Some Computability-Theoretical Aspects of Reals and Randomness

Rodney G. Downey*
School of Mathematical and Computing Sciences
Victoria University
PO Box 600, Wellington, New Zealand

September 10, 2001

Abstract

We study computably enumerable reals (i.e. their left cut is computably enumerable) in terms of their spectra of representations and presentations. Then we study such objects in terms of algorithmic randomness, culminating in some recent work of the author with Hirschfeldt, Laforte, and Nies concerning methods of calibrating randomness.

1 Introduction

We study reals α, $0 < \alpha < 1$, unless otherwise specified and for convenience no real will be rational. This convention allows us to give uniform proofs of many results, which would otherwise split into cases of whether the real at hand was rational or not. In particular if we have a sequence of rationals converging to a real α then this sequence will be infinite, and furthermore every such real will have a unique dyadic expansion.

Much of modern computability theory is concerned with understanding the computational complexity of sets of *positive integers*, yet, even in the original paper of Turing [57], a central topic is interest in effectiveness considerations for *reals.* Of particular interest to computable analysis (e.g. Weihrauch [59], Pour-El [45], Pour-El and Richards [46], Ko [32]), and to algorithmic information theory (e.g. Chaitin [11], Calude [6], Martin-Löf [44], Li-Vitanyi [41]), is the collection of *computably enumerable reals.* These are the reals α such the lower cut $L(\alpha)$ consisting of rationals less than α forms a computably enumerable set.

The first part of these notes consists of an analysis of the basic ways that we present reals, and to clarify the relationship between such presentations and

*Research partially supported by the Marsden Fund of New Zealand. These notes are based upon a short course of lectures given in the fall of 2000 at the University of Notre Dame. The author thanks all the logicians there for their hospitality and support. He also thanks Andrew Arana for his skillful note-taking.

degree classes. In particular we will look at the recent work of Calude, Coles, Hertling, Khoussainov, Downey [13], Downey and Laforte [17], Ho [27], and Wu [59], as well as older of work of Soare [50] and others.

Our main goal is to look at algorithmic randomness, especially with respect to computably enumerable reals. To this end we will next introduce the basic approaches to the study of algorithmic randomness, both topological, as in Martin-Löf randomness, and compressibility notions such as Chaitin-Kolmogorov randomness. We begin by looking at these notions for finite strings and then proceed to reals.

Finally, we will look at some recent material of the calibration of relative randomness using notions such as Solovay reducibility and some new reducibilities rH and sw reducibilities.

Notation is more or less standard and follows Soare [54]. As these notes are aimed at graduate students, and one learns from actively engaging in the material, we will not always provide complete proofs, but will always provide sketches, referring the reader to the appropriate paper when necessary.

Of course, we identify reals with their characteristic functions when considered as dyadic expansions. (Remember, no real is rational.) Hence, if I write $\alpha = .A$, I mean that $\alpha = \Sigma_{n \in A} 2^{-n}$.

2 Reals, computable or otherwise

What is a real? Our first view of this question is that a real is a cut. Let α be a real. Then by $L(\alpha)$ we mean the left cut of α;

$$L(\alpha) = \{q \in \mathbb{Q} : q < \alpha\}.$$

We may approximate α via a Cauchy sequence, viz $\alpha = \lim_s q_s$.

What is a computable real? Here are three guesses based on the Cauchy definition.

(i) α is the limit of a computable sequence of rationals.

(ii) α is the limit of a computable monotone increasing sequence of rationals.

(iii) $\alpha = .A$ for some computable set A. (Here we consider A as identified with its characteristic function so that this is the dyadic expansion of α.)

Now it is a fact that $(iii) \to (ii) \to (i)$ but none of the implications can be reversed. If (iii) holds, (and note that we could equally have used a decimal expansion), then there is an algorithm M allowing us to compute $L(\alpha)$; namely, given n, we can compute $q_n = .A \upharpoonright n+1$ so that $|\alpha - q_n| < 2^{-n}$, so that given q we can calculate q_n's till either q appears in $L(\alpha)$ or it becomes bounded away from α. We cannot guarantee this in either (i) or (ii) since we and effective radius of convergence. Suppose that we call a real $\alpha = .A$ a computable real, if A is a computable set. The following is implicit in Turing's original paper.

Theorem 1 (Turing). *α is a computable real iff it is the limit of a computable sequence of rationals $q_i : i \in B$ and there is a computable algorithm M so that for all n,*

$$|\alpha - q_{M(n)}| < 2^{-n}.$$

The proof is left as an exercise, with the hint for the only if direction being that since the real is not rational there is always another 0 in its dyadic expansion. Note that we have not actually proved that (ii) and (iii) are different yet, only that they seem different. We look at this now.

Definition 1. *We call a real α computably enumerable (also sometimes, left computable, left c.e. semi-computable in the literature) iff $L(\alpha)$ is computably enumerable.*

We will need a technical notion whose use is crucial in later investigations, especially in terms of randomness. A set $A \subseteq 2^{<\omega}$ of strings is called *prefix free* iff for all $\sigma \in A$, and all τ with σ an initial segment of τ, $\tau \notin A$. Prefix free sets are considered for technical reasons since if a set A is prefix free then, as we soon see, by Kraft's inequality, we know that $\Sigma_{n \in A} 2^{-|n|}$ converges and conversely.

Theorem 2 (Calude, Khoussainov, Hertling, Wang [8], Soare [50]). *The following are equivalent.*

(i) α is the limit of a computable enumerable monotone increasing (in the real ordering) sequence of rationals.

(ii) α is computably enumerable.

(iii) There is an infinite computably enumerable prefix free set A with $\alpha = \Sigma_{n \in A} 2^{-|n|}$.

(iv) There is a computable prefix free set A such that $\alpha = \Sigma_{n \in A} 2^{-|n|}$.

(iv) There is a computable function $f(x, y)$ of two variables, such that

(iva) If, for some k, s we have $f(k, s+1) = 0$ yet $f(k, s) = 1$ then there is some $k' < k$ such that $f(k', s) = 0$ and $f(k', s+1) = 1$.

(ivb) $\alpha = \cdot a_1 a_2 ...$ is a dyadic expansion of a with $a_i = \lim_s f(i, s)$.

(v) There is a computable increasing sequence of rationals with limit α.

The reader should be aware of the two orderings at work here. In (i) the rationals are coded and the sequence of codes computably enumerable. It is possible to have the sequence "increasing" as a sequence of rationals in the real ordering yet as codes they could be decreasing. For (v) we mean that there is a computable function $g : \omega \mapsto \mathbb{Q}$ with $\alpha = \lim_s g(s)$ and the range of g a computable set of (codes of) rationals.

It is important that the reader realize that we are *not* defining a c.e. real to be $.A$ for some c.e. set A. Define a real α to be *strongly c.e.* if there is a c.e.

set A such that $\alpha = .A$. It is easy to use the characterization above (specifically (iv)) to construct a c.e. real that is not strongly c.e. (a theorem of Soare [50]).

Specifically, we need to satisfy the requirement

$$R_j : \alpha \neq .W_e.$$

The idea is very simple. Devote positions $2e$ and $2e + 1$ to R_e. We initially set $A(2e + 1) = 1, A(2e) = 0$. If ever $2e + 1 \in W_e$, make $A(2e + 1) = 0$ and $A(2e) = 1$.

Notice that every strongly c.e. real is c.e. but that if A is c.e. and not computable, then $\alpha = .A$ is c.e. and cannot be computable.

The sets A which have enumerations satisfying (iv) we call *nearly c.e.* and occupy a special place in our investigations.

None of the proofs are difficult. Why does (ii) imply (v)? we need to replace $q_0, q_1, \cdots$ with a computable enumeration with the same limit. Let $<_R$ denote the real ordering. We simply find a sequence of rationals with $q_n <_R r_n <_R q_{n+1}$ and such that the code of r_{n+1} exceeds that of r_n, which is possible by the density of the rationals. The sequence r_n so obtained has the same limit as the q_i and is increasing in Gödel number. All of the remaining implications are left to the reader, save the ones involving prefix free sets. For these results, we use a very important theorem called Kraft's inequality.

Theorem 3 (Kraft). *(i) If A is prefix free then $\sum_{n \in A} 2^{-|n|} \leq 1$.*

*(ii) (*sometimes called Kraft-Chaitin, of Chaitin simulation) *Let $d_1, d_2, \cdots$ be a collection of lengths, possibly with repetitions, Then $\Sigma 2^{-d_i} < 1$ iff there is a prefix free set A with members σ_i and σ_i has length d_i. Furthermore from the sequence d_i we can effectively compute the set A.*

Proof. The proof of Kraft's inequality comes from the topological correspondence $0 \mapsto [0, 1/2), 1 \mapsto [1/2, 1), 00 \mapsto [0, 1/4), 01 \mapsto [1/4, 1/2)$, etc with, in general $\sigma \mapsto I_\sigma$, the interval representing the cone above σ, which has measure $2^{-|\sigma|}$. The crucial fact is that if $\sigma | \tau$ then $I_\sigma \cap I_\tau = \emptyset$. Then if A is prefix free, the I_σ for $\sigma \in A$ form a disjoint set of intervals in the interval $[0, 1)$. Hence $\Sigma_{n \in A} 2^{-|n|} \leq 1$. Part (ii) comes from effectively reversing this idea and is left for the student. Alternatively the reader can consult Li-Vitanyi. □

One way to think of the effective version of Kraft's inequality, the so-called Kraft-Chaitin theorem, is the following.

We are effectively given a set of "requirements" $\langle n_k, \sigma_k \rangle$ for $k \in \omega$ with $\Sigma_k 2^{-n_k} \leq 1$. Then we can (primitive recursively) build a prefix free machine M and a collection of strings τ_k with $|\tau_k| = n_k$ and $M(\tau_k) = \sigma_k$.

It is an interesting exercise to see how to use the Kraft inequality in, for example, the proof of the Calude, Khoussainov, Hertling, Wang result. For instance, if α is c.e. then it can be constructed as a computable sequence of dyadic rationals α_s so that $\alpha_{s+1} - \alpha_s$ is of the form $\Sigma_{j \in B_s} 2^{-j}$ and we can have that $\sigma \in B_s$ implies that σ has length less than or equal to s. Thus $\alpha_{s+1} - \alpha_s = n(s) 2^{-(s+1)}$. Hence by Kraft's inequality we can find a A_s of strings of length $s+1$ with $\alpha_{s+1} - \alpha_s = \Sigma_{\sigma \in A_s} 2^{-|\sigma|}$, and so that $A = \cup_s A_s$ is prefix free. *The beauty of the Kraft inequality is that we need only make sure that the lengths work and then the prefix free set is implicitly given without any calculation being necessary.*

3 Other classes of reals.

One interesting and basically unexplored class of reals is the the class of d.c.e. reals. These are defined, perhaps unfortunately, as those reals α for which there exist c.e. reals β and γ such that $\alpha = \beta - \gamma$. They are interesting since the class of c.e. reals is certainly not closed under operations such as difference. Perhaps slightly surprisingly, the d.c.e reals form a field.

Lemma 4 (Ambos-Spies, Weihrauch, Zheng [3]). *α is d.c.e. iff there exists a constant M and a computable sequence of rationals q_n with limit α such that*

$$\Sigma_{j=0}^{\infty} |q_{j+1} - q_j| < M.$$

Proof. (only if) Let x be d.c.e. and $x = y - z$ with y, z c.e. reals. Let $y = \lim_s y_s$, and $z = \lim_s z_s$, and put $x_s = y_s - z_s$. Then $\Sigma_{n=0}^{\infty} |x_{n+1} - x_n| = \Sigma_{n=0}^{\infty} |(y_{n+1} - z_{n+1}) - (y_n - z_n)| \leq \Sigma_{n=0}^{\infty} |y_{n+1} - y_n| + \Sigma_{n=0}^{\infty} |z_{n+1} - z_n| \leq (y - y_0) + z - z_0$.

(if) Let $\Sigma_{n=0}^{\infty} |x_{n+1} - x_n|$ be bounded, then define y, z as limits as follows.

$$y_n = x_0 + \Sigma_{i=0}^{n} (x_{i+1} \dot{-} x_i); z_n = \Sigma_{i=0}^{n} (x_i \dot{-} x_{i+1}).$$

Then the limits exist because of the bounds on the sums, and one can readily verify that $x = y - z$. □

Question 1. *Characterize the computable g such that α is d.c.e. iff $\alpha(i) = \lim_s g(i, s)$ in the sense of (iv) of the Calude et. al. theorem above.*

Theorem 5 (Ambos-Spies, et. al. [3]). *The d.c.e. reals form a field.*

Proof. Rearranging shows closure under addition and subtraction and multiplication. (e.g. $(x - y)(p - q) = (xp + yz) - (yp + xz)$.) Division: suppose that $x_n \to x, y_n \to y$ with x, y d.c.e. and that $\Sigma_{n=0}^{\infty} |x_{n+1} - x_n|, \Sigma_{n=0}^{\infty} |y_{n+1} - y_n|, |x_n|, |y_n|, \frac{1}{y_n} < M$. Now

$$\Sigma_{n=0}^{\infty} |\frac{x_{n+1}}{y_{n+1}} - \frac{x_n}{y_n}| = \Sigma_{n=0}^{\infty} |\frac{y_n x_{n+1} - y_{n+1} x_n}{y_n y_{n+1}}|$$

$$\leq \Sigma_{n=0}^{\infty} |\frac{y_n x_{n+1} - y_n x_n + y_n x_n - y_{n+1} x_n}{y_n y_{n+1}}| \leq 2M^4.$$

□

Question 2. *Say something else about this field. For instance, what degrees do you get? Also what about its analytic properties such as real closure? Finally, what about its randomness properties.*

One could also ask what about other classes of reals. For instance, we have seen that if we have a monotone increasing computable sequence of reals we get a c.e. real. What happens if we weaken the condition that the sequence be monotone as reals? As we have seen if the jumps are bounded, then we get d.c.e. reals. In general, we get the following.

Theorem 6 (Ho [27]). *A real α is of the form $.A$ for A a Δ_2^0 set iff α is the limit of a computable set of rationals.*

Proof. This uses another padding+density argument, as in the Calude, et. al. result, and is left as an exercise. □

We remark that it is not difficult to show that there are d.c.e. reals that are not c.e. Here is a proof. Notice that if D is a d.c.e. set (that is $D = A - B$ for c.e. sets A and B) then $.D$ is a d.c.e. real.

Theorem 7 (Ambos-Spies, et. al.). *There is a d.c.e. set B such that $.B$ is not a left nor right computable real.*

Proof. Let C and D be c.e. Turing incomparable sets. Define the d.c. set B as follows.

$$B = \{4n : n \in \overline{C}\} \cup \{4n+1 : n \in C\} \cup \{4n+2 : n \in D\} \cup \{4n+3 : n \in \overline{D}\}.$$

Using the Calude et. al. characterization of c.e. reals, because of the $4x, 4x+1$ part, $\cdot\chi_B$ cannot be left computable, lest $C \leq_T D$, and similarly by the obvious modification to part (iva) above (reversing), the same shows that $\cdot\chi_B$ is not right computable lest $D \leq_T C$. For instance, if $\cdot\chi_B$ is left computable, let f be the strongly Δ_2^0 approximation given in (iv) of the Theorem. Note that we can run the approximations to C and D and f so that at each stage we can have things looking correct. That is, we can speed the enumeration so that for all s and all $n \leq s$, $n \in C_s$ iff $f(4n+1, s) = 1$ and $f(4n, s) = 0$, $n \notin C_s$ iff $f(4n, s) = 1$ and $f(4n+1, s) = 0$, and similarly for D_s, since this must be true for C, D and f in the limit. Assume that we have such enumerations. We claim that $C \leq_T D$ contrary to hypothesis. Suppose inductively we have computed C up to $n-1$. Let $s > n$ be a stage where the current approximation $f(i, s) : i \leq 4n+3$ correctly computes $C \restriction n-1$, Note this is okay by the induction hypothesis, and means that $C_s \restriction n-1 = C \restriction n-1$, $D \restriction n = D_s \restriction n$ using the D-oracle, and as above, f appears correct for C_s and D_s up to n. Then it can only be that $n \in C$ iff $n \in C_s$. (The point is that if n later enters C at $t > s$ then since $f(4n, t)$ must become 0 something must enter B smaller than $4n+1$. But this is impossible since we have $C \restriction n-1 = C_s \restriction n-1$, and $D \restriction n = D_s \restriction n$.) The non-right computability is entirely analogous. □

4 Degree-theoretical aspects of representations.

Definition 2. *We say that a c.e. sequence of rationals $\{q_i : i \in \omega\}$ with monotonic limit α* represents α.

Representations were first effectively analyzed by Calude, Coles, Hertling and Khoussainov [7]. We have seen that if a real is c.e. then it has a computable representation. If a real is computable then every representation must be computable (exercise). Suppose that a c.e. real is noncomputable. What else can be said about its representations? For instance, the natural degree of a c.e. real is the degree of its left cut: deg$L(\alpha)$. Does α always have a representation of degree deg$L(\alpha)$? of other degrees?

