Publishers' page

Publishers' page

Publishers' page

Publishers' page

CONTENTS

FOREWORD

a foreword

PREFACE

preface

FIVE LECTURES ON ALGORITHMIC RANDOMNESS

Rod Downey
School of Mathematics, Statistics and Computer Science
Victoria University
PO Box 600, Wellington, New Zealand
E-mail: Rod.downey@vuw.ac.nz

This article is devoted to some of the main topics in algorithmic randomness, at least from my idiosyncratic view.

Contents

1. Introduction

In this article, I plan to give a course around certain highlights in the theory of algorithmic randomness. At least, these will be some highlights as I see them.

I will try not to cover too much of the material already covered in my notes [15]. However, since I plan to make these notes relatively self-contained I will by necessity need to include some introductory material concerning the basics of Martin-Löf randomness and Kolmogorov complexity.

There will also be a certain intersection with the articles Downey, Hirschfeldt, Nies and Terwijn [24] and Downey [14].

I will not be able to cover the background computability theory needed, and here refer the reader to Soare [81] and Odifreddi [71, 72]. While I plan to write sketches of proofs within these notes, full details can be found in the forthcoming monograph Downey and Hirschfeldt [19]. Other work

on algorithmic randomness can be found in well-known sources such as Calude [5] and Li-Vitanyi [50].

The subject of algorithmic randomness is a vast one, and has been the under intense development in the last few years. With only five lectures I could not hope to cover all that has happened, nor even report on the history. Here I certainly recommend the reader look at the surveys Downey, Hirschfeldt, Nies and Terwijn [24] and Downey [14].

Probably the most brutal omission is the work on triviality and lowness, which has its roots in Solovay's [84], and its first modern incarnation in Kučera-Terwijn [42] and Downey, Hirschfeldt, Nies, and Stephan [23]. This work is of central importance as has been shown especially through the powerful results of (Hirschfeldt and) Nies [67–69], and subsequently Hirschfeldt, Stephan (e.g. [32]), Slaman and others. The reason for this lamentable omission is that I don't think it is possible to give a fair treatment to Martin-Löf lowness and triviality, as well as other important triviality lowness notions for Schnorr and computable randomness, in even one or two lectures. They could have five to themselves! A short account can be found in Downey, Hirschfeldt, Nies, Terwijn [24], and a full account is, or will be soon, found in Downey and Hirschfeldt [19].

Finally these notes will certainly contain more material than I could possibly cover in any set of lectures in the hope that the extra material will help the participants of the meeting *Computational Prospects of Infinity.* This is especially true of the many results I won't have time to prove in the lectures, but whose proofs I have included.

In these notes in Section 2, I will first develop the basic material on Kolmogorov Complexity. Whilst this approach does not follow the historical development of the subject, it does make logical sense. I will include proofs of the fundamental results including Kraft-Chaitin, the Coding Theorem, and Symmetry of Information.

In Section 3, I will discuss the background material on the three basic approaches to randomness, via measure theory, prediction, and compression. Here I will also include the exciting recent results of Miller and Yu classifying 1-randomness in terms of plain complexity.

In Section 4, I will look at some classic theorems concerning randomness for general classes of reals. This material will include the Kučera-Gács Theorem and other results of Kučera. Other central results treated will be van Lambalgen's Theorem, effective 0-1 laws, and results on PA and FPF degrees. We also introduce n-randomness and variations and look at the exciting recent work showing that 2-randomness is the same as Kolmogorov

randomness.

In Section 5, I will look at various methods of calibrating randomness using initial segment methods. This will include the Slaman-Kučera Theorem and other work on computably enumerable reals, and the work of Solovay, and Miller-Yu on van Lambalgen reducibility and its relationship with $\leq_K$ and $\leq_C$.

Finally, in Section 6, I plan to give sketches of proofs of the poorly known results of Stuart Kurtz from his thesis [45], and some refinements later by Steven Kautz [34]. None of this work has ever been published aside from the presentations in these theses. The techniques, whose origins go back to work of Paris and of Martin, are powerful and are extremely interesting.

We remark that throughout these notes we will be working over the alphabet $\{0,1\}$, and hence will be looking at $2^{<\omega}$, and 2^ω for "reals"meaning members of Cantor Space. This sapce will be equipped with the basis of clopen sets $[\sigma] = \{\alpha : \sigma \prec \alpha\}$, and comes with the usual Lebesgue measure $\mu([\sigma]) = 2^{-|\sigma|}$. The whole development can also be done over other alphabets with little change. Most notation is drawn from Soare [81]. We will use λ to denote the empty string.

2. Lecture 1 : Kolmogorov complexity basics

This section is devoted to the analysis of the Kolmogorov complexity (or, rather complexit*ies*) of finite strings. The fundamental idea idea is well-known, and that is a random string should be one that it hard to compress. The compression devices used will generate different kinds of complexities, and we discuss some of these here. We begin with the most basic notion (plain complexity) first articulated by the seminal paper of Kolmogorov [35].

2.1. *Plain Complexity*

Thus we can imagine a Turing machine M which acts as a transducer and takes an input string τ and, should it halt, produces an output string σ. Then $M(\tau) = \sigma$. We say that τ is an *M-description* of σ. Since we are interested in the extent that σ can be *compressed*, we can then define the M-complexity as $C_M(\sigma)$ is the *length* of the shortest τ such that $M(\tau) = \sigma$. If no such τ exists, then we regard $C_M(\sigma) = \infty$. We can enumerate all Turing machines $\{M_e : e \in \mathbb{N}\}$, and hence we can define

$$C(\sigma) = \min\{C_{M_e}(\sigma) + e + 1 : e \in \mathbb{N}\},$$

to be *the* Kolmogorov complexity of σ. Notice that we could implement C via machine U where, on input $0^e1\tau$, U emulates the action of $M_e(\tau)$. Note that we would have that for any machine M, $C(\sigma) \leq C_M(\sigma) + O(1)$. Hence we may define a notion of compression *up to a constant.* There will be a unique string z of length $C(\sigma)$ such that

(i) $U(z)[s] = \sigma$,
(ii) s is the first stage where there is a string of length $C(\sigma)$ and (i) holds.
(iii) z is the lexicographically least such string.

