Then one can compute $2^{-n}(\alpha + \beta + b)$ and derive from this string the first n binary digits of the real $\alpha + \beta$. These digits are correct provided that e, i, j are correct and b is the carry bit from bit $n+1$ to bit n when adding α and β – this bit is well-defined unless $\alpha + \beta = z \cdot 2^{-m}$ for some integers m, z, but in that case $\alpha + \beta$ is computable and one can get the first n bits of $\alpha + \beta$ directly without having to do the more involved construction given here. $\square$

Corollary 6.3 *The wtt-degrees containing H-trivials form an ideal in the wtt-degrees.*

Proof. By Theorem 6.2, we know that if α and β are H-trivial, then so is $\alpha + \beta$, where $+$ is normal addition. Now let $\alpha' = \alpha(0)0\alpha(1)0\ldots$, where $\alpha(n)$ is the nth bit of α, and let $\beta' = 0\beta(0)0\beta(1)\ldots$. Both α' and β' are H-trivial, since they have the same *wtt*-degrees as α and β, respectively. It follows that $\alpha' + \beta' = \alpha \oplus \beta$ is H-trivial. $\square$

Theorem 6.2 suggests the question of whether addition is a join on the H-degrees. In general, it is not (for example, $\Omega \not\leqslant_H \Omega + (1 - \Omega)$), but for c.e. reals it is. This fact considerably simplifies the analysis of the H-degrees of c.e. reals (compare for instance the difficulties in studying the sw-degrees considered in [11], many of which arise from the lack of a join operation).

Theorem 6.4 *If α, β are c.e. reals then the H-complexity of $\alpha + \beta$ is – up to an additive constant – the maximum of the H-complexities of α and β. In particular, $\alpha + \beta$ represents the join of α and β with respect to H-reducibility.*

Proof. Let $\gamma = \alpha + \beta$. Without loss of generality, the reals represented by α, β are in $(0, 1/2)$, so that we do not to have to care about the problem of represent digits before the decimal point. Furthermore, we have programs i, j, k which approximate α, β, γ, respectively, from below, such that at every stage and also for the limit the equation $\alpha + \beta = \gamma$ holds.

First we show that $H(\gamma \upharpoonright n) \leqslant \max\{H(\alpha \upharpoonright n), H(\beta \upharpoonright n)\} + c$ for some constant c. Fix a universal prefix-free machine U. It is sufficient to produce a prefix-free machine V that for each n computes $(\alpha+\beta)\upharpoonright n$ from some input of length up to $\max\{H(\alpha\upharpoonright n), H(\beta\upharpoonright n)\}+2$.

V receives as input eab where $a,b\in\{0,1\}$ and $e\in\{0,1\}^*$. The length of the input is $|e|+2$. First V simulates $U(e)$. In the case that this simulation terminates with some output σ, let $n=|\sigma|$. Now V simulates the approximation of α and β from below until it happens that either

- $a=0$ and $\sigma=\alpha\upharpoonright n$ or
- $a=1$ and $\sigma=\beta\upharpoonright n$.

Let $\tilde{\alpha},\tilde{\beta}$ be the current values of the approximations of α and β, respectively, when the above simulation is stopped. Now V outputs the first n bits of the real $\tilde{\alpha}+\tilde{\beta}+b\cdot 2^{-n}$.

In order to verify that this works, given n, let a be 0 if the approximation of β is correct on its first n bits before the one of α and let a be 1 otherwise. Let e be the shortest program for $\alpha\upharpoonright n$ in case $a=0$ and for $\beta\upharpoonright n$ in case $a=1$. Then $U(e)$ terminates and $|e|\leqslant\max\{H(\alpha\upharpoonright n), H(\beta\upharpoonright n)\}$. In addition, we know both values $\alpha\upharpoonright n$ and $\beta\upharpoonright n$ once $U(e)$ terminates. So $\tilde{\alpha}$ and $\tilde{\beta}$ (defined as above) are correct on their first n bits, but it might be that bits beyond the first n cause a carry to exist which is not yet known. But we can choose b to be that carry bit and have then that $V(eab)=\gamma\upharpoonright n$.