Theorem 8. *(i)* (**Calude, Coles, Hertling, Khoussainov**) *α has a representation of degree deg$L(\alpha)$.*

(ii) (**Soare [50]**) *If $B = \{q_i\}$ is a representation of α then $B \leq_T L(\alpha)$ and in fact $B \leq_{wtt} L(\alpha)$ where wtt denotes weak truth table reducibility*[1].

(iii) (**Calude, et. al.**)*Every representation of α is half of a c.e. splitting of $L(\alpha)$.*

The theorem above extends earlier work of Soare who examined, in particular, the relationship between $L(a)$ and deg(B) for $a = \Sigma_{n \in B} 2^{-n}$. In [50], Soare observed that $L(a) \leq_T B$ and $B \leq_{tt} L(a)$. However, he also proved that there are strongly c.e. a, as above, with $L(a) \not\leq_{tt} B$.

Evidently (iii) implies (ii). Clearly, if A represents α then A must be an infinite c.e. subset of $L(\alpha)$. The thing to note is that $L(\alpha) - A$ is also c.e.. Given rational q, if q occurs in $L(\alpha)$, we need only wait till either q occurs in A or some rational bigger than q does.

Note that this means that if α is computable then every representation of α is computable. Also note that the proof actually gives that if A represents α, $A \leq_{wtt} L(\alpha)$. (It is interesting to note that strong reducibilities often play a large role in effective mathematics since reducibilities that occur naturally tend to be stronger than $\leq_T$. For instance in a finitely presented group, the word problem tt-reduces to the conjugacy problem ([29]), algebraic closure is related to Q-reducibility ([5, 18, 43, 61]) and wtt-degrees characterize the degrees of bases of a c.e. vector space (Downey-Remmel [23]).)

We would like to prove that if A is half of a splitting of $L(\alpha)$ then A represents α. But it is not difficult to prove that this is not true. We know that if A represents α then there needs to be a computable function g with range A so that, as reals, $g(i) < g(i+1)$. It is easy to construct splittings of some α where no such g exists by a simple diagonalization argument. Calude et. al. did find that the converse of (iii) did happen in some cases.

Theorem 9 (Calude et. al. [7]). *Let A be a representation of α. For subsets B of A, the following are equivalent.*

- *B represents α.*

[1] We say that $A \leq_{wtt} C$ iff there is a Turing procedure Γ and a computable function γ such that for all x,

$$\Gamma(C; x) = A(x), \text{ and } u(\Gamma(C; x)) \leq \gamma(x).$$

- *B is half of a splitting of A.*

The proof of this result is straightforward and is left to the reader. Calude et. al. [7] also obtained a partial degree theoretical converse to (iii). Namely, they showed that *(i) α has a representation of degree deg($L(\alpha)$), and (ii) every representation can be extended to one of degree deg($L(\alpha)$).* In Downey [13], Downey improved the Calude et. al. [7] result, and obtained a complete characterization of the representations of a real x in terms of the m-degrees of splittings of $L(x)$.

Theorem 10 (Downey). *The following are equivalent*

- $\mathbf{b}$ *is the m-degree of a splitting of $L(x)$.*
- $\mathbf{b}$ *is the weak truth table degree of a representation of x.*

Proof. To prove Theorem 10, we need only show that if $L(x) = C \sqcup D$ is any c.e. splitting of $L(x)$ then there is a representation $\widehat{C} = \{c_i\}$ of x of wtt degree that of C. (Without loss of generality, we suppose that C is noncomputable.) We do this in stages. At each stage s, we assume that we have enumerated C_s and D_s so that $L(a)_s = C_s \sqcup D_s$, where $L(a)_s$ is the collection of rationals in $L(a)$ by stage s, including all those of Gödel number $\leq s$. Additionally we will have a parameter $m(s)$. At stage $s+1$ compute C_{s+1} and D_{s+1}. Find the least rational, $q \in C_{s+1}$, by Gödel number, if any, such that $q > m(s)$.

If no such q exists, set $m(s+1) = m(s)$, and do nothing else.

If one exists, put all rationals with Gödel number below $s+1$, in increasing real order, into $\widehat{C}_{s+1}$ and reset $m(s+1)$ to be the maximum rational (as a real) in $L(x)_{s+1}$.

To verify the construction, first note that $\widehat{C}$ is an increasing sequence of rationals. Its limit will be a provided that it is infinite, because of the use of $m(s)$.

First we claim that $m(s) \to \infty$. Suppose not, so that there is an s such that, for all $t \geq s$, $m(s) = m(t)$. Then we claim that C is computable, this being a contradiction. To decide if $z \in C$, go first to stage $s' = s + g(z)$, where $g(z)$ denotes the Gödel number of z. If $z \notin C_{s'}$, then either $z > m(s)$, or $z \in D_{s'}$. In either case, $z \notin C$. Hence $m(s) \to \infty$.

Note that $\widehat{C} \leq_m C$. Only numbers entering C enter $\widehat{C}$ and can do so only at the same stage. Given q go to a stage s bigger than the Gödel number of q. If q is below $m(s)$ then, as before, we can decide computably if $q \in C$. Else, note that $q \in C$ iff $q \in \widehat{C}$. The same argument shows that $C \leq_m \widehat{C}$. □

We remark that many of the theorems of Calude et. al. [7] now come out as corollaries to the characterization above, and known results on splittings and *wtt* degrees. Notice that by Sacks splitting theorem every noncomputable c.e. real x has representations in infinitely many degrees. From known theorems we get the following.

Corollary 11. *There exist computably enumerable reals a_i such that the collection of T-degrees of representations $R(a_i)$ have the following properties.*

(i) $R(a_1)$ consists of every c.e. (m-) degree

(ii) $R(a_2)$ forms an atomless boolean algebra, which is nowhere dense in the c.e. degrees.

For the proofs see Downey and Stob [24].

We also remark that the above has a number of other consequences regarding known limits to splittings. For instance;

Corollary 12. *If a c.e. real a has representations in each T-degree below that of $L(a)$ then either $L(a)$ is Turing complete or low$_2$.*

This follows since Downey [12] demonstrated that a c.e. degree contains a set with splittings in each c.e. degree below it iff it was complete or low$_2$. It is not clear if every nonzero c.e. degree contains a c.e. real that cannot be represented in every c.e. degree below that of $L(\alpha)$.

5 Presentations of reals

The Calude et. al theorem gave many possible ways of representing reals, not just with Cauchy sequences. We explore the other methods with the following definition.

Definition 3. *Let $A \subset \{0,1\}^*$. We say that A is a* presentation *of a c.e. real x if A is a prefix free c.e. set with*

$$x = \Sigma_{n \in A} 2^{-|n|}.$$

Previously we have seen that x has representations of degree $L(x)$. However, presentations can behave quite differently.

Theorem 13 (Downey and Laforte [17]). *There is a c.e. real α which is not computable, but such that if A presents α then A is computable.*

Proof. We briefly sketch the proof, details being found in Downey and Laforte [17]. We must meet the requirements below.

$$R_e : W_e \text{ presents } \alpha \text{ implies } W_e \text{ computable.}$$

We build a presentation of A, via the nearly c.e. definition. That is, we have an approximation $\alpha = \cdot a_{0,s}...$ and obey the conditions that if $a_{i,s} = 1$ and $a_{i,s+1} = 0$ then $a_{j,s+1}$ becomes 1 for some $j < i$. To make α noncomputable, we must also meet the requirements:

$$P_e : \text{ For some } i,\ i \in W_e \text{ iff } a_i = 1.$$

The strategy for P_e is simple. We must pick some i to follow it, and initially make it 0. At some stage s, if we see i enter W_e, then we must make $a_{i,t} = 1$ for some $t \geq s$.

To make this cohere with the R_e we need a little work. First, we need to surround i with some 0's so that there is little interference from the other requirements, modulo finite injury. However, more importantly, we need to also make sure that for those R_k of higher priority if W_k presents a then W_k is computable.

Associated with R_k will be a current "length of agreement".

$$\ell(k,s) = \min\{s, n : \alpha_s - \Sigma_{\sigma\in W_{k,s}} 2^{-|\sigma|} < 2^{-n}\}.$$

We can assume that $\alpha_s > \Sigma_{\sigma\in W_{k,s}} 2^{-|\sigma|}$ since if a stage t occurs where this is not true, we would have $\alpha_t - \Sigma_{\sigma\in W_{k,t}} 2^{-|\sigma|} > 2^{-d}$ for some d, and simply win by keeping $\alpha_s - \alpha_t < 2^{-(d+2)}$ for all stages $s < t$.

We promise that once $\ell(k,s) > d$, then no number of length $\leq d$ can enter W_k.

Now the idea is that when we see some P_e require attention for e bigger than k, if i is smaller than $m(k,s)$ (the interesting case), then we wish to put a relatively big number into a, by changing position i for the sake of P_e, yet we wish to not allow numbers of low length to enter W_k.

The idea is to slowly work backwards. So first we will make position $\ell(k,s)+1 = 1$ by adding something of length $2^{-(\ell(k,s)+1)}$ into A_{s+1}.

We then do nothing until W_k responds by giving us a stage $t > s$ with $\ell(k,t) \geq \ell(k,s)$.

Note that W_k can only change on strings of long length, since we only changed A slightly. Now we repeat, adding another string of the same length $2^{-(\ell(k,s)+1)}$ into A_{s+1}. Again we wait for another expansion stage. Note that this next addition changes things at position $\ell(k,s)$ or earlier. We can continue in this way at most $2^{\ell(k,s)-i}$ many times till we get to change position i. Note that we will temporarily refrain from declaring that we know W_k for strings of length above $\ell(k,s)$ until a stage t is found where we win P_e. This delay is fine since *if* W_k actually presents α, we will eventually get enough recovery stages that we will meet the P_e.

The reader should think of this as a cautious investor wishing to sell of some shares, but not allowing the market to realize this, so they drip feed the shares into the market each time the price recovers.

Now there are two outcomes. Either at some stage, we don't get recovery, so that W_k does not present A, or W_k responds at each stage and we get a change only on long strings. This means that we can compute W_k.

Now to deal with more than one R_k, say R_k and R_j, with $j < k$ we must use a tree of strategies argument. The strategy for R_k guessing that $\ell(j,s) \not\to \infty$ will be to believe that the current $\ell(j,s)$ is its limit. Thus it believes that W_j will not present α and cannot recover to its previous best length of agreement. This version of R_k acts as in the basic module, but P_e working with this version of R_j must ensure that the total amount they could add to $\alpha - \alpha_s$ is $< 2^{-(\ell(j,s)+2)}$.

The version of R_k guessing that $\ell(j,s) \to \infty$ needs to nest its expansion stages in R_j's. The problem is that R_j can recover at many stages before R_k does. During such stages, we cannot delay allowing R_j to increase $\ell(k,t)$, making the allowable "quanta" even smaller. For suppose that the P_e below both of these versions of R_j and R_k wishes to add 2^{-i} to α_s. We begin this process by adding some quanta 2^{-n} good for both j and k at some stage s_0.

At some stage s_1 we might see R_j recovery, but not have had R_k recovery. We cannot add another 2^{-n} to α_{s_1} until we get this R_k recovery. On the other hand this recovery might not happen. Hence we cannot delay the extension of the definition of W_j to wait for this recovery. Thus we will allow $\ell(j,s)$ to increase, lowering the quanta allowable by R_j. Now at stage s_2, after perhpas many j-expansionary stages we also get R_k recovery. At this stage, R_k would allow us to put in 2^{-n} but now R_j only allows 2^{-m} for some $m >> n$.

The solution is that we won't allow another R_k expansionary stage until we have had enough j-expansionary stages that we could (using increments of 2^{-m}) put in 2^{-n}. During this time we will not allow the definition of W_j to be extended.

The depth d strategies are similar. There are d strategies $S_1, \cdots, S_d$ in decreasing order of priority. At some stage we wish to change α while cooperating with these d strategies. We put some small quanta in. While we are waiting for recovery of *all* the d strategies, we would allow the definitions of their W_{j_d} to change, so for $S_1, \cdots, S_{d-1}$, the allowable quanta will be reduced. At recovery, we might wish to put 2^{-n} into α but this must now be put in in quanta which is acceptable to $S_1, \cdots, S_{d-1}$. While we are doing this we delay any further work on S_d until this is fulfilled. Then, like the tower of Hanoi, the same problem propogates upwards. But the whole process is well-founded so that eventually progress is made. Further details can be found in Downey-Laforte [17]. □

We remark that Downey and Laforte demonstrated that degrees containing such "only computably presentable" reals can be high. But if a degree is promptly simple then every c.e. real of that degree must have a noncomputable c.e. presentation. Using a $\mathbf{0}'''$ argument, Wu [59] has constructed a c.e. noncomputable degree $\mathbf{a} \neq \mathbf{0}$ such that, if α is any c.e. noncomputable real of degree below $\mathbf{a}$ then α has a noncomputable presentation.

As with many structures of computable algebra and the like, the classification of the degrees realized as presentation seems to depend on a stronger reducibility than $\leq_T$. In this case, the relevant reducibility seems to be weak truth table reducibility.

The following is easy.

Theorem 14. *Let α be a computably enumerable real, with $\alpha = .\chi_A$ for some set A. Suppose that B is any presentation of α. Then $B \leq_{wtt} A$ with use function the identity.*

The proof is left as an exercise. What is interesting is that there is a sort of converse to this result.

Theorem 15 (Downey and Laforte [17]). *If A is a presentation of a c.e. real α and $C \leq_{wtt} A$ is computably enumerable, then there is a presentation B of α with $B \equiv_{wtt} C$.*

Proof. Suppose $\Gamma(X)$ is a computable functional with a computable use function γ such that $\Gamma(A) = C$. We can assume γ is monotonically increasing. Let $\langle n, m\rangle : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a computable one-to-one function such that for all n, m, $\max\{n, m\} < \langle n, m\rangle$. (Adding 1 to the usual pairing function gives such a function.) Notice that, since A presents α, using the Chaitin-Kraft theorem we can enumerate strings of any length we wish into $B[s]$ at as long as we ensure

$$\sum_{\sigma \in B[s]} 2^{-|\sigma|} \leq \sum_{\sigma \in A[s]} 2^{-|\sigma|}.$$

We fix enumerations of Γ, C and A so that at each stage s, exactly one element enters C and for every $x < s$, $\Gamma_s(A_s; x) = C_s(x)$. We may assume A is infinite, since there is nothing to prove if A is computable. We construct B in stages, using the function $\langle n, m\rangle$ as follows.

At stage 0, let $B[0] = \emptyset$.

At stage $s + 1$, we first find the unique number n_s entering C and all strings σ that enter A at stage $s + 1$. For each $|\sigma| < \gamma(n_s)$, we enumerate $2^{\langle|\sigma|, n_s\rangle - |\sigma|}$ strings of length $\langle|\sigma|, n_s\rangle$ into $B[s + 1]$. For each $|\sigma| \geq \gamma(n_s)$, we enumerate $2^{\langle|\sigma|, |\sigma|+s\rangle - |\sigma|}$ strings of length $\langle|\sigma|, |\sigma| + s\rangle$ into $B[s]$.

This ends the construction of B.

Notice that all of the actions taken at stage $s + 1$ serve to ensure that

$$\sum_{\sigma \in B[s+1]} 2^{-|\sigma|} = \sum_{\sigma \in A[s+1]} 2^{-|\sigma|};$$

hence, we always have enough strings available to keep B prefix-free.

Suppose $n \in \mathbb{N}$. Let $s(n)$ be least so that $B[s(n)]$ agrees with B on all strings less than or equal to length $\langle\gamma(n), n\rangle$. Now, suppose there exists $t > s(n)$ such that $n \in C[t] - C[t - 1]$. In this case, because for every s and $x < s$, $C(x)[s] = \Gamma(A; x)[s]$, there must be some σ with $|\sigma| < \gamma(n)$ which enters A at t. By construction, then, since $n = n_t$, we have $2^{\langle|\sigma|, n_t\rangle - |\sigma|} > 1$ strings of length $\langle|\sigma|, n_t\rangle$ entering B at stage $t > s(n)$, which is a contradiction. Hence we can compute $C(n)$ from $B(n)$ with a use bounded by the number of strings of length less than or equal to $\langle\gamma(n), n\rangle$, which is a computable function. This gives $C \leq_{wtt} B$.

Next consider any binary string τ. Using the computability of $\langle i, n\rangle$ and the fact that $\max\{i, n\} < \langle i, n\rangle$ we can ask whether there exist i and n such that $|\tau| = \langle i, n\rangle$. If not, then $\tau \notin B$. In this case, let $t(n) = 0$. Otherwise, suppose $|\tau| = \langle i, n\rangle$. If $i \geq \gamma(n)$, then τ can only enter B at stage s if $s = n - i$. If, on the other hand, $i < \gamma(n)$. Then if τ enters B at stage $s + 1$, this can only be because $|\tau| = \langle|\sigma|, n_s\rangle$ for some σ entering A at s, and we enumerate $2^{\langle|\sigma|, n_s\rangle - |\sigma|}$ strings of length $\langle|\sigma|, n_s\rangle$ into $B[s + 1]$. In either case, if we let $t(n)$ be the least number greater than $n - i$ so that $C[t(n)] \upharpoonright_{n+1} = C \upharpoonright_{n+1}$, we have $B(\tau) = B(\tau)[t(n)]$. Since n is computable from $|\tau|$, $B \leq_{wtt} C$, as required. $\square$

Note that one corollary is that a strongly c.e. real $\alpha = .A$ with the degree of A wtt-topped[2], has the property that it has presentations in every T degree below that of A.