Then we will denote z by σ^*. (Strictly speaking, we should use σ^*_C, to indicate that we are using C, since later there will be other measures of complexity. However, we anticipate that things will be clear from context.) The reader will note that x^* contains a lot of information. If I am given x^* then I can generate x (by running U) and $C(x)$ by looking at x^*'s length. For a pair $\langle x, y\rangle$ we denote by

(i) $C(x, y)$ the Kolmogorov complexity of the pair $\langle x, y\rangle$, that is $C(\langle x, y\rangle)$ and
(ii) $C(x|y)$ the Kolmogorov complexity of the string x, *given* the string y. (Here we have machines M which take as input the pair p, q and calculate $C(p)$ given the information q as an oracle. We call $C(x|y)$ the *conditional Kolmogorov complexity of x given y.*) Notice that $C(x) = C(x|\lambda) + O(1)$, where λ denotes the empty string.

Then the observations above show that the following is true.

Proposition 2.1:

(i) $C(x, C(x)) = C(x^*) + O(1)$.
(i) $C(x|x^*) = O(1)$
(iii) $C(x, C(x)|x^*) = C(x^*|C(x), x) = O(1)$.
(iv) $C(xy) \leq C(x, y) + O(1)$ where xy denotes the concatenation of x and y.

The basic theory of plain Kolmogorov complexity is based upon the following straightforward counting result.

Theorem 2.1: (Kolmogorov [35])

(i) $C(x) \leq |x| + c$
(ii) $|\{x : |x| = n \wedge C(x) \leq n + c - j\}| = O(2^{n-j})$.

Definition 2.1: (Kolmogorov [35]) We say that a string x is (C-)random iff $C(x) \geq |x|$.

We emphasize that Theorem 2.1 is a *combinatorial fact*, which only has an interpretation in algorithmic information theory. Thus we may define the following.

Definition 2.2: (Nies, Stephan and Terwijn [70]) We say that $F : \Sigma^* \to \Sigma^*$ is a *compression function* if for all x $|F(x)| \leq C(x)$ and F is 1-1.

Using any compression function, we can define C_F, the "Kolmogorov complexity" relative to F as $C_F(x) = |F(x)|$. Clearly, the Theorem 2.1 holds for any compression function, by the same counting argument. This observation will proves very useful later when we meet the results of Nies, Stephan and Terwijn [70] and of Miller [56] Here is an easy application of the use of compression functions. We begin with a simple observation.

Proposition 2.2: (Folklore)

(i) Consider the "C-overgraph"

$$M_C = \{\langle x, y\rangle : C(x) < y\}.$$

Then C_M is weak truth table complete. Indeed $\overline{R_C}$, the collection of non-C-random strings, is wtt-complete.

(ii) The collection of C-random strings is immune.

Proof: (i) To define a reduction, for each n computably pick a length $g(n)$, so that g is 1-1, and $g(n) > n_0$ is sufficiently large to make the following work. At each stage s, we will have a fixed string $\sigma(n, s)$ of length $g(n)$ and the reduction will be that $n \in \emptyset'$ iff $\sigma(n) = \lim_s \sigma(n, s)$ is not random. Initially we choose $\sigma(n, s)$ to be random at stage s. Whilst $n \notin \emptyset'_t$, should $C_t(\sigma(n, t)) < g(n) + c$ (c being the relevant constant for randomness), we will pick a new string $\sigma(n, t + 1)$ to be the next stage t random string of length $g(n)$. Finally, should n enter $\emptyset'$ at some stage u, then we can use the Recursion Theorem to drop the complexity of $\sigma(n, u)$ to below $g(n) + c$. (This is where we would need $g(n)$ to be large enough.)

(ii) Let $A = \{x : C(x) \geq \frac{|x|}{2}\}$. Then A is immune. A is infinite by Theorem 2.1. Suppose that A has an infinite c.e. subset B. Let $h(n)$ be defined as the first element of B to occur in its enumeration of length above n. Then

$$C(h(n)) \geq \frac{|h(n)|}{2} \geq \frac{n}{2}, \text{ but,}$$

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

For large enough n this is a contradiction. □

Now note that that the collection of compression functions forms a Π^0_1 class. The function C is easily seen to be Turing complete. (see Theorem 2.2) However, by the Low Basis Theorem, there must be compression functions which have low degrees and contrasts (i) above. Now note that for for such a low F, if a string is C_F-random it is certainly C-random. Thus in spite of the fact that (ii) above says that there is no infinite c.e. set of C-randoms, we do have an amenable class within the set of C-randoms by all of this. To wit:

Proposition 2.3: There is a low infinite collection of C-random strings.

We will see much deeper applications of this idea when we meet the results of Nies, Terwijn and Stephan [70] later.

We remark that there has been significant investigation of the natural c.e. set M_C, particularly by An A. Muchnik. It is relatively easy to see that since the collection of C-randoms is immune, M_C is not m-complete. Kummer however, proved that the adaptive nature of the reduction in Proposition 2.2 if *not* necessary. Kummer's technique is interesting in that the argument, whilst guaranteeing the existence of a *tt*-reduction, is nonuniform in that we don't know *which* tt-reduction works, and provably so.

Theorem 2.2: (Kummer [44]) $\overline{R}_C$ is truth table complete.

Proof: (Sketch) Kummer's proof is relatively intricate, but the idea is straightforward enough. First, the idea of Proposition 2.2 is replaced by using *blocks* of elements. That is, for each x we will attempt to define a block of elements $S_{i,x}$ so that $x \notin \emptyset'$ iff $S_{i,x}$ only contains C-random reals. Naturally enough, it is within *our* power to be able to drop the complexity of one of the members of any such $S_{i,x}$. But it is also within the power of the opponent to also drop such complexity. The clever part of Kummer's proof is how to be able to select the $S_{i,x}$ so that the opponent can't do this. Roughly speaking, Kummer's idea is to associate (perhaps temporarily) a block of elements from some size n with x, and when they go bad, we use another block, perhaps of a larger length. Different requirements can choose the same length, things being sorted out by priorities. However, the size of blocks are arranged so that $S_{i,x}$ will only be reset at most i times

for some $i \leq 2^{2d+2}$ where d is a parameter from the Recursion Theorem. (This argument uses the pigeonhole principle.) Then in the end using the parameter i_0, the largest i which is reset infinitely often, we will be able to argue that the tt-reduction works for that i_0.