For the other direction, we construct a machine W that computes $(\alpha\upharpoonright n,\beta\upharpoonright n)$ from any input e with $U(e)=\gamma\upharpoonright n$. The way to do this is to simulate $U(e)$ and, whenever it gives an output σ, to simulate the enumerations of α,β,γ until the current approximation $\tilde{\gamma}\upharpoonright n=\sigma$. As $\tilde{\alpha}+\tilde{\beta}=\tilde{\gamma}$, it is impossible that the approximations of α,β will later change on their first n bits if $\gamma\upharpoonright n=\sigma$. So the machine W then just outputs $(\tilde{\alpha}\upharpoonright n,\tilde{\beta}\upharpoonright n)$, which is correct under the assumption that e, and therefore also σ, are correct. $\square$

Recall that a computably enumerable set X is (Kummer) complex iff $K(X\upharpoonright n)\geqslant 2\log n-c$ infinitely often. (No computably enumerable set can have $K(X\upharpoonright n)\geqslant 2\log n-c$ for all n (see [28], Exercise 2.58).) Recall also that, by [24], a computably enumerable degree $\mathbf{d}$ either has complex c.e. sets or every c.e. set $D\in\mathbf{d}$ is Kummer trivial in the sense that for all $\epsilon>0$ there is a constant c such that for all n,

$$K(D\upharpoonright n)\leqslant(1+\epsilon)\log n+d.$$

The relevant degrees containing the complex sets are the array noncomputable degrees of Downey, Jockusch and Stob. Recall that a very strong array $\{F_x : x\in\mathbb{N}\}$ is a strong array such that $|F_x|<|F_{x+1}|$ for all x. A c.e. set A is called anc relative to such a very strong array iff for all c.e. sets W there are infinitely many x such that $W\cap F_x=A\cap F_x$. A relevant fact for our purposes is the following.

Theorem 6.5 (Downey, Jockusch and Stob [13,14]) *For all wtt degrees*

d, *and all very strong arrays* $\{F_x : x \in \mathbb{N}\}$, *if* **d** *contains a set that is anc relative to some very strong array, then* **d** *contains one which is anc relative to* $\{F_x : x \in \mathbb{N}\}$.

We first show that array noncomputable *wtt*-degrees (i.e., ones containing anc c.e. sets) cannot be H-trivial.

Theorem 6.6 *If* **d** *is an array noncomputable c.e. wtt-degree then no set in* **d** *is* H*-trivial.*

Proof. We will build a prefix-free machine M. The range of M will consist of initial segments of 1^ω. By the Recursion Theorem, we can assume we know the coding constant d of our machine in the universal prefix-free machine U. Choose a very strong array such that $|F_e| = 2^{d+e+1}$. By Theorem 6.5, **d** contains a set A anc relative to this array. We claim that A is not H-trivial, and hence the wtt-degree **d** contains no H-trivials.

Suppose that A is H-trivial and that $A \leqslant_H 1^\omega$ with constant c. We will build a c.e. set V with $V \cap F_g \neq A \cap F_g$ for all $g > c$, contradicting the array noncomputability of A. For each e, we do the following. First we "load" 2^{d+e+1} beyond $\max\{x : x \in F_{e+c}\}$, by enumerating into our machine an axiom $\langle 2^{d+e+1}, 1^z\rangle$ for some fresh $z > \max\{x : x \in F_{e+c}\}$. The universal machine must respond at some stage s by converging to $A_s \upharpoonright z$ on some input σ of length $\leqslant d + e + 1 + c$. We then enumerate into V_s, our "kill" c.e. set, the least $p \in F_{e+c}$ not yet in V_s, making $F_{e+c} \cap A[s] \neq V_s \cap F_{e+c}[s]$. Notice that we only trigger enumeration into V at stages *after* a quantum of $2^{e+1+c+d}$ has been added to the measure of the domain of U. Now the possible number of changes we can put into V for the sake of $e + c$ is $|F_{e+c}|$, which is bigger than $2^{e+c+1+d}$. Hence A cannot respond each time, since if it did then the domain of U would have measure bigger than 1. $\square$

One might be tempted to think that the Kummer trivial c.e. sets and the H-trivial sets correspond. The next result shows that at least one inclusion fails. The proof is technical, and we omit it in the interest of space.