Note the following.

Lemma 16. *Suppose that A and B present α. Then there is a presentation of α of wtt degree $A \oplus B$.*

The proof is to note that $C = \{0\sigma : \sigma \in A\} \cup \{1\sigma : \sigma \in B\}$ is prefix free, as both A and B are, and presents α.

It follows that the the wtt-degrees of c.e. sets presenting α forms a Σ^0_3 upper semilattice. Nothing is known about the USL's that can be realized. I would guess that any such USL can be realized.

6 Kolmogorov Complexity

This is a theory of randomness for finite strings. In another section we will look at the infinite case. The main idea is that a string is random if it is "incompressible". That is, the only way to generate the string τ is to essentially hard-wire the string into the algorithm, so that the description of a program to generate τ is essentially the same size as τ itself. (For instance, $0^{10000000}$ can be described by saying that we should repeat 0 10000000 times. This can easily be described by an algorithm shorter than 10000000.)

We formalize this notion, first due to Solomonoff [53], but independently to Kolmogorov and Chaitin, as follows. Let $f : 2^{<\omega} \mapsto 2^{<\omega}$ be a partial computable function. Then we can denote the Kolmogorov complexity of a string σ with respect to f via

$$K_f(\sigma) = \min\{\infty, |p| : f(p) = \sigma\}.$$

Then relative to f, we say that σ is random[3]$K_f(\sigma) \geq |\sigma|$.

We get rid of the dependence of f. If we choose a universal Turing machine U there is a p so that $U(y,p) = f(y)$ for all y, then we can define g via

$$g(0^{|p|}1py) = U(y,p).$$

For this g we see that

$$K_g(x) \leq K_f(x) + \mathcal{O}(1).$$

Note that the constant $\mathcal{O}(1)$ is $2|p|+1$. Hence g is (up to an additive constant), the minimal complexity measure.

Trivial Facts:

(1) $K(x) \leq |x| + \mathcal{O}(1)$.

(2) $K(xx) \leq K(x) + \mathcal{O}(1)$.

---

[2] That is, for all c.e. $B \leq_T A$, $B \leq_{wtt} A$

[3] There are two traditions of notation. One is to use C for Kolmogorov complexity, and K for the prefix-free (disturbingly referred to as prefix complexity) complexity in the next section. The other is to use K for standard Kolmogorov complexity, and to use H for the prefix free complexity of the next section. We adopt the latter and hope that it causes no confusion.

(3) If $h(x)$ is any total computable function, then $K(h(x)) \leq K(x) + \mathcal{O}(1)$.

We would like $K(xy) \leq K(x) + K(y) + \mathcal{O}(1)$. But this is not true. The problem is that we can't decide where x finishes and y starts. We get

(4) $K(xy) \leq K(x) + K(y) + 2\log|x| + \mathcal{O}(1)$.

This uses the "self-delimiting" trick used in the definition of g above for the universal machine. Actually we can replace $2\log|x|$ by $2\log K(x)$.

Theorem 17 (Solomonoff, Kolmogorov). *For all n there exists x with $|x| = n$ and $K(x) \geq n$.*

Proof. Count the number of strings of size n. □

Notice that actually for any k,

$$|\{x \in 2^{<\omega} : K(x) \geq |x| - k\}| \geq 2^n(1 - 2^{-k}).$$

For instance, if $|x| = 1000$, and $k = 500$, then the number of strings of length 1000 that are "half way random" ($K(x) > 500$ is at least $2^{1000}(1-2^{-500})$). That is, almost every string.

Here is a simple application of the "incompressibility method."

How large is the n-th prime? Let m be a binary number and p_j the largest prime divisor of m. To describe m we need only $\langle p_i, \frac{m}{p_i}\rangle$. In fact we need only the pair i, $\frac{m}{p_i}$ $(+\mathcal{O}(1))$. Hence

$$K(m) \leq 2\log|i| + |i| + |\frac{m}{p_i}| + \mathcal{O}(1).$$

The if m is a random number, we see

$$|m| \leq 2\log|i| + |i| + |\frac{m}{p_i}| + \mathcal{O}(1).$$

Hence

$$\log|m| \leq 2\log\log|i| + \log|i| + \log|m| - \log|p_i| + \mathcal{O}(1).$$

Thus

$$\log|p_i| \leq 2\log\log|i| + \log|i| + \mathcal{O}(1).$$

Hence $p_i \leq \mathcal{O}(i\log^2 i)$. This is pretty close to the real answer of $i\log i$.

Another classical application of Kolmogorov complexity is the construction of an immune set. Let

$$A = \{x : K(x) \geq \frac{|x|}{2}\}.$$

Then A is immune. Suppose that A has an infinite c.e. subset C. Let $h(n)$ be defined as the first element of C to occur in its enumeration of length above n. Then

$$K(h(n)) \geq |h(n)|/2 \geq n/2, \text{ but,}$$

$$K(h(n)) \leq K(n) + \mathcal{O}(1) \leq |n| + \mathcal{O}(1).$$

For large enough n this is a contradiction.

I should remark that there is a very well-developed theory of Kolmogorov complexity and its applications. I urge the reader to refer to Li-Vitanyi [41], especially for applications, and to refer to van Lambalgen [58] for a thorough discussion of the foundations of the subject.

7 Prefix-free complexity

The main motivation for this section will be to develop a nice complexity measure for developing complexity on reals. However, Chaitin and Levin argued that prefix-free complexity (the notion we look at here) is the correct complexity even for finite strings.

Their argument for the inadequacy of classical Kolmogorov complexity is the following. The intentional meaning, it is claimed, is that the complexity shortest string ν computing σ, ought to indicate that the *bits* of ν containing all the information necessary to get σ from ν. However, they argue that the universal machine M might first scan ν just to get its length, and only then read the bits of ν. In this way the ν actually represents $|\nu| + \log |\nu|$ many bits of information. If one accepts this argument then one ought to circumvent this. Both Levin [40] and Chaitin [11] suggested prefix free machines to circumvent this.

It has also been pointed out that one can circumvent this by asking that the complexity measure be continuous. This gives rise to the notion of *uniform complexity*, which we will not deal with here. (The uniform complexity of a string $\sigma = a_1 \cdots a_n$ is the minimum length of a string τ such that the universal machine U with oracle τ and argument m computes $a_1 \cdots a_m$ for all $m \leq n$.) We refer the reader to Li-Vitanyi [41] and Barzdin [4] for more details.

A prefix-free machine is one whose domain is prefix-free. It is usual to take the machine as "self delimiting" which means that it has a one way read head which halts when the machine accepts and has accepted the string described by the read head up to its present position. This is a purely technical device that forces the machine to have a prefix free domain.

Facts:

(1) If φ is a partial computable function with prefix free domain, then there is a prefix free (self-delimiting) machine M such that M agrees with φ.

(2) There is a universal (self-delimiting) prefix free machine.

The reader should prove these not altogether obvious results. The reason we want prefix free machines is that we will be looking at reals (eventually) and we wish to apply Kraft's inequality. So the domains will need to be prefix free. Let $H(x)$ denote the prefix free Kolmogorov complexity of x. The counting arguments of the previous section demonstrate that:

$$H(x) \leq |x| + 2\log|x| + \mathcal{O}(1),$$

$$H(x) \leq |x| + H(|x|) + \mathcal{O}(1).$$

We remark that this is tight. A counting argument shows that there are many x with $H(x) > |x| + \log|x|$. (The reader is advised to prove this for themselves[4] . In fact for *finite strings* this would be the typical notion of randomness used if we demanded prefix free complexity.) There is one good trade-off, namely now $H(xy) \leq H(x) + H(y) + \mathcal{O}(1)$. For these and other facts we refer the reader to Li-Vitanyi [41] or Fortnow [25].)

The actual relationships between K and H are

$$H(x) = K(x) + K(K(x)) + \mathcal{O}(K(K(K(x))).$$

$$K(x) = H(x) - H(H(x)) + \mathcal{O}H^3(x).$$

These are due to Solovay in the 1975 manuscript, and are nontrivial.

8 Complexity of reals

Our first attempt to define a random real would be to define $\alpha = .A$ to be random iff there was a constant $\mathcal{O}(1)$ such that, for all n, $K(A \upharpoonright n) + \mathcal{O}(1) > n$. Unfortunately *no* real satisfies this condition. To see this, consider the full binary tree $T = 2^{<\omega}$. We want to make sure that every path is complicated. We will build a machine M that kills every constant k, making sure that every path has complexity above $n - k + c_M$ where c_M is the coding constant of M. To give the idea, let's suppose that $k = 2$ was the only requirement around. Then initially, we could declare that $M(\lambda) = 11$. (Here λ denotes the empty string.) Then we need deal only with strings extending 0 and 10. We use the strings 0 and 1 to deal with the extensions of 10. $M(0) = 100$, $M(1) = 101$. Now we need only deal with strings extending 0. We define $M(\sigma) = 01\sigma$ for all strings σ with $|\sigma| = 2$. Finally, we finish the process by setting $M(\tau) = 00\tau$ for all strings τ of length 3. Now all paths through T are covered. The general case is similar, but tedious and left to the intrepid reader.

However, all problems are removed if we use H in place of K.

Definition 4 (Chaitin). *A real $\alpha = .A$ is Chaitin random if there is an $\mathcal{O}(1)$ such that, for all n*

$$H(A \upharpoonright n) \geq n - \mathcal{O}(1).$$

It can be shown that if

$$K(A \upharpoonright n) \geq n - \mathcal{O}(1) \text{ for } \textit{infinitely many } n,$$

(this being called *Kolmogorov* random) then the real α is Chaitin random. Unfortunately Schnorr [49] proved that the converse does not hold. (It can, however, be shown that the set of languages which are Chaitin random but not Kolmogorov random has measure zero.) There are reals that are K-random but

[4] Suppose that for all x, $H(x) \leq |x| + \log|x|$. Then $\Sigma_{\sigma \in \Sigma^*} 2^{-H(\sigma)} \geq \Sigma_{\sigma \in \Sigma^*} 2^{-(|\sigma| + \log|\sigma|)} \geq \Sigma_n \Sigma_{|\sigma|=n} 2^{-(n+\log n)} \geq \Sigma_n 2^n (2^{-(n+\log n)}) \geq \Sigma_n 1/n = \infty$, a contradiction, since $\Sigma_\sigma 2^{-H(\sigma)} < 1$.

not Chaitin random. Before we prove the existence of such a real, we look at other (and earlier) topological views of randomness.

The main idea is that a real would be random iff it had no rare properties. Using measure theory, this translates as no "effectively null" properties.

We define c.e. open set to be a c.e. collection of open rational intervals. The first guess one might make for a random real is that

"a real x is random iff for all computable collections of c.e. open sets $\{U_n : n \in \omega\}$, with $\mu(U_n) \to 0$, $x \notin \cap_n U_n$."

This is a very strong definition, and is stronger than the most commonly accepted version of randomness. Let's call this *strong randomness*. The key is that we wish to avoid all "effectively null" sets. Surely an effectively null set would be one where the measures went to zero in some computable way. Such considerations lead to the definition of Martin-Löf randomness below.

Definition 5 (Martin-Löf, [44]). *We say that a real is* Martin-Löf random *or 1-*random *iff for all computable collections of c.e. open sets $\{U_n : n \in \omega\}$, with $\mu(U_n) \leq 2^{-n}$, $x \notin \cap_n U_n$.*

We call aa computable collection of c.e. open sets a *test*, and ones with $\mu(U_n) \leq 2^{-n}$ for all n, a Martin-Löf test. The usual terminology is to say that a real is Martin-Löf random if it passes all Martin-Löf tests. Of course a real passes the test if it is not in the intersection.

We remark that while strong randomness clearly implies Martin-Löf randomness, the converse if not true. This is an observation of Solovay. Later we show that there are c.e. reals that are Martin-Löf random. Hence the inequivalence of strong randomness and Martin-Löf randomness will follow by showing that no strong random real is c.e.. The following proof of this observation is due to Martin (unpublished).

Let $\alpha = \lim_s q_s$ as usual, and define

$$U_n = \{y : \exists s \geq n[y \in (q_n, q_n + 2(q_s - q_n))]\}.$$

Then $\mu(U_n) \to 0$, yet $\alpha \in \cap_n U_n$. (Actually this shows that α cannot even be Δ^0_2.)

In a famous unpublished manuscript, Solovay proposed a alternative notion of randomness.

Definition 6 (Solovay [54]). *We say that a real x is* Solovay random *iff for all computable collections of c.e. $\{U_n : n \in \omega\}$ such that $\Sigma_n \mu(U_n) < \infty$, x is in only finitely many U_i.*

The reader should note the following alternative version of Definition 6.

A real is Solovay random iff for all computably enumerable collections of rational intervals $I_n : n \in \omega$, if $\Sigma_n |I_n| < \infty$, then $x \in I_n$ for at most finitely many n.

Again, we can define a Solovay test as a collection of rational intervals $\{I_i : i \in \omega\}$, with $\sum_i I_i < \infty$. Then a real is Solovay random iff it passes every Solovay test, meaning that it is in only finitely many I_i. Clearly if x is Solovay random, then it is Martin-Löf random. The converse also holds.

Theorem 18 (Solovay [54]). *A real x is Martin-Löf random iff x is Solovay random.*

Proof. Suppose that x is Martin-Löf random. Let $\{U_n\}$ be a computable collection of c.e. open sets with $\Sigma_n \mu(U_n) < \infty$. We can suppose, by leaving some out, that $\Sigma_n \mu(U_n) < 1$. Define a c.e. open set

$$V_k = \{y \in (0,1) : y \in U_n \text{ for at least } 2^k\ U_n\}.$$

Then $\mu(V_k) \leq 2^{-k}$ and hence as x is Martin-Löf random, $x \notin \cap_n V_n$, giving the result. $\square$

It is also true that Chaitin random is equivalent to Martin-Löf random.

Theorem 19 (Schnorr). *A real x is Chaitin random iff it is Martin-Löf random.*

Proof. $(\rightarrow)$ Suppose that x is Martin-Löf random. Let

$$U_k = \{y : \exists n H(y \upharpoonright n) \leq n - k\}.$$

Recall that there is a C such that (for a fixed n),

$$\mu(\{y : H(y \upharpoonright n) \leq H(n) + n - k\}) \leq C 2^{-k},$$

and hence

$$\mu(\{y : H(y \upharpoonright n) \leq n - k\} \leq C 2^{-H(n) - k}$$

Now we can estimate the size of U_k:

$$\mu(U_k) \leq C 2^{-k} (\Sigma_{n=1}^{\infty} 2^{-H(n)}) \leq 2^{-k}.$$

Hence the sets $\{U_k : k \in \omega\}$ form a Martin-Löf test, and if x is Martin-Löf random $x \notin \cap_n U_n$. Thus there is a k such that, for all n, $H(x \upharpoonright n) > n - k$. $\square$

The other direction of the proof is more difficult, and the most elegant proof known to the author is the one of Chaitin [11]. This approach is slightly more abstract since it is *axiomatic* and and stresses the *minimality* of H as a measure of complexity. It is thus of interest in its own right.

Specifically, Chaitin defined a *information content measure* as any function $\widehat{H}$ such that

$$\Omega_{\widehat{H}} = \Sigma_{\sigma \in 2^{<\omega}} 2^{-\widehat{H}(\sigma)} < 1, \text{ and,}$$

$$\{\langle \sigma, k \rangle : \widehat{H}(\sigma) \leq k\} \text{ is c.e..}$$

Naturally one can enumerate the information content measures $\{H_k : k \in \omega\}$[5] and then defines

$$H(x) = \min_{k \geq 0} \{H_k(x) + k + 1\}.$$

[5]It is easy to spot when the measure threatens to exceed 1, at which point one would stop enumerating a bad M_k.

Notice that by the universal Turing machine, $\{\langle\sigma, k\rangle : H(\sigma) \leq k\}$ is c.e.. Furthermore,

$$\Sigma_\sigma 2^{-H(\sigma)} = \Sigma_{k\geq 1} 2^{-k}(\Sigma_\sigma 2^{-H_k(\sigma))} < 1.$$

Notice that therefore for any information content measure

$$H(\sigma) \leq H_k(\sigma) + \mathcal{O}(1).$$

Thus we see that (of course) H is the prefix free Kolmogorov complexity, and this information content measure is minimal among all such measures. Before we turn to the proof of the other direction of Schnorr's theorem, here's one application of this idea. We prove that

$$H(x) \leq |x| + H(|x|) + \mathcal{O}(1).$$

This result was mentioned before, but we only alluded to a proof suggesting that it was merely a counting argument. Here's Chaitin's proof.

$$1 > \Omega = \Sigma_{x\in 2^{<\omega}} 2^{-H(x)} = \Sigma_{n\in\mathbb{N}}[2^{-n}\Sigma_{|x|=n} 2^{-H(x)}], \text{ (that same trick)},$$

$$= \Sigma_n \Sigma_{|x|=n} 2^{-(n+H(x))} = \Sigma_{x\in 2^{<\omega}} 2^{-(|x|+H(|x|))}.$$

Thus $H(x) \leq |x| + H(|x|) + \mathcal{O}(1)$, as H is minimal.