Full details can be found in Kummer [43], and Downey-Hirschfeldt [19]□

Similar (and easier) methods can be used to show the following. We give its proof as an illustrative example.

Theorem 2.3: (An. A. Muchnik [65]) The collection

$$M = \{(x, y, n) : C(x|y) < n\}$$

is creative[a].

Proof: The construction will have a parameter d which can be worked out in advance, and known by the recursion theorem. For our purposes think of d in the following big enough to make everything work. We will construct a series of (possible) m-reductions g_x for $x \in [1, 2^d]$. Then for each z either we will know that z enters $\emptyset'$ computably, or there will be a unique y such that $g_x(z) = (x, y, d)$ and $x \in \emptyset'$ iff $g_x(z) \in M$. For some maximal x for which we enumerate elements $g_x(v)$ into M infinitely often, this will then give the m-reduction since on those elements which don't computably enter $\emptyset'$, g_x is (computable) and defined.

Construction For each active $y \leq s$, find the least $q \in [1, 2^p]$ with

$$(q, y, d) \notin M_s.$$

(Notice that such an x needs to exist since $\{q : (q, y, d) \in M\} < 2^d$.)

If this q is new at stage $s + 1$, (that is, $(q', y, d) \notin M_s$ for some $q' < q$) find the least z with $z \notin \emptyset'[s + 1]$ and define

$$g_q(z) = (q, y, d).$$

Now for any v, if v enters $\emptyset'[s + 1]$, find the largest r, if any, with $g_r(z)$ defined. If one exists, enumerate $g_r(z)$ into M. Find $\hat{y}$ with $g_r = (r, \hat{y}, d)$. Declare that $\hat{y}$ is no longer active. (Therefore, we will do this exactly once for any fixed $\hat{y}$ so the cost is modest, and known by the Recursion Theorem.)
End of Construction

[a]This proof can be made to work for any of the usual complexity measures, such as K which we meet in the next section, and for monotone complexity.

Note that there must a largest $x \leq 2^d$ such that $\exists^\infty v(g_x(v) \in M)$. Call this x. We claim that g_x is the required m-reduction. Work in stages after which g_{x+1} enumerates nothing into M.

Given z, since g_x is defined on infinitely many arguments and they are assigned in order,we can go to a stage s where either z has entered $\emptyset'[s]$, or $g_x(z)$ becomes defined, and $g_x(z) = (x, y, d)$ for some active y. $g_x(z)$ will be put into M should z enter $\emptyset'$ after s. The result follows. □

The reductions in these theorems are exponential (or worse) in the number of queries they use, and there has been a lot of fascinating work by Allender and others looking at what can be *efficiently* reducible to sets of random strings. This may seem strange indeed, but these questions seem to have a lot to say about complexity classes. For instance, one open hypothesis is that $PSPACE$ is precisely the collection of computable sets in $\cap_V P^{R_C^V}$, where R_C^V denotes the collection of random strings with universal machine V. (see Allender et. al. [1], Allender, Buhrmann, and Koucký [2].)

2.2. *Symmetry of Information*

We would like that $C(xy) \leq C(x) + C(y) + O(1)$. This, however, is *not* true in general. The problem is how to combine x^* and y^*. In fact, for sufficiently long strings, we always have compressible initial segments.

Lemma 2.1: (Martin-Löf [54]) Let k be given. Suppose that z is sufficiently long. The there is an initial segment x of z whose complexity is below $|x| - k$. Hence if z is C-random and we write $z = xy$,

$$C(z) > C(x) + C(y).$$

Proof: Take some initial segment q of z. This string is the r-th string of $2^{<\omega}$ under the standard length/lex ordering. Let x denote the initial segment of z of length $|q| + r$. Note that $C(x) \leq r + O(1)$, since to figure out x we need only input the final segment m of x following q, read its length which is r, use that to resurrect q and then output $qm = x$. It is easy to arrange q so that $r < |x| - k$. □

The following powerful theorem gives the precise relationships between $C(xy)$ and $C(x)$ and $C(y)$. The *information content* of a string y in a string x is defined as

$$I(x : y) = C(y) - C(y|x).$$

Theorem 2.4: (Symmetry of Information, Levin and Kolmogorov [102])

$$\begin{aligned} I(x:y) &= I(y:x) \pm O(\log n) \\ &= I(y:x) \pm O(\log C(x,y)) \end{aligned}$$

where $n = \max\{|y|, |x|\}$.

Levin and Kolmogorov's Symmetry of Information Theorem will follow from the reformulation below.

Theorem 2.5: (Symmetry of Information-Restated)

$$C(y|x) + C(x) = C(x,y) \pm O(\log C(x,y))$$

Theorem 2.4 will follow from Theorem 2.5 by the following calculation:

$$\begin{aligned} C(\langle x,y\rangle) &= C(y) + C(x|y) \pm O(\log C(x,y)) \\ &= C(x) + C(y|x) \pm O(\log C(x,y)) \\ \text{then } C(x) - C(x|y) &= C(y) - C(y|x) \pm O(\log C(x,y)) \end{aligned}$$

Proof: (of Theorem 2.5) The following neat proof follows that of Li-Vitanyi [50]. First it is easy to see that $C(x,y) \leq C(x) + C(y|x) \pm O(\log C(x,y))$, since we can describe $\langle x,y\rangle$ via a description of x, of y given x and an indication of where to delimit the two descriptions.

For the hard direction, that

$$C(\langle x,y\rangle) \geq C(y) + C(x|y) \pm O(\log C(x,y)),$$

define two sets

$$A = \{\langle u,v\rangle : C(\langle u,v\rangle) \leq C(\langle x,y\rangle), \text{ and}$$

$$A_u = \{v : \langle u,v\rangle \in A\}.$$

A is finite and uniformly computably enumerable given $\langle x,y\rangle$, as is A_u for each u. Hence, one can describe y given x and its place in the enumeration order of A_x and given $|C(x,y)|$.