Theorem 6.7 *There is a c.e. Turing degree* **a** *which consists only of Kummer trivials but contains no* H*-trivials.*

Array noncomputable degrees have one further connection with our investigations. Recall that a set A is low for random iff every random set is still random relative to A. Kučera and Terwijn [22] were the first to construct such sets. They used a theorem of Sacks [32] to prove that any low for random set A must be of GL_1 Turing degree. That is, $A \oplus \emptyset' \equiv_T A'$. This was improved by Nies [31], who also showed that there are only countably many low for random sets, and that they are all Δ^0_2 and hence low (i.e., $A' \equiv_T \emptyset'$). The following result seems to be a theorem of Zambella. Following Ismukhametov [16] we call a set A *traceable* or *weakly computable* iff there is a computable function f such that for all $g \leqslant_T A$, there is a weak array $\{W_{h(x)} : x \in \mathbb{N}\}$ such that

(i) $|W_{h(x)}| \leqslant f(x)$ for almost all x and

(ii) $g(x) \in W_{h(x)}$ for all x.

Ismukhametov [16] observed that if a degree is weakly computable then it is array computable, and the notions coincide for computably enumerable sets. Ismukhametov proved the remarkable theorem that the c.e. degrees with strong minimal covers are exactly the weakly computable degrees. Furthermore, any weakly computable degree (in general) has a strong minimal cover.

Theorem 6.8 *Suppose that A is low for random. Then A is low* **(Nies [31])** *and additionally A must be weakly computable.*

Proof sketch. If one mimics the Terwijn-Zambella proof that Schnorr low sets are computably traceable ([37]), but using Martin-Löf lowness in place of Schnorr lowness, then the "if" direction proves the theorem. □

References

[1] Ambos-Spies K., and A. Kučera, *Randomness in computability theory*, in *Computability Theory and its Applications* (Cholak, Lempp, Lerman, Shore, eds.), Contemporary Mathematics 257, Amer. Math. Soc., Providence, 2000, 1–14.

[2] Calude, C., *Information Theory and Randomness, an Algorithmic Perspective,* Springer-Verlag, Berlin, 1994.

[3] Calude, C., P. Hertling, B. Khoussainov, B., and Y. Wang, *Recursively enumerable reals and Chaitin's Ω numbers*, Theoretical Computer Science 255 (2001), 125–149.

[4] Calude, C., and A. Nies, *Chaitin Ω numbers and strong reducibilities*, Journal of Universal Computer Science 3 (1998), 1162–1166.

[5] Chaitin, G., *A theory of program size formally identical to information theory*, Journal of the Association for Computing Machinery 22 (1975), 329–340.

[6] Chaitin, G. *Information-theoretical characterizations of recursive infinite strings,* Theoretical Computer Science 2 (1976), 45–48.

[7] Downey, R., *Δ^0_2 degrees and transfer theorems*, Illinois J. Math 31 (1987), 419–427.

[8] Downey, R. and E. Griffiths, *On Schnorr randomness*, in preparation.

[9] Downey, R. and D. Hirschfeldt, *Aspects of Complexity* (Short courses in complexity from the New Zealand Mathematical Research Institute Summer 2000 meeting, Kaikoura) Walter De Gruyter, Berlin and New York, 2001.

[10] Downey, R. and D. Hirschfeldt, *Algorithmic Randomness and Complexity*, Springer-Verlag, in preparation.

[11] Downey, R, D. Hirschfeldt, and G. Laforte, *Randomness and reducibility*, in *Mathematical Foundations of Computer Science 2001* (Sgall, Pultr, P. Kolman, eds.), Lecture Notes in Computer Science 2136, Springer, 2001, 316–327.

[12] Downey, R., D. Hirschfeldt, and A. Nies, *Randomness, computability, and density*, *SIAM Journal on Computing* 31 (2002) 1169–1183 (extended abstract in proceedings of STACS 2001).

[13] Downey, R., C. Jockusch and M. Stob, *Array nonrecursive sets and multiple permitting arguments,* in *Recursion Theory Week* (Ambos-Spies, Muller, Sacks, eds.) Lecture Notes in Mathematics 1432, Springer-Verlag, Heidelberg, 1990, 141–174.