The reader should think of proofs like this as using the minimality of H to avoid explicit mention of Kraft-Chaitin. Now to the proof of Schnorr's Theorem:

Proof. (cont'd) This time suppose that x is not Martin-Löf random. We prove that x is not Chaitin random. Thus we have $\{U_n\}$ with $x \in \cap U_n$ and $\mu(U_n) \leq 2^{-n}$. We note that $\Sigma_n 2^{-n^2+n}$ converges, and indeed, $\Sigma_{n\geq 3} 2^{-n^2+n} < 1$. Notice that

$$\Sigma_{n\geq 3}\Sigma_{\sigma\in U_{n^2}} 2^{-(|\sigma|-n)} \leq \Sigma_{n\geq 3} 2^n \mu(U_{n^2}) \leq \Sigma_{n\geq 3} 2^{-n^2+n} < 1.$$

Thus by the minimality of H, $\sigma \in U_{n^2}$ and $n \geq 3$ implies that $H(\sigma) \leq |\sigma| - n + \mathcal{O}(1)$. Therefore, as $x \in \cap U_{n^2}$ for all $n \geq 3$ we see that $H(x \upharpoonright k) \leq k - n + \mathcal{O}(1)$, and hence it drops arbitrarily away from k. Hence, x is not Chaitin random. $\square$

If the reader wished to reinstate Kraft-Chaitin here, then the argument above is roughly the following. Since $x \in U_{n^2}$ (or any reasonable function of n, $2n$ would probably be enough), since the measure is small ($< 2^{-n^2}$), we can use Kraft-Chaitin to enumerate a machine which maps strings of length $k - n$ to initial segments of length k of strings in U_{n^2}. Specifically, as we see strings σ with $I(\sigma) \in U_{n^2}$ and length at least n^2, then we could enumerate a requirement $|\sigma| - k, \sigma$. (The total measure will be bounded by 1 and hence Kraft-Chaitin applies.)

9 Relative randomness

We wish to look at reals, especially c.e. reals under notions of relative randomness. Ultimately, we would seek to understand $\leq_H$ and $\leq_K$ reducibilities, for instance, where for $E = H$ or K, we have

$$\alpha \leq_E \beta \text{ iff } \forall n[E(\alpha \upharpoonright n) \leq E(\beta \upharpoonright n) + \mathcal{O}(1)].$$

There are a number of natural reducibilities which imply $\leq_E$. One was introduced by Solovay, and some are more recent. In this section we will look at some recent material on such reducibilities.

Definition 7 (Solovay [54]). *We say that a real α is Solovay reducible to β (or β dominates α), $\alpha \leq_S \beta$ iff there is a constant c and a partial computable function f, so that for all $q \in \mathbb{Q}$, with $q < \beta$,*

$$c(\beta - q) > \alpha - f(q).$$

The intuition is that a sequence of rationals converging to β can be used to generate one converging to α at the same rate. The point is that if we have a c.e. sequence $\{q_n : n \in \omega\}$ of rationals converging to β then we know that $f(q_n)\downarrow$. Notice that if $r_n \to \alpha$ then for all m there is some k such that $\alpha > r_k > f(q_m)$. (The reals are not rational.) Noticing this yields the following characterization of Solovay reducibility.

Lemma 20 (Calude et. al. [7]). *For c.e. reals, $\alpha \leq_S \beta$ iff for all c.e. $q_i \to \beta$ there exists a total computable g, and a constant c, such that, for all m,*

$$c(\beta - q_m) > \alpha - r_{g(m)}.$$

Another characterization of $\leq_S$ is the following:

Theorem 21 (Downey, Hirschfeldt, Nies [15]). *For c.e. reals, $\alpha \leq_S \beta$ iff for all c.e. sequences $\{q_i : i \in \omega\}$ such that $\beta = \Sigma_i q_i$, there is a computable function $\epsilon : \omega \mapsto [0,1]$ and a constant c, such that,*

$$\alpha = c(\Sigma_i \epsilon(i) q_i).$$

Hence $\alpha \leq_S \beta$, iff there exists a c and a c.e. real γ such that

$$c\beta = \alpha + \gamma.$$

Proof. (if) One direction is easy. Suppose that c and ϵ exist. Notice that

$$c(\beta - \Sigma_{i=1}^n q_i) > \alpha - \Sigma_{i=1}^n \epsilon(i) q_i.$$

Hence $\alpha \leq_S \beta$. $\square$

For the other direction, we need the following Lemmas. The first is inplicit in Solovay's manuscript, but is first proven in [20].

Lemma 22. *Let α and β be c.e. reals, and let $\alpha_0, \alpha_1, \dots$ and $\beta_0, \beta_1, \dots$ be computable increasing sequences of rationals converging to α and β, respectively. Then $\beta \leq_S \alpha$ if and only if there are a constant d and a total computable function f such that for all $n \in \omega$,*

$$\beta - \beta_{f(n)} < d(\alpha - \alpha_n).$$

The proof is straightforward and is left as an exercise.

Lemma 23 (Downey, Hirschfeldt, Nies [15]). *Let $\beta \leq_S \alpha$ be c.e. reals and let $\alpha_0, \alpha_1, \dots$ be a computable increasing sequence of rationals converging to α. There is a computable increasing sequence $\hat{\beta}_0, \hat{\beta}_1, \dots$ of rationals converging to β such that for some constant c and all $s \in \omega$,*

$$\hat{\beta}_s - \hat{\beta}_{s-1} < c(\alpha_s - \alpha_{s-1}).$$

Proof. Fix a computable increasing sequence $\beta_0, \beta_1, \dots$ of rationals converging to β, let d and f be as in Lemma 22, and let $c > d$ be such that $\beta_{f(0)} < c\alpha_0$. We may assume without loss of generality that f is increasing. Define $\hat{\beta}_0 = \beta_{f(0)}$.

There must be an $s_0 > 0$ for which $\beta_{f(s_0)} - \beta_{f(0)} < d(\alpha_{s_0} - \alpha_0)$, since otherwise we would have

$$\beta - \beta_{f(0)} = \lim_s \beta_{f(s)} - \beta_{f(0)} \geq \lim_s d(\alpha_s - \alpha_0) = d(\alpha - \alpha_0),$$

contradicting our choice of d and f. It is now easy to define $\hat{\beta}_1, \dots, \hat{\beta}_{s_0}$ so that $\hat{\beta}_0 < \dots < \hat{\beta}_{s_0} = \beta_{f(s_0)}$ and $\hat{\beta}_s - \hat{\beta}_{s-1} \leq d(\alpha_s - \alpha_{s-1}) < c(\alpha_s - \alpha_{s-1})$ for all $s \leq s_0$. For example, if we let μ the minimum value of $d(\alpha_s - \alpha_{s-1})$ for $s \leq s_0$ and let t be least such that $\hat{\beta}_0 + d(\alpha_t - \alpha_0) < \beta_{f(s_0)} - 2^{-t}\mu$ then we can define

$$\hat{\beta}_{s+1} = \begin{cases} \hat{\beta}_s + d(\alpha_{s+1} - \alpha_s) & \text{if } s+1 < t \\ \beta_{f(s_0)} - 2^{-(s+1)}\mu & \text{if } t \leq s+1 < s_0 \\ \beta_{f(s_0)} & \text{if } s+1 = s_0. \end{cases}$$

We can repeat the procedure in the previous paragraph with s_0 in place of 0 to obtain an $s_1 > s_0$ and $\hat{\beta}_{s_0+1}, \dots, \hat{\beta}_{s_1}$ such that $\hat{\beta}_{s_0} < \dots < \hat{\beta}_{s_1} = \beta_{f(s_1)}$ and $\hat{\beta}_s - \hat{\beta}_{s-1} < c(\alpha_s - \alpha_{s-1})$ for all $s_0 < s \leq s_1$.

Proceeding by recursion in this way, we define a computable increasing sequence $\hat{\beta}_0, \hat{\beta}_1, \dots$ of rationals with the desired properties. □

We are now in a position to prove Lemma 21 for the other direction.

Proof. Suppose that $\beta \leq_S \alpha$. Given a computable sequence of rationals $a_0, a_1, \dots$ such that $\alpha = \sum_{n \in \omega} a_n$, let $\alpha_n = \sum_{i \leq n} a_i$ and apply Lemma 23 to obtain c and $\hat{\beta}_0, \hat{\beta}_1, \dots$ as in that lemma. Define $\varepsilon_n = (\hat{\beta}_n - \hat{\beta}_{n-1})a_n^{-1}$. Now $\sum_{n \in \omega} \varepsilon_n a_n = \sum_{n \in \omega} \hat{\beta}_n - \hat{\beta}_{n-1} = \beta$, and for all $n \in \omega$,

$$\varepsilon_n = (\hat{\beta}_n - \hat{\beta}_{n-1})a_n^{-1} = (\hat{\beta}_n - \hat{\beta}_{n-1})(\alpha_n - \alpha_{n-1})^{-1} < c.$$

□

What has this to do with Kolmogorov complexity? The following lemma of Solovay is the decisive fact we use for this (and other) reducibilities.

Lemma 24 (Solovay). *For all k there is a constant c_k depending on k alone, such that for all n, $|\sigma| = |\tau| = n$ and $|\sigma - \tau| < 2^{k-n}$, then for $E = H$ or K,*

$$E(\sigma) \leq E(\tau) + c_k.$$

Proof. Here is the argument for K. We can write a program depending on k which, when given σ, reads the length of σ then computes the ν such that ν has the same length as σ and $|\sigma - \nu| < 2^{k-n}$. Then, given a program for σ, all we need to generate τ is to use the program for the ν's and compute which ν is τ on the list. This is nonuniform, but only needs about $\log k$ many bits since the size of the list depends on k alone.

The argument for H is similar. Suppose that we have a prefix free M. When we see some ν with $M(\nu) = \sigma$, then we can enumerate a requirement $|\nu| + 2^{k+1}, \tau$ for each of the 2^k τ with $|\sigma - \tau| < 2^{k-n}$. Now apply Kraft-Chaitin. □

Now we use Lemma 24 to relate Solovay reducibility to complexity.

Theorem 25 (Solovay). *Suppose that $\alpha \leq_S \beta$. Then for $E = H$ or K, $\alpha \leq_E \beta$.*

Proof. Suppose that $\alpha \leq_S \beta$ via $c < 2^k$, f. Notice that

$$\alpha - f(\beta \upharpoonright (n+1)) < 2^k(\beta - \beta \upharpoonright (n+1)).$$

In particular,

$$\alpha \upharpoonright n - f(\beta \upharpoonright (n+1)) \upharpoonright n < 2^{k-n},$$

and we can apply Lemma 24. □

It is natural to try to understand the nature of Solovay reducibility on the c.e. reals and how precisely it relates to $\leq_H$ and $\leq_K$.

First Solovay noted that Ω was Solovay complete. (Be aware that this means for all c.e. *reals* (not just c.e. *sets*) α, $\alpha \leq_S \Omega$. This is obvious from the definition. Furthermore if $\Omega \leq_S \alpha$, for any (not necessarily c.e.) real α then α must be random. This follows by the Chaitin definition of randomness and by Theorem 25. Finally Kučera and Slaman showed that domination provides a precise characterization of randomness.

Theorem 26 (Kučera and Slaman [37]). *Suppose that α is random and c.e.. Then for all c.e. reals β, $\beta \leq_S \alpha$.*

Proof. Suppose that α is random and β is a c.e. real. We need to show that $\beta \leq_S \alpha$. We enumerate a Martin-Löf test $F_n : n \in \omega$ in stages. Let $\alpha_s \to \alpha$ and $\beta_s \to \beta$ computably and monotonically. We assume that $\beta_s < \beta_{s+1}$. At stage s if $\alpha_s \in F_n^s$, do nothing, else put $(\alpha_s, \alpha_s + 2^{-n}(\beta_{s+1} - \beta_s))$ into F_n^{s+1}. One verifies that $\mu(F_n) < 2^{-n}$. Thus the F_n define a Martin-Löf test. As α is random, there is a n such that for all $m \geq n$, $\alpha \notin F_m$. This shows that $\beta \leq_S \alpha$ with constant 2^{-n}. □

So we see that Solovay reducibility is good with respect to randomness. Notice that Kučera and Slaman's theorem says something very strong. Consider a random c.e. real x. Then for e.g. H, we know that

$$H(x \upharpoonright n) \geq n + \mathcal{O}(1).$$

However we also know that

$$H(\sigma) \leq |\sigma| + 2\log(|\sigma|) + \mathcal{O}(1).$$

It would seem that there could be random y where withinfinitely many n where $x \upharpoonright n$ had H-complexity $n + \log n$, yet y had H-complexity n. Why not? After all the the complexity only needs to be above n to "qualify" as random, and it certainly can be as large as $n + \log n$.

However, Kučera and Slaman's theorem says that this is not *so. All random c.e. reals have "high" complexity (like $n + \log n$) and low complexity (like n) at the same n's!* Similarly, for K, a real x is random iff

$$K(x \upharpoonright n) \geq n + \mathcal{O}(1)$$

infinitely often. This definition is enough to guarantee that the reals have the same K-complexity for all n, a remarkable fact.

Before we turn to the structure of the Solovay degrees of c.e. reals, we mention that we know of no characterization of this (or any of the other reducibilities we examine) in terms of *test sets*. What we are thinking here is that $\alpha \leq \beta$ iff every test failed by β is failed by α, or something. This, of course is not correct since α and β will no doubt be different rational intervals. But there should be some computable map, perhaps from test sets to test sets, like an m-reduction which will be along these lines.

10 The structure of Solovay degrees of c.e. reals.

Despite the many attractive features of the Solovay degrees of c.e. reals, their structure is largely unknown. Recently progress has been made.

Theorem 27 (Downey, Hirschfeldt and Nies [15]). *The Solovay degrees of c.e. reals*

(i) forms a distributive upper semilattice, where the operation of join is induced by $+$, arithmetic addition (or multiplication) (namely $[x] \vee [y] \equiv_S [x+y]$.)

(ii) is dense,

(iii) If $\mathbf{a}$ is incomplete and $\mathbf{b} <_S \mathbf{a}$, then there exist $\mathbf{a_1} |_\mathbf{S} \mathbf{a_2}$ such that $\mathbf{b} < \mathbf{a_1}, \mathbf{a_2}$, and $\mathbf{a} = \mathbf{a_1} \vee \mathbf{a_2}$. That is every incomplete degree splits over all lesser ones.

(iv) If $[\Omega] = \mathbf{a} \vee \mathbf{b}$ *then either* $[\Omega] = \mathbf{a}$ *or* $[\Omega] = \mathbf{b}$.

Proof. We will sketch the proof of some of the above. We begin with (i). We will be applying Theorem 21, but for convenience will write ϵ_i instead of $\epsilon(i)$.

Suppose that $\beta \leq_S \alpha_0 + \alpha_1$. Let $a_0^0, a_1^0, \dots$ and $a_0^1, a_1^1, \dots$ be computable sequences of rationals such that $\alpha_i = \sum_{n \in \omega} a_n^i$ for $i = 0, 1$. By Lemma 21, there are a constant c and a computable sequence of rationals $\varepsilon_0, \varepsilon_1, \dots < c$ such that $\beta = \sum_{n \in \omega} \varepsilon_n (a_n^0 + a_n^1)$. Let $\beta_i = \sum_{n \in \omega} \varepsilon_n a_n^i$. Then $\beta = \beta_0 + \beta_1$ and, again by Lemma 21, $\beta_i \leq_S \alpha_i$ for $i = 0, 1$. This establishes distributivity.

To see that the join in the Solovay degrees is given by addition, we again apply Lemma 21. Certainly, for any c.e. reals β_0 and β_1 we have $\beta_i \leq_S \beta_0 + \beta_1$ for $i = 0, 1$, and hence $[\beta_0 + \beta_1] \geq_S [\beta_0], [\beta_1]$. Conversely, suppose that $\beta_0, \beta_1 \leq \alpha$. Let $a_0, a_1, \dots$ be a computable sequence of rationals such that $\alpha = \sum_{n \in \omega} a_n$. For each $i = 0, 1$ there is a constant c_i and a computable sequence of rationals $\varepsilon_0^i, \varepsilon_1^i, \dots < c_i$ such that $\beta_i = \sum_{n \in \omega} \varepsilon_n^i a_n$. Thus $\beta_0 + \beta_1 = \sum_{n \in \omega} (\varepsilon_n^0 + \varepsilon_n^1) a_n$. Since each $\varepsilon_n^0 + \varepsilon_n^1$ is less than $c_0 + c_1$, a final application of Lemma 21 shows that $\beta_0 + \beta_1 \leq_S \alpha$. Multiplication is similar.

Now we turn to the density properties. The proof that if $\alpha <_S \Omega$ then there is a β with $\alpha <_S \beta <_S \Omega$ is a relatively straightforward finite injury argument, based especially on the fact that we don't need to actually build the reduction $\beta \leq \Omega$. We omit this proof. The argument every incomplete degree splits over all lesser ones has some novel features.

We will prove the following.

Let $\gamma <_S \alpha <_S \Omega$. There are β^0 and β^1 s.t. $\gamma <_S \beta^0, \beta^1 <_S \alpha$ and $\beta^0 + \beta^1 = \alpha$.