We take $e \in \mathbb{N}$ such that $2^{e+1} > \text{card}(A_x) \geq 2^e$. Then

$$\begin{aligned} C(y|x) &\leq \log \text{card}(A_x) + 2|C(\langle x,y\rangle)| + O(1) \\ &\leq e + O(\log C(x,y)). \end{aligned}$$

Now consider the set $B = \{u : |A_u| \geq 2^e\}$. It is clear that $x \in B$. We see

$$\mathrm{card}(B) \leq \frac{\mathrm{card}(A)}{2^e} \leq \frac{2^{C(\langle x,y\rangle)}}{2^e}.$$

This is independent of the pairing function used, provided the function is 1-1. Note that $\mathrm{card}(\cup_u A_u) \leq \mathrm{card}(A)$.

Then, to specify x, we take $C(x, y)$ and e we can computably enumerate the strings which are possibilities u for x by satisfying

$$A_u = \{z : C(u, z) \leq C(x, y)\} \text{ and,}$$

$$2^e < \ \mathrm{card}(A_u).$$

Therefore,

$$\begin{aligned} C(x) &\leq |e| + \log \frac{2^{C(\langle x,y\rangle)}}{2^e} + O(\log C(x, y)) \\ &\leq C(\langle x, y\rangle) - e + O(\log C(x, y)), \end{aligned}$$

and thus

$$C(x) + C(y|x) \leq C(\langle x, y\rangle) + O(\log C(x, y))$$

as required. □

2.3. *Prefix-free complexity*

We would like that the information contained in the *bits* of x^* encapsulates the complexity of x. Now, Theorem 2.1, says that for C this is not so. x^* gives $|x^*|$ *plus* $\log |x^*|$ many bits of information. It was Levin [51], [102] who finally figured out how to define complexity so that this formal relationship held. He did do using monotone machines (which ask that if $\sigma \prec \tau$, then $M(\sigma) \preceq M(\tau)$, should they both halt), and later both he and Chaitin [9] used the notion of a prefix-free machine. Recall that a set of strings S is called *prefix-free* if whenever $\sigma \in S$ and $\sigma \prec \tau$, then $\tau \notin S$. Then we may define *prefix-free Kolmogorov complexity* as the same as C except that only prefix-free machines, that is ones with prefix-free domains, are allowed. Note that the same proof shows that there are universal prefix-free machines. We let K denote prefix-free complexity.

Prefix-free machines and prefix-free Kolmogorov complexity will play a central role in our story. Note that if a machine M has prefix-free domain,

then its domain has (Lebesgue) measure. That is, for $\sigma \in 2^{<\omega}$, we recall that $\mu([\sigma]) = 2^{-|\sigma|}$, we note that by prefix-freeness a prefix-free machine's domain has measure, called its *halting probability*.

$$\mu(M) = \sum_{M(\sigma)\downarrow} 2^{-|\sigma|}.$$

The following result gives an *implicit* way of constructing prefix-free machines and will be used extensively in the rest of these notes. The result says, roughly, if the lengths needed for some prefix-free machine work out, then there is such a machine.

Theorem 2.6: (Kraft [36], Kraft-Chaitin [9, 11]) Let $d_1, d_2, \cdots$ be a collection of lengths, possibly with repetitions, Then $\Sigma 2^{-d_i} \leq 1$ 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.

The result as stated here first appears in Chaitin [9], where the result is attributed to Pippinger.

Proof: Consider the correspondence $\Delta : [\sigma] \mapsto [0.\sigma, 0.\sigma + 2^{-|\sigma|})$ taking the string σ to an interval of size $2^{-|\sigma|}$, gives a correspondence between a set of disjoint intervals in $[0, 1)$ and a prefix-free set.

Consider first the following non-effective proof of the result. We are given the lengths $\{d_i : i \in \mathbb{N}\}$ in some random order. But suppose that we re-arrange these lengths in increasing order, say $l_1 \leq l_2 \leq \ldots$. Then we can easily choose disjoint intervals I_j, with the right end-point of I_n as the left endpoint of I_{n+1} and the length of I_{n+1} being $2^{-l_{n+1}}$. Then we can again use the correspondence by setting $[\sigma_n] = \Delta^{-1}(I_n)$.

Now in the case that the intervals are *not* presented in increasing order, how to effectivize this process? The following organizational device for the Chaitin [9] proof was suggested by Joe Miller. We will be given the strings $d_0, d_1, \ldots, d_n$ with d_n given at stage n. The idea is that, at each stage n, we have a mapping $d_i \mapsto [\sigma_i]$, $|\sigma_i| = d_i$, together with a binary string $x[n] = .x_1 x_2 \ldots x_m$ representing the length $1 - \sum_{j \leq n} 2^{-d_j}$, and ask that for each 1 in the string $x[n]$ that there is a string of precisely that length in $2^{<\omega} - \{\sigma_j : j \leq n\}$.

To continue the induction, at stage $n+1$, when a new length d_{n+1} enters, if position $x_{d_{n+1}}$ is a 1, then we can find the corresponding string $\tau_{d_{n+1}}$ in $2^{<\omega} - \{\sigma_j : j \leq n\}$ and set $\sigma_{n+1} = \tau_{d_{n+1}}$. Then of course we make $x_{d_{n+1}} = 0$ in $x[n+1]$.

If position $x_{d_{n+1}}$ is a 0, find the largest $j < d_{n+1}$ with $x_j = 1$, find the lexicographically least string τ extending τ_j of length d_{n+1}, let $\sigma_{n+1} = \tau$, and let $x[n+1] = x[n] - .\nu$ where ν is the string which is zero except for 1 in position d_{n+1}.

Notice that nothing changes in $x[n+1]$ from $x[n]$ except in positions j to d_{n+1}, and these all change to 1, with the exception of x_j which changes to 0. Since τ was chosen as the lexicographically least string in the cone $[\tau_j]$, there will be corresponding strings in $[\tau_j]$ of lengths $j-1, \ldots, d_{n+1}$, as required to complete the induction. □

In the proofs in the literature, we often refer to the requests "I would like a string of length m mapping to a string σ" as KC-*axioms,* written as $\langle m, \sigma\rangle$ or sometimes $\langle 2^{-m}, \sigma\rangle$. For a c.e. set of such requests, the result above says that they can be met provided that their measure request is possible; that is provided the sum of the first coordinates is ≤ 1.

What about K-randomness? The counting for C shows that $C(x) \leq |x| + c$ for all x. However, for K we have the following.