[14] Downey, R., C. Jockusch and M. Stob, *Array nonrecursive degrees and genericity*, in *Computability, Enumerability, Unsolvability* (Cooper, Slaman, Wainer, eds.), London Mathematical Society Lecture Notes Series 224, Cambridge University Press (1996), 93–105.

[15] Fortnow, L., *Kolmogorov complexity,* in [9], 73–86.

[16] Ishmukhametov, S., *Weak recursive degrees and a problem of Spector*, in *Recursion Theory and Complexity* (Arslanov and Lempp, eds.), de Gruyter, Berlin, 1999, 81–88.

[17] Kautz, S., *Degrees of Random Sets*, Ph.D. Diss., Cornell University, 1991.

[18] Ko, K.-I, *Complexity of Real Functions*, Birkhäuser, Berlin, 1991.

[19] Ko, K.-I, and H. Friedman, *On the computational complexity of real functions,* Theoretical Computer Science 20 (1982), 323–352.

[20] Kučera, A., *On relative randomness,* Annals of Pure and Applied Logic 63 (1993), 61–67.

[21] Kučera, A., *On the use of diagonally nonrecursive functions,* in *Logic Colloquium, '87* (Ebbinghaus, Fernandez-Prida, Garrido, Lascar, eds.), Studies in Logic and the Foundations of Mathematics 129, North-Holland, Amsterdam, 1989, 219–239.

[22] Kučera, A., and S. Terwijn, *Lowness for the class of random sets,* Journal of Symbolic Logic 64 (1999), 1396–1402.

[23] Kučera, A. and T. Slaman, *Randomness and recursive enumerability,* SIAM Journal on Computing 31 (2001), 199–211.

[24] Kummer, M., *Kolmogorov complexity and instance complexity of recursively enumerable sets,* SIAM Journal on Computing 25 (1996), 1123–1143.

[25] Kurtz, S., *Randomness and Genericity in the Degrees of Unsolvability*, Ph.D. Thesis, University of Illinois at Urbana-Champaign, 1981.

[26] Ladner, R. E. and L. P. Sasso, Jr., *The weak truth table degrees of recursively enumerable sets*, Ann. Math. Logic 8 (1975), 429–448.

[27] Levin, L., *The various measures of the complexity of finite objects (an axiomatic description)*, Soviet Mathematics Doklady 17 (1976), 522–526.

[28] Li, M. and P. Vitanyi, *An Introduction to Kolmogorov Complexity and its Applications*, 2nd edition, Springer-Verlag, New York, 1997.

[29] Loveland, D. *A variant of the Kolmogorov concept of complexity*, Information and Control 15 (1969), 510–526.

[30] Martin-Löf, P., *The definition of random sequences*, Information and Control 9 (1966), 602–619.

[31] Nies, A., *Low for random sets are* Δ^0_2, Technical Report, University of Chicago, 2002.

[32] Sacks, G., *Degrees of Unsolvability,* Princeton University Press, 1963.

[33] Soare, R., *Recursively enumerable sets and degrees*, Springer, Berlin, 1987.

[34] Solomonoff, R., *A formal theory of inductive inference I and II*, Information and Control 7 (1964), 1–22 and 224–254.

[35] Solovay, R. *Draft of a paper (or series of papers) on Chaitin's work*, unpublished notes, May, 1975, unpublished manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 215 pages.

[36] Turing, A., *On computable numbers with an application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society 42 (1936), 230–265, correction in Proceedings of the London Mathematical Society 43 (1937), 544–546.

[37] Terwijn, S. and D. Zambella, *Algorithmic randomness and lowness,* Journal of Symbolic Logic 66 (2001), 1199–1205.

[38] van Lambalgen, M., *Random Sequences,* Ph. D. Diss. University of Amsterdam, 1987.

[39] Weihrauch, K., *Computability*, EATCS Monographs on Theoretical Computer Science 9, Springer-Verlag, Berlin, 1987.

[40] Zambella, D., *On Languages with simple initial segments*, Technical Report, University of Amsterdam, 1990.