Recall: $\alpha \leq_S \beta$ iff there are a computable f and a constant d such that $\alpha - \alpha_{f(n)} < d(\beta - \beta_n)$ for all n.

We want to build β^0 and β^1 such that

- $\beta^0, \beta^1 \leq_S \alpha$,
- $\beta^0 + \beta^1 = \alpha$, and
- the following requirement is satisfied for each $e, k \in \omega$ and $i < 2$:

$$R_{i,e,k} : \Phi_e \text{ total} \Rightarrow \exists n (\alpha - \alpha_{\Phi_e(n)} \geq k(\beta^i - \beta_n^i)).$$

The argument is finite injury, however, there are several problems with the implementation. It suffices to discuss a two-requirement scenario.

- $R_0 : \Phi \text{ total } \Rightarrow \exists n (\alpha - \alpha_{\Phi(n)} \geq k(\beta^0 - \beta_n^0))$
- $R_1 : \Psi \text{ total } \Rightarrow \exists n (\alpha - \alpha_{\Psi(n)} \geq l(\beta^1 - \beta_n^1))$

Naturally, we will be measuring whether Φ and Ψ are total and only work when this appears so. Thus, without loss of generality, we will assume that Φ and Ψ are total. The reader should imagine the construction as follows. There are

- two containers, labeled β^0 and β^1, and
- a large funnel, through which bits of α are being poured.

As with any priority argument, R_0 and R_1 fight for control of the funnel. In particular, bits of α must go into the containers (because we want $\beta^0+\beta^1=\alpha$) at the same rate as they go into α (because we want $\beta^0, \beta^1 \leq_S \alpha$). However, each R_i wants to funnel enough of α into β^{1-i} to be satisfied.

As R_0 is stronger, it could potentially put all of α into β^1, but that would leave R_1 unsatisfied. The trouble comes from trying to recognize when enough of α has been put into β^1 so that R_0 is satisfied.

Definition 8. *R_0 is* satisfied through n at stage s *if $\Phi(n)[s]\downarrow$ and $\alpha_s - \alpha_{\Phi(n)} > k(\beta^0_s - \beta^0_n)$.*

To achieve satisfaction, the idea is that R_0 sets a quota for R_1 (how much may be funneled into β^0 from that point on). If the quota is 2^{-m} and R_0 finds that either

- it is unsatisfied or
- the least number through which it is satisfied changes,

then it sets a new quota of $2^{-(m+1)}$ for how much may be funneled into β^0 from that point on.

Lemma 28. *There is an n through which R_0 is eventually permanently satisfied, that is,*

$$\exists n, s\ \forall t > s\ (\alpha_t - \alpha_{\Phi(n)} > k(\beta^0_t - \beta^0_n)).$$

Proof. (of Lemma) Suppose not. Then R_1's quota $\to 0$, so β^0 is computable. Also, $\forall n, s\, \exists t > s\, [\alpha_t - \alpha_{\Phi(n)} \leq k(\beta^0_t - \beta^0_n)]$. So $\forall n\, [\alpha - \alpha_{\Phi(n)} < (k+1)(\beta^0 - \beta^0_n)]$. Thus $\alpha \leq_S \beta^0$ is computable. Contradiction. $\square$

Thus the strategy above yields a method for meeting R_0. At the end of this process, R_0 is permanently satisfied, and R_1 has a final quota 2^{-m} that it is allowed to put into β^0.

Now we hit the crucial problem, precisely where we need incompleteness for α. If R_1 waits until a stage s s.t. $\alpha - \alpha_s < 2^{-m}$ then it can put all of $\alpha - \alpha_s$ into β^0 and t will, in turn, be satisfied.

The problem is that R_1 *cannot tell when such an s arrives.* If R_1 jumps the gun, it may find itself unsatisfied and unable to do anything about it since it will have used all of its quota *before* s arrives.

The key new idea is that

R_1 uses Ω as an investment advisor.

Let s be the stage at which R_1's final quota of 2^{-m} is set. At each stage $t \geq s$, R_1 puts as much of $\alpha_{t+1} - \alpha_t$ into β^0 as possible so that the total amount put into β^0 since stage s *does not exceed* $2^{-m}\Omega_t$. The total amount put into β^0 after stage s is $\leq 2^{-m}\Omega < 2^{-m}$, so the quota is respected. We finish the proof with the following Lemma

Lemma 29. *There is a stage t after which R_1 is allowed to funnel all of $\alpha - \alpha_t$ into β^0.*

Proof. It is enough that $\exists u \geq t \geq s\ \forall v > u\ (2^{-m}(\Omega_v - \Omega_t) \geq \alpha_v - \alpha_t)$. Suppose not. Then $\forall u \geq t \geq s\ \exists v > u\ [\Omega_v - \Omega_t < 2^m(\alpha_v - \alpha_t)]$. Thus $\forall t \geq s\ [\Omega - \Omega_t \leq 2^m(\alpha - \alpha_t)]$. So there is a d s.t. $\forall t\ [\Omega - \Omega_t < d(\alpha - \alpha_t)]$, and hence $\Omega \leq_S \alpha$. Contradiction. $\square$

Finally, we turn to the last part of the theorem. That is, we wish to prove that

If α and β are c.e. reals and $\alpha + \beta$ is random then at least one of α and β is random.

This fact will follow easily from a stronger result which shows that, despite the upwards density of the Solovay degrees, there is a sense in which the complete Solovay degree is very much above all other Solovay degrees. We begin by noting the following lemma, which gives a useful sufficient condition for domination.

Lemma 30 (Downey, Hirschfeldt, Nies [15]). *Let f be an increasing total computable function and let $k > 0$ be a natural number. Let α and β be c.e. reals for which there are infinitely many $s \in \omega$ such that $k(\alpha - \alpha_s) > \beta - \beta_{f(s)}$, but only finitely many $s \in \omega$ such that $k(\alpha_t - \alpha_s) > \beta_{f(t)} - \beta_{f(s)}$ for all $t > s$. Then $\beta \leq_S \alpha$.*

Proof. By taking $\beta_{f(0)}, \beta_{f(1)}, \ldots$ instead of $\beta_0, \beta_1, \ldots$ as an approximating sequence for β, we may assume that f is the identity.

By hypothesis, there is an $r \in \omega$ such that for all $s > r$ there is a $t > s$ with $k(\alpha_t - \alpha_s) \leq \beta_t - \beta_s$. Furthermore, there is an $s_0 > r$ such that $k(\alpha - \alpha_{s_0}) > \beta - \beta_{s_0}$. Given s_i, let s_{i+1} be the least number greater than s_i such that $k(\alpha_{s_{i+1}} - \alpha_{s_i}) \leq \beta_{s_{i+1}} - \beta_{s_i}$.

Assuming by induction that $k(\alpha - \alpha_{s_i}) > \beta - \beta_{s_i}$, we have

$$k(\alpha - \alpha_{s_{i+1}}) = k(\alpha - \alpha_{s_i}) - k(\alpha_{s_{i+1}} - \alpha_{s_i}) > \beta - \beta_{s_i} - (\beta_{s_{i+1}} - \beta_{s_i}) = \beta - \beta_{s_{i+1}}.$$

Thus $s_0 < s_1 < \cdots$ is a computable sequence such that $k(\alpha - \alpha_{s_i}) > \beta - \beta_{s_i}$ for all $i \in \omega$.

Now define the computable function g by letting $g(n)$ be the least s_i that is greater than or equal to n. Then $\beta - \beta_{g(n)} < k(\alpha - \alpha_{g(n)}) \leq k(\alpha - \alpha_n)$ for all $n \in \omega$, and hence $\beta \leq_S \alpha$. $\square$

We finish the proof of Theorem 27 (iv) by establishing the following.

Theorem 31 (Downey, Hirschfeldt, Nies [15]). *Let α and β be c.e. reals, let f be an increasing total computable function, and let $k > 0$ be a natural number. If β is random and there are infinitely many $s \in \omega$ such that $k(\alpha - \alpha_s) > \beta - \beta_{f(s)}$ then α is random.*

Proof. (sketch) By taking $\beta_{f(0)}, \beta_{f(1)}, \ldots$ instead of $\beta_0, \beta_1, \ldots$ as an approximating sequence for β, we may assume that f is the identity. If α is rational then we can replace it with a nonrational computable real α' such that $\alpha' - \alpha'_s \geq \alpha - \alpha_s$ for all $s \in \omega$, so we may assume that α is not rational.

We assume that α is nonrandom and there are infinitely many $s \in \omega$ such that $k(\alpha - \alpha_s) > \beta - \beta_s$, and show that β is nonrandom. The idea is to take a Solovay test $A = \{I_i : i \in \omega\}$ such that $\alpha \in I_i$ for infinitely many $i \in \omega$ and use it to build a Solovay test $B = \{J_i : i \in \omega\}$ such that $\beta \in J_i$ for infinitely many $i \in \omega$.

Let

$$U = \{s \in \omega : k(\alpha - \alpha_s) > \beta - \beta_s\} \ .$$

It is not hard to show that U is Δ^0_2, except in the trivial case in which $\beta \equiv_S \alpha$. Thus a first attempt at building B could be to run the following procedure for all $i \in \omega$ in parallel. Look for the least t such that there is an $s < t$ with $s \in U[t]$ and $\alpha_s \in I_i$. If there is more than one number s with this property then choose the least among such numbers. Begin to add the intervals

$$[\beta_s, \beta_s + k(\alpha_{s+1} - \alpha_s)], [\beta_s + k(\alpha_{s+1} - \alpha_s), \beta_s + k(\alpha_{s+2} - \alpha_s)], \ldots \qquad (1)$$

to B, continuing to do so as long as s remains in U and the approximation of α remains in I_i. If the approximation of α leaves I_i then end the procedure. If s leaves U, say at stage u, then repeat the procedure (only considering $t \geq u$, of course).

If $\alpha \in I_i$ then the variable s in the above procedure eventually assumes a value in U. For this value, $k(\alpha - \alpha_s) > \beta - \beta_s$, from which it follows that $k(\alpha_u - \alpha_s) > \beta - \beta_s$ for some $u > s$, and hence that $\beta \in [\beta_s, \beta_s + k(\alpha_u - \alpha_s)]$. So β must be in one of the intervals (1) added to B by the above procedure.

Since α is in infinitely many of the I_i, running the above procedure for all $i \in \omega$ guarantees that β is in infinitely many of the intervals in B. The problem is that we also need the sum of the lengths of the intervals in B to be finite, and the above procedure gives no control over this sum, since it could easily be the case that we start working with some s, see it leave U at some stage t (at which point we have already added to B intervals whose lengths add up to $\alpha_{t-1} - \alpha_s$), and then find that the next s with which we have to work is much smaller than t. Since this could happen many times for each $i \in \omega$, we would have no bound on the sum of the lengths of the intervals in B.

This problem would be solved if we had an infinite computable subset T of U. For each I_i, we could look for an $s \in T$ such that $\alpha_s \in I_i$, and then begin to add the intervals (1) to B, continuing to do so as long as the approximation of α remained in I_i. (Of course, in this easy setting, we could also simply add the single interval $[\beta_s, \beta_s + k \text{ card}\{I\}]$ to B.) It is not hard to check that this would guarantee that if $\alpha \in I_i$ then β is in one of the intervals added to B, while also ensuring that the sum of the lengths of these intervals is less than or equal to $k \text{ card}\{I_i\}$. Following this procedure for all $i \in \omega$ would give us the desired Solovay test B. Unless $\beta \leq_S \alpha$, however, there is no infinite computable $T \subseteq U$, so we use Lemma 30 to obtain the next best thing.

Let
$$S = \{s \in \omega : \forall t > s(k(\alpha_t - \alpha_s) > \beta_t - \beta_s)\} \ .$$
If $\beta \leq_S \alpha$ then β is nonrandom, so, by Lemma 30, we may assume that S is infinite. Furthermore, S is co-c.e. by definition, but it has the additional useful property that if a number s leaves S at stage t then so do all numbers in the interval (s, t).

To construct B, we run the following procedure P_i for all $i \in \omega$ in parallel. Note that B is a multiset, so we are allowed to add more than one copy of a given interval to B.

1. Look for an $s \in \omega$ such that $\alpha_s \in I_i$.

2. Let $t = s + 1$. If $\alpha_t \notin I_i$ then terminate the procedure.

3. If $s \notin S[t]$ then let $s = t$ and go to step 2. Otherwise, add the interval
$$[\beta_s + k(\alpha_{t-1} - \alpha_s), \beta_s + k(\alpha_t - \alpha_s)]$$
to B, increase t by one, and repeat step 3.

This concludes the construction of B. It is not hard to show that the sum of the lengths of the intervals in B is finite and that β is in infinitely many of the intervals in B. □

(sketch)

So we finally get to prove Theorem 27 (iv) that if α^0 and α^1 are c.e. reals such that $\alpha^0 + \alpha^1$ is random then at least one of α^0 and α^1 is random.

Let $\beta = \alpha^0 + \alpha^1$. For each $s \in \omega$, either $3(\alpha^0 - \alpha^0_s) > \beta - \beta_s$ or $3(\alpha^1 - \alpha^1_s) > \beta - \beta_s$, so for some $i < 2$ there are infinitely many $s \in \omega$ such that $3(\alpha^i - \alpha^i_s) > \beta - \beta_s$. By Theorem 31, α^i is random. □

We point out that Theorem 27 only applies to c.e. reals. Consider, for instance, if $\Omega = .a_0a_1....$ then if we put $\alpha = .a_0 0 a_2 0 a_4 0 \ldots$ and $\beta = .0 a_1 0 a_3 0 \ldots$, then clearly neither α nor β can be random yet $\alpha + \beta = \Omega$, but they are not c.e..

Before we leave the Solovay degrees of c.e. reals, we note that the structure must be very complicated.

Theorem 32 (Downey, Hirschfeldt, Laforte [21]). *The Solovay degrees of c.e. reals has an undecidable first order theory.*

The proof of theorem 32 uses Nies's method of interpreting effectively dense boolean algebras, together with a technical construction of a certain class of (strongly) c.e. reals. Calude and Nies [9] have proven that the random reals are all *wtt*-complete. Very little else is known about the Solovay degrees of c.e. reals.

11 Other measures of relative randomness

A reducibility $\leq$ on reals is a *measure of relative randomness* if it satisfies the *Solovay property*:

$$\text{If } \beta \leq \alpha \text{ then } \exists c\ (\forall n\ (H(\beta \restriction n) \leq H(\alpha \restriction n) + c)).$$

This can also be expressed for K in place of H. S-reducibility is a measure of relative randomness, but not the only one, and it has some problems.

- Restricted to c.e. reals.
- Too fine.
- Too uniform.

For instance, one can easily construct a real α which is d.c.e. and is not S above any c.e. real.

To see this, imagine you are building a real β, making sure that it is noncomputable, and trying to defeat all φ_e, c_e potential Solovay reductions. We are slowly making $\beta_s > \beta_t$ for $s > t$. Additionally, we are building a computable nonrational real $\alpha = \lim_s \alpha_s$. At some stage s, we get that $\varphi_{e,s}(\beta_t)\downarrow$, and

$$c_e(\beta_s - \beta_t) > \alpha_s - \varphi_{e,s}(\beta_t).$$

Then at stage $s+1$, we simply make β_{s+1} sufficiently close to β_t to make

$$c_e(\beta_{s+1} - \beta_t) < \alpha_s - \varphi_{e,s}(\beta_t).$$

Thus at the very first place it can, Solovay reducibility fails to be useful for classifying relative complexity.

Even on the c.e. reals Solovay reducibility fails badly to encompass relative complexity. In [20], Downey, Hirschfeldt, and Laforte introduced another measure of relative complexity called *sw-reducibility* (strong weak truth table reducibility):

Definition 9. *$\beta \leq_{sw} \alpha$ if there is a functional Γ such that $\Gamma^\alpha = \beta$ and the use of Γ is bounded by $x + c$ for some c.*

It is easy to see that by Lemma 24, for any (not necessarily c.e.) reals $\alpha \leq_{sw} \beta$, for all n, and $E = H$ or $E = K$,

$$E(\alpha \restriction n) \leq E(\beta \restriction n) + \mathcal{O}(1).$$

The *sw* degrees have a number of nice aspects, and $\leq_{sw}$ agrees with $\leq_S$ on the *strongly* c.e. reals. Furthermore if α is a c.e. real which is noncomputable, then there is a noncomputable strongly c.e. real $\beta \leq_{sw} \alpha$, and this is *not* true in general, for $\leq_S$. We have the following theorem.

Theorem 33 (Downey, Hirschfeldt, Laforte [20]). *There is a noncomputable c.e. real α such that all strongly c.e. reals dominated by α are computable.*

Proof. Recall that if we have c.e. reals $\beta \leq_S \alpha$ then there are a c.e. real γ and a positive $c \in \mathbb{Q}$ such that $\alpha = c\beta + \gamma$.

Now let α be the noncomputable c.e. real α such that if A presents α then A is computable. We claim that, for this α, if $\beta \leq_S \alpha$ is strongly c.e. then β is computable.