Lemma 2.2: (Chaitin [9, 11], Levin [46]) Let $f : \Sigma^* \to \mathbb{N}$. Suppose that $\sum_\sigma 2^{-f(\sigma)}$ diverges. (The prototype here is $f(x) = \log x$.)
Then $K(\sigma) > |\sigma| + f(\sigma)$ infinitely often.

Proof: Suppose that for all x, $K(x) \leq |x| + f(x)$. Then $\sum_{\sigma\in 2^{<\omega}} 2^{-K(\sigma)} \geq \sum_\sigma 2^{-(|\sigma|+f(\sigma))} \geq \sum_n \sum_{|\sigma|=n} 2^{-(n+f(n))} \geq \sum_n 2^n(2^{-(n+f(n))}) \geq \sum_n 2^{-f(n)} = \infty$, a contradiction, since $\sum_\sigma 2^{-K(\sigma)} \leq 1$, as the machine is prefix free. □

The analog of $C(x) \leq |x| + O(1)$ is given by the following basic result.

Theorem 2.7: (Counting Theorem, Chaitin [9])

(i) $K(x) \leq |x| + K(|x|) + \mathcal{O}(1)$.
(ii) For all n,

$$\max\{K(x) : |x| = n\} = n + K(n) + \mathcal{O}(1).$$

(iii) For any k,

$$|\{\sigma : |\sigma| = n \wedge K(\sigma) \leq n + K(n) - k\}| \leq 2^{n-k+\mathcal{O}(1)}.$$

Proof: (i) Let U be the universal prefix-free machine. Consider the special prefix-free machine M, which will halt only on strings of the form $z\sigma$,

provided that on input $U(z) = |\sigma|$. For such a string $z\sigma$, M outputs σ. Then $K_M(\sigma) = |(|\sigma|^*)| + |\sigma| + \mathcal{O}(1)$. Hence $K(\sigma) \leq |\sigma| + K(|\sigma|) + \mathcal{O}(1)$.□

For the proof of (ii), we will use the "semimeasure" method which originates with the work of Gács and Levin, and is cleverly exploited by Chaitin [11]. Chaitin defined an *information content measure* as a partial function $\widehat{K} : 2^{<\omega} \to \mathbb{N}$ such that

(i) $\sum_{\sigma \in 2^{<\omega}} 2^{-\widehat{K}(\sigma)} \leq 1$, and,
(ii) $\{\langle \sigma, k\rangle : \widehat{K}(\sigma) \leq k\}$ is c.e..

Chaitin's information content measures are more or less the same as the computably enumerable *discrete semimeasures* introduced by Gács [27] and Levin [47].

Definition 2.3: (Discrete semimeasure) A discrete semimeasure is a function $m : 2^{<\omega} \to \mathbb{R}^+ \cup \{0\}$ such that

$$\sum_{\sigma \in 2^{<\omega}} m(\sigma) \leq 1.$$

Here a function g is computably enumerable iff there is a computable function $h(\cdot, \cdot)$ such that h is nondecreasing in both variables, and $g(n) = \lim_s h(n, s)$ for all n, so that it is a special kind of Δ^0_2 function. For instance, the binary expansion of a halting probability of a prefix-free Turing machine gives a c.e. function $f(n)$ which is the value of the first n bits of this expansion.

An equivalent way to think of a discrete semimeasure is to identify $2^{<\omega}$ with $\mathbb{N}$ and think of $\mathbb{N}$ as being our measure space. Notice that under this identification, all strings are incompatible. Clearly, the standard Lebesgue measure we have looked at so far is *not* a discrete semimeasure. The standard Lebesgue measure is a *continuous* measure. (Continuous semi-measures give rise to yet another concept of randomness and relate to semimartingales, as we later see.) The discrete Lebesgue measure is $\lambda(\sigma) = 2^{-2|\sigma|-1}$. There is a computable enumeration $\{\widehat{K}_k : k \in \mathbb{N}\}$ of all information content measures (and similarly one of all computably enumerable discrete semimeasures). Thus, there is a universal minimal one:

$$\widehat{K}(x) = \min_{k \geq 0}\{\widehat{K}_k(x) + k + 1\}.$$

Information content measures and prefix-free machines, are essentially the same. Using Kraft-Chaitin, build a prefix-free machine M which emulates

precisely the information content measure $\widehat{K}$; namely for all σ, there is a $\tau \in \mathrm{dom}M$, such that $M(\tau) = \sigma$ and $K(\sigma) = |\tau| - O(1)$, and conversely. (Namely, at stage s, if we see $K_s(\sigma) = k$ and $K_{s+1}(\sigma) = k' < k$ enumerate a Kraft-Chaitin axiom $\langle 2^{-(k'+1)}, \sigma\rangle$ to describe M, and hence generate $\widehat{K} = K_M$. Thus we see that $\widehat{K}$ is within a constant of K, and is thus prefix-free Kolmogorov complexity. Henceforth we will identify K with $\widehat{K}$, without further comment.

Another restatement of all of this is obtained by letting m denote the minimal universal discrete semimeasure. We have the following.

Lemma 2.3: $K(\sigma) = -\log m(\sigma) + O(1)$.

Proof: (ii) and (iii) Now for the proof of (iii), from which (ii) follows. We note that

$$\sum_{n\in\Sigma^*} 2^{-K(n)} = \sum_{n\in\Sigma^*} \sum_{|\sigma|=n} 2^{-K(\sigma)}.$$

(Recall, that we are identifying a string with a unique number.) Thus, as $-\log(\sum_{|\sigma|=n} 2^{-K(\sigma)})$ is an information content measure (using $-\log(\sum_{|\sigma|=n} 2^{-|\sigma|})$ as a dyadic real and letting $\widehat{K}(n)$ as the first nonzero entry in this expansion.) Then as K is minimal, we have

$$2^{-K(n)+O(1)} \geq \sum_{|\sigma|=n} 2^{-K(\sigma)}.$$

Now for the sake of a contradiction suppose that there are more than 2^{n-k+c} strings of length n with $K(\sigma) < n + K(n) - k$. Let $F = \{\sigma : |\sigma| = n \wedge K(\sigma) < n + K(n) - k\}$. Suppose that $|F| = (1+\epsilon)2^{n-k+c}$. Then

$$2^{-K(n)+c} \geq \sum_{|\sigma|=n} 2^{-K(\sigma)} \geq$$

$$\sum_{\sigma\notin F} 2^{-K(\sigma)} + \sum_{\sigma\in F} 2^{-K(\sigma)} > (1+\epsilon)2^{n-k+c}2^{n-K(n)-k} > 2^{-K(n)+c},$$

a contradiction. □

2.4. *The Coding Theorem*

We have already seen that $K(\sigma) = -\log m(\sigma)$ up to a constant. There are of course many measures we can put on strings. A particularly useful one is the following.