To verify this claim, let $\beta \leq_S \alpha$ be strongly c.e.. We know that there is a positive $c \in \mathbb{Q}$ such that $\alpha = c\beta + \gamma$. Let $k \in \omega$ be such that $2^{-k} \leq c$ and let $\delta = \gamma + (c - 2^{-k})\beta$. Then δ is a c.e. real such that $\alpha = 2^{-k}\beta + \delta$.

It is easy to see that there exist computable sequences of natural numbers $b_0, b_1, \ldots$ and $d_0, d_1, \ldots$ such that $2^{-k}\beta = \sum_{i \in \omega} 2^{-b_i}$ and $\delta = \sum_{i \in \omega} 2^{-d_i}$. Furthermore, since β is strongly c.e., so is $2^{-k}\beta$, and hence we can choose $b_0, b_1, \ldots$ to be pairwise distinct, so that the nth bit of the binary expansion of $2^{-k}\beta$ is 1 if and only if $n = b_i$ for some i.

Since $\sum_{i \in \omega} 2^{-b_i} + \sum_{i \in \omega} 2^{-d_i} = 2^{-k}\beta + \delta = \alpha < 1$, Kraft's inequality tells us that there is a prefix-free c.e. set $A = \{\sigma_0, \sigma_1, \ldots\}$ such that $|\sigma_0| = b_0$, $|\sigma_1| = d_0$, $|\sigma_2| = b_1$, $|\sigma_3| = d_1$, etc.. Now $\sum_{\sigma \in A} 2^{-|\sigma|} = \sum_{i \in \omega} 2^{-b_i} + \sum_{i \in \omega} 2^{-d_i} = \alpha$, and thus A presents α.

By our choice of α, this means that A is computable. But now we can compute the binary expansion of $2^{-k}\beta$ as follows. Given n, compute the number m of strings of length n in A. If $m = 0$ then $b_i \neq n$ for all i, and hence the nth bit of binary expansion of $2^{-k}\beta$ is 0. Otherwise, run through the b_i and d_i until either $b_i = n$ for some i or $d_{j_1} = \cdots = d_{j_m} = n$ for some $j_1 < \cdots < j_m$. By the definition of A, one of the two cases must happen. In the first case, the nth bit of the binary expansion of $2^{-k}\beta$ is 1. In the second case, $b_i \neq n$ for all i, and hence the nth bit of the binary expansion of $2^{-k}\beta$ is 0. Thus $2^{-k}\beta$ is computable, and hence so is β. □

We remark that *sw* reducibility is also *bad* in many ways, too. For instance, the *sw*-degrees of c.e. reals do not form a semilattice! (Downey, Hirschfeldt, Laforte [20]) It is unknown if Ω is *sw*-complete (for c.e. reals), that being the analog of Slaman's theorem. Furthermore *sw* and S are incomparable.

We would like a measure of relative randomness combining the best of S-reducibility and sw-reducibility.

Both S-reducibility and sw-reducibility are uniform in a way that relative initial-segment complexity is not. This makes them too strong, in a sense, and it is natural to wish to investigate nonuniform versions of these reducibilities. Motivated by this consideration, as well as by the problems with sw-reducibility, we introduce another measure of relative randomness, called relative H reducibility, which can be seen as a nonuniform version of both S-reducibility and sw-reducibility, and which combines many of the best features of these reducibilities. Its name derives from a characterization, discussed below, which shows that there is a very natural sense in which it is an *exact* measure of relative randomness.

Definition 10. *Let α and β be reals. We say that β is* relative H reducible *(rH-reducible) to α, and write $\beta \leq_{rH} \alpha$, if there exist a partial computable binary function f and a constant k such that for each n there is a $j \leq k$ for which $f(\alpha \upharpoonright n, j)\downarrow = \beta \upharpoonright n$.*

Clearly $\leq_{rH}$ is transitive. It might seem like a weird definition at first, but the actual motivation came from the consideration of Lemma 24. There we argued that if two strings are very close and of the same length then they have essentially the same complexity no matter whether we use H or K. Note that *sw* reducibility gives a method of taking an initial segment of length n of β to one of length $n-c$ of α. However, it would be enough to take some string k-close to an initial segment or β to one similarly close to one of α. This idea gives a notion equivalent to rH reducibility and leads to the definition above.

There are, in fact, several characterizations of rH-reducibility, each revealing a different facet of the concept. We mention three, beginning with a "relative entropy" characterization whose proof is quite straightforward. For a c.e. real β and a fixed computable approximation $\beta_0, \beta_1, \dots$ of β, we will let the mind-change function $m(\beta, n, s, t)$ be the cardinality of

$$\{u \in [s,t] \mid \beta_u \upharpoonright n \neq \beta_{u+1} \upharpoonright n\}.$$

Lemma 34 ([20]). *Let α and β be c.e. reals. The following condition holds if and only if $\beta \leq_{rH} \alpha$. There are a constant k and computable approximations $\alpha_0, \alpha_1, \dots$ and $\beta_0, \beta_1, \dots$ of α and β, respectively, such that for all n and $t > s$, if $\alpha_t \upharpoonright n = \alpha_s \upharpoonright n$ then $m(\beta, n, s, t) \leq k$.*

The following is a more analytic characterization of rH-reducibility, which clarifies its nature as a nonuniform version of both S-reducibility and sw-reducibility.

Lemma 35 ([20]). *For any reals α and β, the following condition holds if and only if $\beta \leq_{rH} \alpha$. There are a constant c and a partial computable function φ such that for each n there is a τ of length $n + c$ with $|\alpha - \tau| \leq 2^{-n}$ for which $\varphi(\tau)\downarrow$ and $|\beta - \varphi(\tau)| \leq 2^{-n}$.*

Proof. First suppose that $\beta \leq_{rH} \alpha$ and let f and k be as in definition 10. Let c be such that $2^c \geq k$ and define the partial computable function φ as follows. Given a string σ of length n, whenever $f(\sigma, j)\downarrow$ for some new $j \leq k$, choose a new $\tau \supseteq \sigma$ of length $n + c$ and define $\varphi(\tau) = f(\sigma, j)$. Then for each n there is a $\tau \supseteq \alpha \upharpoonright n$ such that $\varphi(\tau)\downarrow = \beta \upharpoonright n$. Since $|\alpha - \tau| \leq |\alpha - \alpha \upharpoonright n| \leq 2^{-n}$ and $|\beta - \beta \upharpoonright n| \leq 2^{-n}$, the condition holds.

Now suppose that the condition holds. For a string σ of length n, let S_σ be the set of all μ for which there is a τ of length $n + c$ with $|\sigma - \tau| \leq 2^{-n+1}$ and $|\mu - \varphi(\tau)| \leq 2^{-n+1}$. It is easy to check that there is a k such that $\operatorname{card}\{S_\sigma\} \leq k$ for all σ. So there is a partial computable binary function f such that for each σ and each $\mu \in S_\sigma$ there is a $j \leq k$ with $f(\sigma, j)\downarrow = \mu$. But, since for any real γ and any n we have $|\gamma - \gamma \upharpoonright n| \leq 2^{-n}$, it follows that for each n we have $\beta \upharpoonright n \in S_{\alpha \upharpoonright n}$. Thus f and k witness the fact that $\beta \leq_{rH} \alpha$. $\square$

The most interesting characterization of rH-reducibility (and the reason for its name) is given by the following result, which shows that there is a very natural sense in which rH-reducibility is an exact measure of relative randomness. Recall that the prefix-free complexity $H(\tau \mid \sigma)$ of τ *relative to* σ is the length of the shortest string μ such that $M^{\sigma}(\mu)\downarrow= \tau$, where M is a fixed self-delimiting universal computer. (Similarly for K.)

Theorem 36 ([20]). *Let α and β be reals. Then $\beta \leq_{rH} \alpha$ if and only if there is a constant c such that $H(\beta \upharpoonright n \mid \alpha \upharpoonright n) \leq c$ for all n. (And $K(\beta \upharpoonright n \mid \alpha \upharpoonright n) \leq c$.)*

Proof. We give the argument for H. First suppose that $\beta \leq_{rH} \alpha$ and let f and k be as in definition 10. Let m be such that $2^m \geq k$ and let $\tau_0, \ldots, \tau_{2^m-1}$ be the strings of length m. Define the prefix-free machine N to act as follows with σ as an oracle. For all strings μ of length not equal to m, let $N^{\sigma}(\mu)\uparrow$. For each $i < 2^m$, if $f(\sigma, i)\downarrow$ then let $N^{\sigma}(\tau_i)\downarrow= f(\sigma, i)$, and otherwise let $N^{\sigma}(\tau_i)\uparrow$. Let e be the coding constant of N and let $c = e + m$. Given n, there exists a $j \leq k$ for which $f(\alpha \upharpoonright n, j)\downarrow= \beta \upharpoonright n$. For this j we have $N^{\alpha\upharpoonright n}(\tau_j)\downarrow= \beta \upharpoonright n$, which implies that $H(\beta \upharpoonright n \mid \alpha \upharpoonright n) \leq |\tau_j| + e \leq c$.

Now suppose that $H(\beta \upharpoonright n \mid \alpha \upharpoonright n) \leq c$ for all n. Let $\tau_0, \ldots, \tau_k$ be a list of all strings of length less than or equal to c and define f as follows. For a string σ and a $j \leq k$, if $M^{\sigma}(\tau_j)\downarrow$ then $f(\sigma, j)\downarrow= M^{\sigma}(\tau_j)$, and otherwise $f(\sigma, j)\uparrow$. Given n, since $H(\beta \upharpoonright n \mid \alpha \upharpoonright n) \leq c$, it must be the case that $M^{\alpha\upharpoonright n}(\tau_j)\downarrow= \beta \upharpoonright n$ for some $j \leq k$. For this j we have $f(\alpha \upharpoonright n, j)\downarrow= \beta \upharpoonright n$. Thus $\beta \leq_{rH} \alpha$. □

An immediate consequence of this result is that rH-reducibility satisfies the Solovay property.

Corollary 37. *If $\beta \leq_{rH} \alpha$ then there is a constant c such that $H(\beta \upharpoonright n) \leq H(\alpha \upharpoonright n) + c$ for all n.*

It is not hard to check that the converse of this corollary is not true in general, but the following question is natural.

Question *Let α and β be c.e. reals such that, for some constant c, we have $H(\beta \upharpoonright n) \leq H(\alpha \upharpoonright n) + c$ for all n. Does it follow that $\beta \leq_{rH} \alpha$? Does it even follow that $\beta \leq_T \alpha$? (See Theorem 40)*

We will look at this very interesting question in the next section.

Theorem 38 ([20]). *Let α and β be c.e. reals. If $\beta \leq_S \alpha$ or $\beta \leq_{sw} \alpha$, then $\beta \leq_{rH} \alpha$.*

Corollary 39. *A c.e. real α is rH-complete if and only if it is random.*

Despite the nonuniform nature of its definition, rH-reducibility implies Turing reducibility.

Theorem 40 (Downey, Hirschfeldt, Nies [20]). *If $\beta \leq_{rH} \alpha$ then $\beta \leq_T \alpha$.*

Proof. Let k be the least number for which there exists a partial computable binary function f such that for each n there is a $j \leq k$ with $f(\alpha \upharpoonright n, j)\downarrow= \beta \upharpoonright n$.

There must be infinitely many n for which $f(\alpha \upharpoonright n, j)\downarrow$ for all $j \leq k$, since otherwise we could change finitely much of f to contradict the minimality of k. Let $n_0 < n_1 < \cdots$ be an α-computable sequence of such n. Let T be the α-computable subtree of 2^ω obtained by pruning, for each i, all the strings of length n_i except for the values of $f(\alpha \upharpoonright n_i, j)$ for $j \leq k$.

If γ is a path through T then for all i there is a $j \leq k$ such that γ extends $f(\alpha \upharpoonright n_i, j)$. Thus there are at most k many paths through T, and hence each path through T is α-computable. But β is a path through T, so $\beta \leq_T \alpha$. $\square$

Notice that, since any computable real is obviously rH-reducible to any other real, the above theorem shows that the computable reals form the least rH-degree.

Structurally, the rH-degrees of c.e. reals are nicer than the sw-degrees of c.e. reals.

Theorem 41 (Downey, Hirschfeldt, Laforte [20]). *(i) The rH-degrees of c.e. reals form an uppersemilattice with least degree that of the computable sets and highest degree that of* Ω.

(ii) The join of the rH-degrees of the c.e. reals α *and* β *is the rH-degree of* $\alpha + \beta$.

(iii) For any rH-degrees $\mathbf{a} < \mathbf{b}$ *of c.e. reals there is an rH-degree* $\mathbf{c}$ *of c.e. reals such that* $\mathbf{a} < \mathbf{c} < \mathbf{b}$.

(iv) For any rH-degrees $\mathbf{a} < \mathbf{b} < \deg_{rH}(\Omega)$ *of c.e. reals, there are rH-degrees* $\mathbf{c_0}$ *and* $\mathbf{c_1}$ *of c.e. reals such that* $\mathbf{a} < \mathbf{c_0}, \mathbf{c_1} < \mathbf{b}$ *and* $\mathbf{c_0} \vee \mathbf{c_1} = \mathbf{b}$.

(v) For any rH-degrees $\mathbf{a}, \mathbf{b} < \deg_{rH}(\Omega)$ *of c.e. reals,* $\mathbf{a} \vee \mathbf{b} < \deg_{rH}(\Omega)$.

Proof. We prove only (i), the remainder of the parts are proved by analogous methods to those used for $\leq_S$. All that is left to show is that addition is a join. Since $\alpha, \beta \leq_S \alpha + \beta$, it follows that $\alpha, \beta \leq_{rH} \alpha + \beta$. Let γ be a c.e. real such that $\alpha, \beta \leq_{rH} \gamma$. Then Lemma 34 implies that $\alpha + \beta \leq_{rH} \gamma$, since for any n and $s < t$ we have $m(\alpha + \beta, n, s, t) \leq 2(m(\alpha, n, s, t) + m(\beta, n, s, t)) + 1$. $\square$

We remark that the remaining part of Theorem 27 was that $\leq_S$ is distributive on the c.e. reals. This is open at present.

We see that rH-reducibility shares many of the nice structural properties of S-reducibility on the c.e. reals, while still being a reasonable reducibility on non-c.e. reals. Together with its various characterizations, especially the one in terms of relative H-complexity of initial segments, this makes rH-reducibility a tool with great potential in the study of the relative randomness of reals. As one would expect, little else is known about the structure of rH degrees.

We remark that the methods of this section have been used by Downey, Hirschfeldt and Laforte [20], to prove that the H-degrees of c.e. reals are dense.

12 $\leq_H$, $\leq_K$ and $\leq_T$.

Let return to the question below we deferred from the last section.
Question *Let α and β be c.e. reals such that, for some constant c, we have $H(\beta \upharpoonright n) \leq H(\alpha \upharpoonright n) + c$ for all n. Does it follow that $\beta \leq_{rH} \alpha$? Does it even follow that $\beta \leq_T \alpha$?*

Although it might seem at first that the answer to this question should obviously be negative, at first glance, Theorem 42 would seem to indicate that any counterexample would probably have to be quite complicated, and gives us hope for a positive answer.

Theorem 42 (Downey, Hirschfeldt, Laforte [20]). *Let α and β be c.e. reals such that $\liminf_n H(\alpha \upharpoonright n) - H(\beta \upharpoonright n) = \infty$. Then $\beta <_{sw} \alpha$.*

Proof. Let $c_\alpha(n)$ be the least s such that $\alpha_s \upharpoonright n = \alpha \upharpoonright n$, and define $c_\beta(n)$ analogously. Let M be a universal self-delimiting computer and define the self-delimiting computer N as follows. For each n, s, and σ, if $M(\sigma)[s]\downarrow = \beta_s \upharpoonright n$ and $N(\sigma)$ has not been defined before stage s then let $N(\sigma)\downarrow = \alpha_s \upharpoonright n$. Let e be the coding constant of N. For each n, if $c_\beta(n) \geq c_\alpha(n)$ then $\forall\sigma(M(\sigma)\downarrow = \beta \upharpoonright n \Rightarrow N(\sigma)\downarrow = \alpha \upharpoonright n)$, which implies that $H(\alpha \upharpoonright n) \leq H(\beta \upharpoonright n) + e$. Thus our hypothesis implies that $c_\beta(n) < c_\alpha(n)$ for almost all n, which clearly implies that $\beta \leq_{sw} \alpha$. We note that, $\alpha \not\leq_{sw} \beta$, so $\beta <_{sw} \alpha$ □

Stephan [55] has shown that the Theorem above has limited use because it is hard to satisfy the hypotheses of the Theorem. Let c_α denote the computation function of α: $c_\alpha(x)$ is the least $s \geq x$ with $\alpha \upharpoonright x = \alpha_s \upharpoonright x$. The following lemma is easy.