Definition 2.4: Given a prefix-free machine D, let $Q_D(\sigma) = \mu(D^{-1}(\sigma))$

$Q_D(\sigma)$ is the probability that D outputs σ. The following is an important and useful basic theorem.

Theorem 2.8: (Coding Theorem) $-\log m(\sigma) = -\log Q(\sigma) + O(1) = K(\sigma) + O(1)$.

Proof: We note that $Q(\sigma) \geq 2^{-K(\sigma)} = 2^{-|\sigma^*|}$, since $D(\sigma^*) = \sigma$. Therefore $-\log Q(\sigma) \leq K(\sigma)$. But, $\sum 2^{-logQ(\sigma)} \leq \sum_\sigma Q(\sigma) \leq 1$. Hence, by minimality of K, $Q(\sigma) \leq K(\sigma) + O(1)$ and hence $Q(\sigma) = K(\sigma) + O(1)$, as required. □

From this proof, $-\log Q(\sigma)$ is a measure of complexity, and hence, by the minimality of K among measures of complexity, we know that $2^{-K(\sigma)} \leq Q(\sigma)$. By Theorem 2.8, we know that for some constant d,

$$2^{-K(\sigma)} \leq Q(\sigma) \leq d2^{-K(\sigma)}.$$

Thus we can often replace usage of K by Q.

2.5. *Prefix-free symmetry of information*

Because of its close approximation to information content, prefix-free Kolmogorov complexity can be more pliable than its plain cousin. For instance, we can attach one prefix-free machine M_1 to another M_2 and make a (prefix-free) machine M whose action is $M(\sigma\tau) = M_1(\sigma)M_2(\tau)$. This means that

$$K(xy) \leq K(x) + K(y) + O(1).$$

Additionally Symmetry of Information is more aligned to our intuition in the prefix-free case. We define the *K-information content* as

$$I(x : y) = K(y) - K(y|x).$$

(Here, we are using $K(y|x)$ in the same way as for C, meaning the conditional prefix-free complexity of x given y. Similar comments hold for the use of $x^* = x^*_K$, for instance, in this context.)

Theorem 2.9: (Symmetry of Information, Levin and Gács [27], Chaitin [9]) $I(\langle x, K(x)\rangle : y) = I(\langle y, K(y)\rangle : x) + O(1)$.

Note that, given the relationship $K(z, K(z)) = K(z*) + O(1)$, the Symmetry of Information Theorem for prefix-free complexity may be neatly rewritten as

$$I(x^* : y) = I(y^* : x) + O(1).$$

As with the C case, Levin's Symmetry of Information Theorem follows from a reformulation:

Theorem 2.10: (Symmetry of Information, Levin and Gács [27], Chaitin [9]) $K(x,y) = K(x) + K(y|x, K(x)) + O(1) = K(x) + K(y|x^*) + O(1)$.

Proof: To prove Theorem 2.9 from Theorem 2.10, by Theorem 2.10, we have $K(x,y) = K(x)+K(y|x,K(x))+O(1) = K(y)+K(x|y,K(y))+O(1)$, and hence,

$$K(y) - K(y|x, K(x)) = K(x) - K(x|y, K(y)) + O(1),$$

and Theorem 2.9 follows.

Now we turn to the proof of Theorem 2.10.

First we prove that

$$K(x,y) \leq K(x) + K(y|x, K(x)) + O(1).$$

Given x^* and $z = K^*(y|x, K(x))$, we can construct a prefix-free machine M which, upon input x^*z, will compute x and $K(x) = |x^*|$. It will then compute y from x and $K(x)$ and z

To finish we need to prove that

$$K(x,y) \geq K(x) + K(y|x, K(x)) + O(1).$$

To achieve this, we prove that

$$K(y|x^*) \leq K(x,y) - K(x) + O(1).$$

We run the computation of U assuming that exactly one string halts at each stage. Call this p_s at stage s. Then, at each stage s, compute $\langle x_s, y_s\rangle$ with

$$U(p_s) = \langle x_s, y_s\rangle.$$

By the Coding Theorem, Theorem 2.8, there is a constant c such that

$$2^{K(x)-c}(\sum_y Q(\langle x,y\rangle)) \leq 1,$$

for all x. (To see this, imagine we are building a machine V which, each time we see $U(p)\downarrow = \langle x,y\rangle$, declares a Kraft-Chaitin axiom $\langle |p|, x\rangle$. Then, relative to V, $Q_V(x) = \sum_y Q_U(\langle x,y\rangle)$, meaning that $\sum_y Q(\langle x,y\rangle) \leq Q(x) + O(1)$.)

We will now define a new conditional machine M using Kraft-Chaitin. With z on the oracle tape, M tries to compute z' with $U(z) = z'$, and hence

with x^* on the tape, computes x. M then simulates the machine M_x with the Kraft-Chaitin set

$$\langle |p_t| - |x^*| + c, y_t \rangle,$$

for each p_t of the form $\langle x, y_t \rangle$. Let W denote the computably enumerable collection of such requirements.

Notice that $\sum_{t \in W} 2^{-(|p_t| - |x^*| + c)} \leq 2^{K(x)-c}(\sum_y Q(\langle x, y \rangle)) \leq 1$, and hence Kraft-Chaitin can be applied to M_x.

For each p with $U(p) = \langle x, y \rangle$, there is a $\widehat{p}$ with $U(\widehat{p}|x^*) = M_x(\widehat{p}) = y$, and with $|\widehat{p}| = |p| - K(x) + c$. This shows that

$$K(y|x^*) \leq K(x, y) - K(x) + O(1). \qquad \square$$

Another way to express Theorem 2.10 is

Corollary 2.1: $K(x, y) = K(x) + K(y|x^*) + O(1)$.