Lemma 43. *Let A be a c.e. set (or c.e. real). Suppose that c_A dominates all partial computable functions. Then A is wtt-complete.*

Theorem 44 (Stephan [55]). *Suppose that α and β satisfy the hypotheses of Theorem 42. Then α is wtt-complete.*

Proof. Given M a prefix free universal machine and φ a partial computable function, define

$$\widehat{M}(a\tau) = \begin{cases} M(\tau) & \text{if } a = 0, \\ \alpha_{\varphi(|M(\tau)|)} \upharpoonright M(|\tau|) & \text{if } a = 1, M(\tau)\downarrow, \text{ and } \varphi(|M(\tau)|)\downarrow, \\ \uparrow & \text{otherwise.} \end{cases}$$

Then $\widehat{M}$ is also a prefix-free universal machine. If c_α does not dominate φ, then there are infinitely many n with $\varphi(n)\downarrow > c_\alpha(n)$, and thus

$$H_{\widehat{M}}(\alpha \upharpoonright n) = \min\{H_{\widehat{M}}(\sigma) : |\sigma| = n\}.$$

That is, $\alpha \upharpoonright n$ has minimum H-complexity of all strings of length $|\alpha \upharpoonright n| = n$.

Consequently,

$$H_{\widehat{M}}(\alpha \upharpoonright n) \leq H_{\widehat{M}}(\beta \upharpoonright n),$$

for these n, and $\liminf(H_{\widehat{M}}(\alpha \upharpoonright n) - H_{\widehat{M}}(\beta \upharpoonright n) \leq 0$.

So suppose that α is not *wtt*-complete. Then there is some partial computable function not dominated by c_α. So there is no β with

$$\liminf(H_{\widehat{M}}(\alpha \upharpoonright n) - H_{\widehat{M}}(\beta \upharpoonright n) = \infty.$$

□

Stephan has clarified the situation for the relationship between $\leq_K$ and $\leq_T$.

Theorem 45 (Stephan [55]). *Suppose that we have c.e. α, β with $\alpha \leq_K \beta$. Then $\alpha \leq_T \beta$.*

Proof. So we suppose that there is a c such that for all n,

$$K(\alpha \upharpoonright n) \leq K(\beta \upharpoonright n) + c.$$

IF $\beta \equiv_T \emptyset'$, then there is nothing to prove. So we suppose that $\beta <_T \emptyset'$. In that case, for any total β-computable function g, we know

$$\exists^\infty x[x \in K - K_{g(x)}].$$

Let $\psi(x)$ be the partial computable function of the least stage that $x \in K_s$. The there are infinitely many x with $\psi(x) \downarrow > g(x)$. So let g be the computation function of β. Then there is an infinite $D \leq_\beta$ with $D \subset K$ and $\psi(x) > g(x)$ for all $x \in D$.

For any $x \in D$ we have the following program:

$$\varphi_e(x) = \beta_{\psi(x)} \upharpoonright x.$$

For this set of x we have $K(\beta \upharpoonright x|x) \leq e$, and hence

$$K(\alpha \upharpoonright x|x) \leq e + \mathcal{O}(1).$$

Now relativizing Loveland's theorem below, we see that $\alpha \leq_T \beta$. □

The missing ingredient is an old result of Loveland: (actually this is stated in slightly generalized form)

Theorem 46 (Loveland [42]). *Suppose that there is e and an infinite computable set A such that for all $x \in A$, $K(\alpha \upharpoonright x|x) \leq e$. Then α is computable.*

The proof is straightforward. The main observation is that, again, the possibilities for α can be used to form a Π^0_1 class with only finitely many paths, generated by the largest $e' \leq e$ such that $K(\alpha \upharpoonright x|x) = e'$ infinitely often.

One of the keys to the above is the uniformity implicit in $K(x \upharpoonright n|y \upharpoonright n)$. A much more interesting theorem is the following of Chaitin which indicates a hidden uniformity in K.

Theorem 47 (Chaitin [11]). *Suppose that $K(\alpha \upharpoonright n) \leq K(n) + \mathcal{O}(1)$ for all n (for an infinite computable set of n), or $K(\alpha \upharpoonright n) \leq \log n + \mathcal{O}(1)$, for all n. Then α is computable (and conversely). Furthermore for a given constant $\mathcal{O}(1) = d$, there are only finitely many ($\mathcal{O}(2^d)$) such x.*

The proof of Chaitin's theorem involves lemma of independent interest. The proof below is along the lines of Chaitin's, but we hope that it is somewhat less challenging than the original.

Let $D : \Sigma^* \mapsto \Sigma^*$ be partial computable. Then a *D-description* of σ is a pre-image of σ.

Lemma 48 (Chaitin [11]). *Let $f(d) = 2^{(d+c)}$, $c = c_{d,D}$ to be determined. Then for each $\sigma \in \Sigma^*$,*

$$|\{q : D(q) = \sigma \wedge |q| \leq K(\sigma) + d\}| \leq f_D(d).$$

That is, the number of D-descriptions of length $\leq K(\sigma) + d$, is bounded by an absolute constant depending upon d, D alone (and not on σ)

Note that this applies in the special case that D is the universal machine.

Proof. Let σ be given, and $k = K(\sigma) + d$. For each m there are at most $2^{k-m} - 1$ strings with $\geq 2^m$ D-descriptions of length $\leq k$, since there are $2^k - 1$ strings in total. Given k, m we can effectively list strings σ with $\geq 2^m$ D-descriptions of length $\leq k$, uniformly in k, m. (Wait till you see 2^m q's of length $\leq k$ with $D(q) = \nu$ and and then put ν on the list $L_{k,m}$.) The list $L_{k,m}$ has length $\leq 2^{k-m}$.

If σ has $\geq 2^m$ D-descriptions of length $\leq k$, then it is given by

- m
- a string q of length 2^{k-m},

the latter indicating the position of σ in $L_{k,m}$. This description has length bounded by $\log m + k - m + c$ where c depends only upon D. If we choose m large enough so that $\log m + k - m + c < k - d$, we can then get a description of σ of length $< k - d = K(\sigma)$. If we let $f(d)$ be 2^n where n is the least m with $\log m + c + d < m$ then we are done. □

The next lemma tells us that there are relatively few string with short descriptions, and the number depends on d alone.

Lemma 49 (Chaitin [11]). *There is a computable h depending only on d ($h(d) = \mathcal{O}(2^d)$) such that, for all n,*

$$|\{\sigma : K(\sigma) \leq K(n) + d\}| \leq h(d).$$

Proof. Consider the partial computable function D defined via $D(p)$ is the unary representation of $U(p)$. Then let $h(d) = f_D(d)$, with f given by the previous lemma. Suppose that $K(\sigma) \leq K(n) + d$, and pick the shortest p with $U(p) = \sigma$. Then p is a D-description of n and $|p| \leq K(n) + d$. Thus there at most $f(d)$ many $p's$, and hence σ's. □

Proof. (of Theorem 47, concluded.) Let

$$= \{\sigma : \forall p \subseteq \sigma(K(p) \leq \log |p| + d)\}.$$

If n is random then $K(n) = \log n + c$, so that by the second lemma above, the number of strings in T of length n is $\leq h(d)$. Taking the maximum number $\leq h(d)$ attained infinitely often, we can then construct a computable subtree of the c.e. tree T, upon which x must be a path. Note that the number of paths is bounded by $h(d)$. □

It is still an open question whether, for c.e. reals, $\leq_K$ implies $\leq_{rK}$, although the answer is "surely not".

The situation for $\leq_H$ is quite different. The argument of Stephan above shows that $\alpha \leq_H \beta$ implies that for all $x \in D$, $H(\beta \upharpoonright x|x) \leq e$, and hence $H(\beta \upharpoonright x) \leq e + H(x) + \mathcal{O}(1)$, for this set of x. All would be sweet if the folowing statement, true for K was also true for H: $H(\alpha \upharpoonright x) \leq H(x) + \mathcal{O}(1)$ for all (a computable set of) x, implied that α is computable. Chaitin observed using a relativized form of Loveland's observation that

$$H(\alpha \upharpoonright x) \leq H(x) + \mathcal{O}(1) \text{ implies } \alpha \leq_T \emptyset'.$$

Surprisingly we cannot replace $\emptyset'$ by $\emptyset$ for H. That is even though α looks identical to ω we cannot conclude that α is computable even for strongly c.e. reals α.

This was proved by Solovay in his 1974 manuscript. The proof there is very complicated and only constructs a Δ_2^0 real. For the remainder of the section we will prove a slight generalization of Solovay's theorem. In fact we will give *two* proofs as the result is so interesting, and each proof yields a different technique. In particular, the second is a modification of Solovay's original proof, which contains an important lemma of independent interest. The first is short and easy once you have found it. Both are due to Downey, Hirschfeldt and Nies.

Theorem 50 (Downey, Hirschfeldt, Nies, after Solovay [54]). *There is a c.e. noncomputable set A such that for all n*

$$H(A \upharpoonright n) \leq H(n) + \mathcal{O}(1).$$

Proof. 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 $B = \{0^n : n \in \omega\}$ had 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 was to compute initial segments of B. The idea was if the universal machine U enumerated $\langle \sigma, n \rangle$, then in our machine we would enumerate $\langle \sigma, 0^n \rangle$. Notice that, in fact, using Kraft-Chaitin it would be enough to build M *implicitly* be enumerating the length axiom (or "requirement") $\langle |\sigma|, n \rangle$. We are guaranteed that

$$\Sigma_{\sigma \in \mathrm{dom}(U)} 2^{-|\sigma|} = \Sigma_{\tau \in \mathrm{dom}(M)} 2^{-|\tau|} < 1.$$

Hence Kraft-Chaitin applies.

Note also that we could, for convenience, as we do in the main construction, use a string of length $|\sigma|+1$, in which case we would force

$$\Sigma_{\tau\in\mathrm{dom}(M)}2^{-|\tau|} < \frac{1}{2}.$$

The idea is the following. We will build a noncomputable c.e. set A in place of B 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, in our machine M, enumerate $\langle\tau, A_s\restriction n\rangle$, where $|\tau|=|\sigma|+1$. To make A noncomputable, we will also sometimes make $A_s\restriction n \neq A_{s+1}\restriction n$. Then for each j with $n\leq j\leq s$, we will for the currently shortest string σ_j computing j, we will also need to put into M,

$$\langle\tau_j, A_{s+1}\restriction j\rangle.$$

This construction works by making this quantity small. We are ready to define A:

$$A=\{\langle e,n\rangle : W_{e,s}\cap A_s=\emptyset\wedge\langle e,n\rangle\in W_{e,s}\wedge \sum_{\langle e,n\rangle\leq j\leq s}2^{-H(j)[s]}<2^{-(e+1)}\}.$$

Then clearly A is c.e.. It is noncomputable since the H-complexity of $P_n=\{m : m\geq n\}$ tends to zero as $n\to\infty$, and finally, M is a Chaitin machine, since the errors are bounded by $\Sigma_e 2^{-(e+1)}$ (once for each e), whence

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

And by force we have for all n, $H(A\restriction n)\leq H(n)+\mathcal{O}(1)$. □

The second proof is a modification of Solovay's. It is more complicated. The basic idea is to try to let U do the work for us. Specifically, consider the task of constructing a noncomputable α with $H(\alpha\restriction n)\leq H(n)+\mathcal{O}(1)$ for all n. The natural idea would be that we would pick some diagonalization place i and wait for i, keep it out of $\alpha_s = .A_s$ until i appears in $W_{e,s}$ for the requirement R_e saying $\overline{A}\neq W_e$. Then one would put i into A_{s+1}.

Now this stage s could be very late. Furthermore we need that $H(\alpha\restriction i)\leq H(i)+\mathcal{O}(1)$. In the one above we allow ourselves to do this provided that the amount of damage we do is small. Solovay's idea is to only let ourselves do this provided we can keep $H(\alpha\restriction i)\leq H(i)[s]$. The idea that we will let the opponent do the work for us. Occasionally the opponent must drop the stage s complexity of i to something lower. Our idea is that *then* at that very stage we can change $A_s(i)$ and the amount of entropy we need will simply follow the universal computer on i. Thus the argument looks very easy.

There is a big problem, which necessitates all the following. Suppose that U changes its current complexity on i at the stage t. At stage t, *we have enumerated A up to length t*. Now if we change A on i, then for all $t\geq n\geq i$, we *also change $A\restriction n$*. Hence, for each of these $A\restriction n$ we *also* would need to also enumerate some string σ computing $A \upharpoonright n$ of the same length as the one computing n, and perhaps only i has a new string. Why should n?

The key idea of Solovay is that if one looks at appropriately sparse stages of the construction, then one can prove that there will, infinitely often, be stages where *all* of the $n \geq i$ get new shorter descriptions *together*. This is by no means obvious. We turn to the formal proof.

Fix a universal prefix-free machine U and define H relative to U. We may assume that $H(n) \leq n+1$ for all n, and hence we adopt the convention that if there is no τ such that $|\tau| \leq n$ and $U(\tau)[s]\downarrow = n$ then $H(n)[s] = n+1$.

Let A be any function with primitive recursive graph that dominates all primitive recursive functions (e.g. Ackermann's function) and define $t_0 = 0$ and $t_{n+1} = A(t_n)$. Let $\sigma(i)$ be the largest $j \leq i$ such that $H(n)[t_i] = H(n)[t_{i+1}]$.

Theorem 51 (Solovay). *For any total computable function g there are infinitely many i such that $g(\sigma(i)) < i$.*

Proof. Fix a total computable function g. Let $G(n)$ be the least m such that $g(m) \geq n$. To show that there are infinitely many i such that $g(\sigma(i)) < i$, it is enough to show that there are infinitely many i such $G(i) > \sigma(i)$. By increasing g if necessary, we may assume that g has primitive recursive graph and that $g(n) \geq n$ for all n, which implies that G is primitive recursive.

For each k, let n_k be the least n such that

$$\sum_{G(n) \leq j \leq n} 2^{-H(j)[t_n]} \leq 2^{-2k},$$

which exists since for any n we have

$$\sum_{G(n) \leq j \leq n} 2^{-H(j)[t_n]} < \sum_{j \geq G(n)} 2^{-H(j)},$$

and this last sum goes to 0 as n increases. Note that the graph of the function $k \mapsto t_{n_k}$ is primitive recursive.

Consider the following enumeration of requirements. For each $k > 0$ and each $j \in [G(n_k), n_k]$, enumerate the requirement $\langle j, H(j)[t_{n_k}] - k\rangle$. Since

$$\sum_{k>0} \sum_{G(n_k) \leq j \leq n_k} 2^{-(H(j)[t_{n_k}]-k)} = \sum_{k>0} 2^k \sum_{G(n_k) \leq j \leq n_k} 2^{-(H(j)[t_{n_k}])} \leq \sum_{k>0} 2^k 2^{-2k} = 1,$$

the Kraft-Chaitin Theorem implies that there is a prefix-free M satisfying these requirements. Furthermore, M can be built to satisfy each requirement $\langle j, H(j)[t_{n_k}] - k\rangle$ in time primitive recursive in t_{n_k}, and hence before time t_{n_k+1} for sufficiently large k.

Thus, for all sufficiently large k, we have $H_M(j)[t_{n_k+1}] = H(j)[t_{n_k}] - k$ for all $j \in [G(n_k), n_k]$. This means that, for all sufficiently large k, we have $H(j)[t_{n_k+1}] < H(j)[t_{n_k}]$ for all $j \in [G(n_k), n_k]$, which implies that $G(n_k) > \sigma(n_k)$. So there are infinitely many n such that $G(n) > \sigma(n)$. □

We call a real α with $H(\alpha \upharpoonright n) \leq H(n) + \mathcal{O}(1)$ for all n *H-trivial.* Now we can define two reals

$$\Lambda = \Sigma_{i \in \omega} 2^{-2(\sigma(i))},$$

$$\Lambda_C = \Sigma\{2^{-(2(\sigma(i)^2+j)} : i \in \omega \wedge \sigma(i)[t_{i+1}] \leq i \text{ at least } j \text{ times}\}.$$

Then Λ and Λ_C are H-trivial, and additionally, the latter is a strongly c.e. real. (For instance, if we assume that Λ is computable, then the stage when the first i bits of Λ stop moving allows us to define a computable function g, after which $\sigma(i)$ cannot drop below i, contrary to the Lemma. Also $\sigma(i)$ can drop below i only i (in fact $\log i$) times, and hence Λ exists.)

We remark that the first construction clearly combines with, for instance, permitting: below any c.e. nonzero degree there is a noncomputable c.e. H-trivial set. Also, one can use it to construct a promptly simple one, or a variant to avoid a given low c.e. set, using the Robinson trick. However, we do not know if there is a complete H-trivial set. An answer either way would be very interesting. In the positive way it says that the relationship between $\leq_H$ and $\leq_T$ fails as badly as it can. In the negative way, then the first proof above provides a priority free solution to Post's problem[6]. While these are known, the construction we give is particularly simple.

13 Other areas

Naturally in a short course such as this I cannot hope to cover all areas falling under the umbrella of the intrinsic relationship between computability and randomness. In this last section, I will point towards other material of which I am aware, and direct the reader towards the literature. I certainly do not claim completeness here. In particular, I will not even discuss the rich area of resource bounded randomness. (See e.g. Ambos-Spies et. al. [2]) Otherwise the reader has Ambos-Spies and Kučera [1], van Lambalgen [58], and Li-Vitanyi [41] as general references.