2.6. *Prefix-free randomness*

Note that now there are really two possibilities for defining prefix-free randomness for strings. First we might think that a string should be random iff its shortest description is at least as long as it is. This gives what is described, perhaps nonstandardly, in [19] as being *weakly Chaitin random.* That is, σ is weakly Chaitin random iff $K(\sigma) > |\sigma|$. On the other hand, a string could be thought of as being random if it has maximum possible K-complexity, meaning that to describe the string you need $K(|x|)$ for the prefix-free-ness and $|x|$ many bits for the string: to wit, we will say that x is *strongly* Chaitin random iff $K(x) > |x| + K(|x|)$.

The following implications hold between the concepts.

Theorem 2.11: (Solovay [84])

(i) x is strongly Chaitin random[b] implies x is Kolmogorov random, but not conversely.
(ii) x is Kolmogorov random implies x is weakly Chaitin random, but not conversely.

[b]Strictly speaking this theorem is happening up to fixed constants. In Downey and Hirschfeldt [19], we refer to the "up to constant" behaviour as "essentially" behaviour. That is, for a fixed c, having $C(x) > |x| - c$ is to be "essentially Kolmogorov random,"for instance.

The first part of (ii) is immediate since each prefix-free machine is also a plain machine. We will not prove the "but not conversely" statements here since they involve relatively intricate constructions, and simply refer the reader to Downey and Hirschfeldt [19]. We will give a proof of (i)'s statement that every strongly Chaitin random string is Kolmogorov random, as it give the reader some insight into the methods used.

For the proof, the following concepts are useful. We define the *randomness deficiencies* as follows. Let c_C and c_K denote the relevant coding constants.

$$m_C(\sigma) = |\sigma| + c_c - C(\sigma), \text{ and,}$$

$$m_K(\sigma) = |\sigma| + K(|\sigma|) + c_K - K(\sigma).$$

Lemma 2.4: (Solovay [84]) For a string x, we have $m_K(x) \geq m_C(x) - O(\log m_C(x) + 2)$.

Assuming the Lemma, we can get (i) by observing that if x is strongly Chaitin random then for some constant c, $m_K(x) \leq c$. By the Lemma, we see that $m_C(x) - O(\log m_C(x) + 2) \leq c'$ for some fixed constant c' and hence $m_C(x) \leq c''$ for some fixed c''.

Proof: (of Lemma 2.4) We know $C(x) = |x| + c_C - m_C(x)$. Thus, $K(C(x)) = K(|x| + c_C - m_C(x)) \leq K(|x|) + K(c_C - m_C(x)) \leq K(|x|) + O(\log m_C(x) + 2)$. Next we prove the following claim.

$$K(x) \leq C(x) + K(C(x)) + O(1).$$

To see this Let U be a universal prefix-free machine and V a universal machine. We will define a prefix-free machine D via the following.

On input z, D first attempts to simulate U. Hence if $z = z_1 z_2$, then C will first simulate $U(z_1)$. It will then read exactly $U(z_1)$ further bits of input, if possible. These further bits of input will be some word z_3. D will then compute $V(z_3)$, and gives this as its output.

Notice that D is prefix-free because firstly U is, and if C halts on z, then $z = z_1 z_2$ with $U(z_1) \downarrow$, and $|z| = |z_1| + |U(z_1)|$. Thus all extensions of z_1 upon which D halts have the same length, and hence cannot be prefixes of other such strings. Let π_D be the coding constant of D in U.

Let y_3 be a minimal Kolmogorov program for x, and y_1 a minimal prefix-free program for $|y_3|$. Then $U(\pi_D y_1 y_3) = C(y_1 y_3) = V(y_3) = x$. hence $K(x) \leq C(x) + K(C(x)) + |\pi_D|$. This establishes the claim.

To finish the proof, using the claim we get the following calculation.

$$K(x) \leq |x| + K(|x|) + O(1) + O(\log m_C(x) + 2) - m_C(x).$$

Thus $0 \leq m_K(x) + O(\log m_C(x) + 2) - m_C(x)$. Hence,

$$m_K(x) \geq m_C(x) - O(\log m_C(x) + 2). \qquad \square$$

Actually the relationships between C and K are very complex. The following definitive results were obtained by Solovay [84].

Theorem 2.12: (Solovay [84])

$$K(x) = C(x) + C^{(2)}(x) + O(C^{(3)}(x)). \tag{1}$$

and

$$C(x) = K(x) - K^{(2)}(x) + O(K^{(3)}(x)). \tag{2}$$

Solovay [84] showed that (1) and (2) above are *sharp!* That is, for instance,

$$K(x) = C(x) + C^{(2)}(x) + C^{(3)}(x) + O(C^{(4)}(x))$$

is *not* true in general. The proof can be found in Downey and Hirschfeldt [19] and is, as you would expect, highly combinatorial.

2.7. *The overgraph functions*

Notice that, again, we can look at the "overgraph" functions. Now we consider

$$M_K = \{\langle x, y\rangle : K(x) < y\},$$

and the conditional case

$$M'_K = \{\langle x, y, z\rangle : K(x|y) < z\},$$

and finally

$$\overline{R}_K = \{x : K(x) \geq |x| + K(|x|) - c\}.$$

Using exactly the same proof, Muchnik proved that M'_K is m-complete. He also considered M_K. We remark that $\overline{R}_K$ is a tricky object to deal with. The point is that both sides of the definition vary in time. Ever since the manuscript of Solovay it has been open whether $\{x : K(x) < |x|+K(|x|)-c\}$ is computably enumerable. This was finally solved by Joe Miller in early 2005.

Theorem 2.13: (Miller [60, 61])

(i) Fix $c \geq 0$ and let $B = \{v : K(v) < |v| + K(|v|) - c\}$. If A contains B and has property (*) below, then A is not a c.e. set.

(*) For all n,

$$|A \cap 2^n| < 2^n.$$

(ii) Hence for all sufficiently large c, $B = \{v : K(v) < |v| + K(|v|) - c\}$ is not Σ^0_1.