13.1 Π_1^0 classes

One natural direction is to examine not necessarily c.e. reals, and perhaps the collection of all random reals. A counting argument shows that the set of random reals has measure 1. Kurtz [39] and Kautz [30] have a lot of material here. A nice observation more or less due to Martin-Löf [44], is that the random reals form a Σ_2^0 class: an effective union of Π_1^0 classes. To see this let

$$C_k = \{x \in [0,1] : \forall n H(x \upharpoonright n) \geq n - k\}.$$

[6] Downey, Hirschfeldt, Nies, and Stephan [16] have recently proven that an H-trivial set is never T-complete, and hence the above is a priority-free solution to Post's Problem

Then evidently the C_k form Π^0_1 classes and x is random iff there is a k with $x \in C_k$.

$$RAND = \cup_k C_k.$$

s a consequence, all the apparatus of Π^0_1 classes apply. There are, for instance, random reals of low degree by the low basis theorem. Kučera [34, 35] has a lot of material here, additionally relating these notions to genericity and other notions such as DNR functions.

13.2 Martin-Löf Lowness

One very interesting area comes from relativizing the notion of a test. We can define the notion of a Martin-Löf test relative to an oracle, and hence get the class $RAND^X$. Van Lambalgen asked if there is a Martin-Löf low set X: a set X such that $RAND^X = RAND$. This question has an affirmative answer.

Theorem 52 (Kučera and Terwijn [36]). *There is a c.e. set A that is Martin-Löf low.*

Proof. We give an alternative proof to that in [36]. It is clear that there is a primitive recursive function f, so that $U^A_{f(n}$ is the universal Martin-Löf test relative to A. Let I^A_n denote the corresponding Solovay test. Then X is A-random iff X is in at most finitely many I^A_n. We show how to build a $\{J_n : n \in \omega\}$, a Solovay test, so that for each $(p,q) \in I^A_n$ is also in J_n. This is done by simple copying: if $(p,q) < s$ is in $\cup_{j \leq s} I^{A_s}_j$ is not in $J_i : i \in s$, add it. Clearly this "test" has the desired property of covering I^A_n. We need to make A so that the "mistakes" are not too big.

The crucial concept comes from Kučera and Terwijn: Let $M_s(y)$ denote the collection of intervals $\{I^{A_s}_n : n \leq s\}$ which have $A_s(y) = 0$ in their use function. Then we put $y > 2e$ into $A_{s+1} - A_s$ provided that e is least with $A_s \cap W_{e,s} = \emptyset$, and

$$\mu(M_s(y)) < 2^{-e}.$$

It is easy to see that this can happen at most once for e and hence the measure of the total mistakes is bounded by $\Sigma 2^{-n}$ and hence the resulting test is a Solovay test. The only thing we need to prove is that A is noncomputable. This follows since, with priority e, whenever we see the some y with $\mu(M_s(y)) \geq 2^{-e}$, such y will *not* be added and hence this amount of the A-Solovay test will be protected. But since the total measure is bounded by 1, this cannot happen forever. □

There is no known characterization of the degrees of such sets. Clearly the above argument permits and hence each nonzero c.e. degree has a nonzero Martin-Löf low predecessor. Kučera and Terwijn show that each Martin-Löf set is in the class GL_1: the sets A with $A' \equiv_T A \oplus \emptyset'$.

Intriguingly, there is a *complete* characterization for the Schnorr low sets of the next section.

13.3 Schnorr lowness

As noted in the earlier sections, the notion of Martin-Löf randomness is by no means the *only* notion of algorithmic randomness. The choice of it as the "correct" notion is as much philosophical as mathematical. There are a number of competing notions. One that has much support is due to Schnorr.

Definition 11. *A real x is called* Schnorr random *iff it passes all Schnorr tests. A Schnorr test is a Martin-Löf test $\{U_n : n \in \omega\}$ such that for all n*

$$\mu(U_n) = 2^{-n}.$$

Recall that the idea of a Martin-Löf test was to avoid all sets which were *effectively null*. The difference between a Schnorr and a Martin-Löf test is the relevant level of effectiveness demanded. There are no universal Schnorr tests. Indeed, one can construct a computable real passing a given Schnorr test. Clearly every Martin-Löf random set is Schnorr random. The converse fails.

Theorem 53 (Schnorr). *There are c.e. reals that are Schnorr random but not Martin-Löf random.*

The idea of the proof is to build out real α and a Martin-Löf test $\{U_i : i \in \omega\}$, by enumerating all partial Schnorr tests, and waiting till the opponent enumerates a lot of his test, then building in the complement. (Thus we can choose to pretend that a partial Schnorr test is not really one until he enumerates to within ϵ of the claimed measure of $V_1, V_2 ... V_n$ for some fixed n.)

Actually this theorem follows from some recent work of Downey and Griffiths [14]. Downey and Griffiths have shown that every Schnorr random c.e. real is of high c.e. degree. However, they also use a relatively difficult $\mathbf{0}''$ agrument to prove that there exist incomplete Schnorr random c.e. reals. Since all Martin-Löf random c.e. reals are T-complete, such an incomplete Schnorr random c.e. real cannot be Martin-Löf random. We refer the reader to Downey-Griffiths [14] for this and other results here.

Little is known about the degrees of Schnorr random reals. There is no known combinatorial characterization like Chaitin randomness for Schnorr randomness. It seems to the author there is a whole constellation of questions about this and other notions of randomness such as weak randomness of Kurtz [39], awaiting the development of the appropriate technology.

One really nice aspect of Schnorr randomness is that there is a complete characterization of Schnorr low sets. As usual, let D_x denote the x-th canonical finite set.

Theorem 54 (Terwijn and Zambella [56]). *A set X is Schnorr low iff there is a computable function p, such that, for all functions $g \leq_X$, there is a function h where, for all n,*

(i) $|H_{h(n)}| < p(n)$,

(ii) $g(n) \in D_{h(n)}$.

The proof is nontrivial. It relies in one direction, on ideas of Rasonnier [47] on rapid filters for the "mathematical" proof of Shelah's theorem that you cannot take the inaccessible cardinal away from Solovay's construction of a model where every set of reals is Lebesgue measurable. Note that all such Schnorr low degrees are hyperimmune free and hence are *not* below $\mathbf{0}'$. This is quite different from the situation for Martin-Löf lowness as there the set constructed was c.e.. It is unknown how the two notions relate. It is unknown if there is a similar characterization for Martin-Löf lowness. It is known that not all hyperimmune free degrees are Schnorr low.

13.4 Computably enumerable sets

An important subtopic is the complexity of strongly c.e. reals, that is, c.e. sets. We mention only one result here but there are many more, and many open questions. As we have seen, the Kolmogorov complexity of a c.e. set $A \restriction n$ is bounded by $2 \log n - \mathcal{O}(1)$. Solovay asked if this bound was attainable. Certainly for K-complexity no c.e. set has initial segment complexity on length n always greater than $2 \log n - \mathcal{O}(1)$.

In a very interesting paper, Kummer [38] proved that there are c.e. *complex* sets.

Theorem 55 (Kummer [38]). *There is a set A such that there is a constant c, with*

$$K(A \restriction n) \geq 2 \log n - c$$

for infinitely many n.

Proof. Kummer's proof runs as follows. First we have intervals defined via $t_0 = 0$, $t_{i+1} = 2^{t_i}$ and then $I_i = (t_i, t_{i+1}]$. The Kummer defined

$$f(k) = \Sigma_{i=t_k+1}^{t_{k+1}} (i - t_k + 1),$$

$$g(k) = \max\{d : 2^d - 1 < f(k)\}.$$

Note that $f(k)$ asymptotically approaches $1/2t_{k+1}^2$ and $g(k)$ approaches $2 \log t_{k+1} - 2$. Then at stage $s+1$ our action is the following for $k = 0, \cdots s$, if $K(A_s \restriction n) \leq g(k)$ for all $n \in I_k$, put the minimum element in $\overline{A_s} \cap I_k$ into A_{s+1}.

Now suppose that $K(A \restriction n) \leq g(k)$ for all $n \in I_k$. Then all of I_k is put into A. For a fixed n there are at least $n - t_k + 1$ many strings $\sigma = A \restriction n$ with $|\sigma| = n+1$ and $K(\sigma) \leq g(k)$. Therefore there are at least $f(k)$ many strings of K complexity at most $g(k)$ and this contradict the fact that $f(k) > 2^{g(k)+1} - 1$. $\square$

Actually Kummer classified the degrees containing complex c.e. sets. From Downey, Jockusch, and Stob [22], a degree $\mathbf{a}$ is called *array noncomputable* iff for all $g \leq_{tt} \emptyset'$ there is a function $h \leq_T \mathbf{a}$ not dominated by g. The anc degrees form a upwards closed class of the c.e. degrees including some low degrees, but such that each c.e. degree has a nonzero array computable predecessor. The array noncomputable degrees capture a notion of "multiple permitting" common to a number of degree constructions. For example, the are the degrees $A \oplus B$ such that A and B are c.e. and have no complete separating set. Ishmukhametov [28] has the following characterization of the (c.e.) array computable degrees.

a *is array computable iff there is a computable function* p *such that, for all* $g \leq_T$ **a**, *there is a computable function* h *such that*

(i) $|W_{h(n)}| < p(n)$, *and*

(ii) $g(n) \in W_{h(n)}$.

The reader might like to compare this characterization with the one for Schnorr low sets. Surely there must be some connection here! I remark that Ishmukhametov [28] used this characterization to prove that the c.e. degrees with strong minimal covers are exactly the array computable ones. Of interest to us here is the following.

Theorem 56 (Kummer [38]). *A c.e. degree contains a complex set iff it is array noncomputable. Furthermore if the degree is array computable and A is any c.e. set of the degree, then for any $\epsilon > 1$,*

$$K(A \upharpoonright n) \leq (1 + \epsilon) \log n + \mathcal{O}(1).$$

Clearly there are other connections between degree, domination and complexity.

References

[1] Ambos-Spies K., and A. Kučera, *Randomness in computability theory*, in *Computability Theory and its Applications*, (Cholak, Lempp, Lerman, Shore, eds) Contemp. math. Vol. 257 (2000), 1-14.

[2] Ambos-Spies K., and E. Mayordomo, *Resource bounded measure and randomness*, in *Complexity, Logic and Recursion Theory,* (A. Sorbi, ed.) Marcel-Decker, New York, 1997, 1-48.

[3] Ambos-Spies, K. Weihrauch and X. Zhang, J. Complexity, Vol. 16 (4)(2000), 676-690.

[4] Barzdin, J., *Complexity of programs to determine whether natural numbers not greater than n belong to a recursively enumerable set,* Soviet Mat. Dokl. vol. 9 (1968), 1251-1254.

[5] O. Belegradek, *On algebraically closed groups*, Algebra i Logika, **13** No. 3 (1974), 813-816.

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

[7] Calude, C., Coles, R., Hertling, P., Khoussainov, B., *Degree-theoretic aspects of computably enumerable reals*, in *Models and Computability,* (ed. Cooper and Truss) Cambridge University Press, 1999.

[8] Calude, C., Hertling, P., Khoussainov, B., Wang, Y., *Recursively enumerable reals and Chaitin's Ω number*, in STACS '98, Springer Lecture Notes in Computer Science, Vol 1373, 1998, 596-606.

[9] Calude, C, and A. Nies, *Chaitin's Ω numbers and strong reducibilities*, Journal of Universal Computer Science, 1997.

[10] Chaitin, G. *Information-theoretical characterizations of recursive infinite strings,* Theor. Comput. Sci., vol. 2 (1976), 45-48.

[11] Chaitin, G., *A theory of program size formally identical to information theory*, Journal of the ACM 22 (1975), pp. 329-340.

[12] Downey, R., *On the universal splitting property,* Mathematical Logic Quarterly, **43** (1997) 311-320.

[13] Downey, R., *Computability, definability, and algebraic structures*, to appear, Proceedings of the 7th Asian Logic Conference, Taiwan.

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

[15] Downey, R., D. Hirschfeldt, and A. Nies, *Randomness, computability and density* submitted to SIAM J. Comput. (Extended abstract accepted for STACS'01)

[16] Downey, R., D. Hirschfeldt, A. Nies, and F. Stephan, in preparation.

[17] Downey, R. and G. Laforte, *Presentations of computably enumerable reals,* to appear, Theoretical Computer Science.

[18] Downey, R. G., G. Laforte, and A. Nies, Enumerable sets and quasi-reducibility, Annals of Pure and Applied Logic, Vol. 95 (1998), 1-35.

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

[20] Downey, R., D. Hirschfeldt, and G. Laforte, *Randomness and Reducibility*, submitted (Extended abstract appeared in MFCS, 2001).

[21] Downey, R., D. Hirschfeldt, and G. Laforte, *Undecidability of Solovay and other degree structures for c.e. reals*, in preparation.

[22] 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 Math. vol. 1432 (1990), 141-174.

[23] Downey, R. G. and J. B. Remmel, *Classification of degree classes associated with r.e. subspaces*, Ann. Pure and Appl. Logic, **42** (1989) 105-125

[24] Downey, R. and M. Stob, *Splitting theorems in recursion theory*, Ann. Pure and Appl. Logic, **65** (1)((1993) 1-106).

[25] Fortnow, L., *Kolmogorov complexity,* in [19], to appear.

[26] Hirschfeldt, D., personal communication, Feb, 2001.

[27] Ho, Chun-Kuen, *Relatively recursive reals and real functions*, Theoretical Computer Science, Vol. 219 (1999), 99-120.

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

[29] C. G. Jockusch Jr., Fine degrees of word problems in cancellation semigroups, *Z. Math. Logik Grund. math.*, Vol. 26 (1980), 93-95.

[30] Kautz, S., *Degrees of random sets,* Ph.D. Diss. Cornell, 1991.

[31] Ko, Ker-I, *On the continued fraction representation of computable real numbers*, Theor. Comput. Sci, A, 47 (1986), 299-313,

[32] Ko, Ker-I, *Complexity of Real Functions*, Birkhauser, Berlin, 1991.

[33] Ko, Ker-I, and H. Friedman, *On the computational complexity of real functions,* Theor. Comput. Sci., 20 (1982), 323-352.

[34] Kučera, A., *On relative randomness,* Ann. Pure and Appl. Logic, vol. 63, (1993), 61-67.

[35] Kučera, A., *On the use of diagonally nonrecursive functions,* in *Logic Colloquium, '87*, North-Holland, Amsterdam, 1989, 219-239.

[36] Kučera, A., and S. Terwijn, *Lowness for the class of random sets,* J. Symb. Logic, vol. 64 (1999), 1396-1402.

[37] Kučera, A. and T. Slaman, *Randomness and recursive enumerability,* SIAM J. Comput, to appear.

[38] Kummer, M., *Kolmogorov complexity and instance complexity of recursively enumerable sets,* SIAM J. Comput., Vol. 25 (1996), 1123-1143.

[39] Kurtz, S., Ph. D. Thesis, University of Illinois at Urbana,

[40] Levin, L., *Measures of complexity of finite objects (axiomatic description),* Sov. Math. Dokl. vol. 17 (1976), 552-526.

[41] Li, Ming and Vitanyi, P., *Kolmogorov Complexity and its Applications*, Springer-Verlag, 1993.

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

[43] A. Macintyre, *Omitting quantifier free types in generic structures*, Journal of Symbolic Logic, **37** (1972), pp. 512-520.

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

[45] Pour-El, M., *From axiomatics to intrinsic characterization, some open problems in computable analysis*, Theor. Comput. Sci, A., to appear.

[46] Pour-El, M. and I. Richards, *Computability in Analysis and Physics*, Springer-Verlag, Berlin, 1989.

[47] Rasonnier, J., *A mathematical proof of S. Shelah's theorem on the measure problem and related results,* Israel J. Math. vol. 48 (1984), 48-56.

[48] Rice, H., *Recursive real numbers*, Proc. Amer. Math. Soc., 5 (1954), 784-791.

[49] Schnorr, C. P., *A unified approach to the definition of a random sequence,* Math. Systems Theory, 5 (1971), 246-258.

[50] Soare, R., *Recursion theory and Dedekind cuts*, Trans. Amer. Math. Soc., 140 (1969), 271-294.

[51] Soare, R., *Cohesive sets and recursively enumerable Dedekind cuts*, Pacific Journal of Math., vol. 31, no. 1 (1969), 215-231.

[52] Soare, R., *Recursively enumerable sets and degrees* (Springer, Berlin, 1987).

[53] Solomonoff, R., *A fromal theory of inductive inference, part 1 and part2,* Inform. Control, 7 (1964), 224-254.

[54] Solovay, R. *Draft of paper (or series of papers) on Chaitin's work*, unpublished notes, May, 1975, 215 pages.

[55] Stephan, F, personal communication.

[56] Terwijn, S. and D. Zambella, *Algorithmic randomness and lowness,* J. Symb. Logic, to appear.

[57] Turing, A., *On computable numbers with an application to the Entscheidungsproblem*, Proc. London Math. Soc., 42 (1936), 230-265, correction in Proc. London Math. Soc., 43 (1937), 544-546.

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

[59] Weihrauch, K., *Computability*, Springer-Verlag, Berlin, 1987.

[60] Weihrauch, K., and Zheng, X., *Arithmetical hierarchy of real numbers*, MFCS'99, Sklarska Poreba, Poland, September, 1999, 23-33.

[61] M. Ziegler, *Algebraisch abgeschlossen gruppen* in *Word Problems II, The Oxford Book*, ed. S.I. Adian, W.W. Boone, and G. Higman, North Holland, 1980, pp.449-576.