We remark that it is not known whether $\overline{R}_K$ *can be* tt-complete. Here I say *can be* since Muchnik prove the following remarkable result which demonstrates that for prefix-complexity things can become machine dependent. Let M^Q_K denote set of strings that are not weakly Chaitin random relative to the universal machine Q, and similarly $\overline{R}^Q_K$.

Theorem 2.14: (Muchnik, An. A. [65]) There exist universal prefix-free machines V and U such that

(i) M^V_K is tt-complete.
(ii) M^U_K (and hence $\overline{R}^U_K$) is not tt-complete.

The proof of (ii) is fairly remarkable. In the construction we will be building a universal machine U and a set B diagonalizing against tt-reductions Γ_e making sure that $\Gamma_e^{M^U_K} \neq B$. To do this, we would pick some follower n and put n into B if there was some way to make $\Gamma_e^{M^U_K}(n) = 0$ and otherwise try to force $\Gamma_e^{M^U_K}(n) = 1$ and keep n out of B. The problem is that at any stage s, U and hence M^U_K are only in a state of formation. It is within the opponent's power to be able to drop the complexity of some string x and hence add some $\langle x, y\rangle$ into M^U_K. This might change the value of $\Gamma_e^{M^U_K}(n)$. We are in control of some part of U (about half in the actual construction) and it would be then in our power to possibly change some complexity to perhaps restore $\Gamma_e^{M^U_K}(n)$ to its previous value.

Muchnik's idea is to view this as a game played on a finite directed graph, with $(\langle x, y\rangle, \langle x, y'\rangle)$ an edge representing the dropping of the complexity of x from y to y'. Then, the whole thing can be viewed as a game played on a finite graph determining the value of $\Gamma_e^{M^U_K}(n)$, by moves alternatively by the opponent then us. There is a computable strategy for such finite games, and this strategy will determine what value to set $B(n)$ to be.

The details are a bit messy, but this is the fundamental idea. We refer the reader to either Muchnik and Positelsky [65] or Downey and Hirschfeldt [19].

3. Lecture 2: Randomness for reals

3.1. *Martin-Löf randomness*

It is a fascinating problem to give mathematical content to our intuition that the real $1111\ldots$ and any other real α are equally likely in terms of measure theory yet our intuition would be that the real of all 1's is not random. The first real attempt to address this question occurs in a remarkable paper by von Mises [94]. Von Mises was a probabilist, and suggested that a stochastic approach to "defining" randomness. To wit, he suggested that given a real $\alpha = a_1a_2\ldots$, if we were to "select" some subsequence assuming "acceptable" selection rules, say we choose positions $f(1), f(2)\ldots$, then we should have that the limit as n went to infinity of the number of $a_{f(i)} = 1$ divided by those with $a_{f(i)} = 0$ for $i \leq n$ should be 1. That is, in the limit, we should select equal numbers of 0's and 1's. This approach can be viewed as a generalization of the law of large numbers. Von Mises had no canonical way to formulate the notion of acceptable rule, but did observe that countable collections of selection rules could be dealt with. It remained until the clarification of the notion of a computable function for reasonable classes of f's to be suggested. For instance, we might suggest that something is stochastically random iff it defeats any computable selection rule. With a little care this gives rise to notions like Church randomness. As we will see later, von Mises approach has a lot to say about current research. However, in even the computable formulation of von Mises basic notion, the approach had several drawbacks. These are thoroughly discussed in van Lambalgen's thesis [92]. The first widely acceptable definition of randomness came from the fundamental work of Martin-Löf in 1966 in [54]. Martin-Löf's fundamental observation was that we can think of *effective* statistical tests as being *effective* null sets of reals. Thus a real should be random if it avoids all effective null sets. A computably enumerable open set would be a collection $W = \{[\sigma] : \sigma \in W_e\}$ for some e.

Definition 3.1: (Martin-Löf, [54]) 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 a computable collection of c.e. open sets a *test* since it corresponds to a statistical 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 meaning that it is not in the intersection. Since there are only countably many such tests, almost all reals

are Martin-Löf random.

Using the enumeration of all c.e. sets, we can enumerate all c.e. tests, $\{W_{e,j,s} : e, j, s \in \mathbb{N}\}$ and stops the enumeration of one if the measure $\mu(W_{e,j,s})$ threatens to exceed $2^{-(j+1)}$ at any stage s of the simultaneous enumeration. Then we can let

$$U_n = \cup_{e \in \mathbb{N}} W_{e,n+e+1}.$$

Then we note that U_n is a Martin-Löf test, and moreover, a real A passes all Martin-Löf tests iff $A \notin \cap_{n \in \mathbb{N}} U_n$. We have established the following.

Theorem 3.1: (Martin-Löf [54]) There exist *universal* Martin-Löf tests: That is there is a Martin-Löf test $\{U_n : n \in \mathbb{N}\}$ such that, for any Martin-Löf test $\{V_n : n \in \mathbb{N}\}$, $x \in \cap_{n \in \mathbb{N}} V_n$ implies $x \in \cap_{n \in \mathbb{N}} U_n$.

The reader should note the following alternative version of Definition 3.1.

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

The following is an easy exercise.

Theorem 3.2: (Solovay [84]) A real x is Martin-Löf random iff x is Solovay random.

3.2. *Schnorr's Theorem and the computational paradigm*

When we looked at strings, our approach to randomness centered around the computational/incompressibility paradigm. This approach for reals was pioneered by Levin [46,102] using monotone and prefix-free complexity, the latter also used by Chaitin [9]. We have seen that the plain complexity of sufficiently long strings will always drop, and this can be formalized for reals into the following.

Theorem 3.3: (Li-Vitanyi [50], also Staiger [85]) Let $f : \mathbb{N} \to \mathbb{N}$ be any total computable function. Suppose that $\sum_{n=1}^{\infty} 2^{-f(n)} = \infty$. Then for any real α, $C(\alpha \upharpoonright n|n) \leq n - f(n)$ infinitely often.

Corollary 3.1: (Li-Vitanyi [50], after Martin-Löf [55]) Let $f : \mathbb{N} \to \mathbb{N}$ be any total computable function, such that $\sum_{n=1}^{\infty} 2^{-f(n)} = \infty$, and such that, for all n, $C(n|n - f(n)) = \mathcal{O}(1)$. Then $C(\alpha \upharpoonright n) \leq n - f(n)$ infinitely often.

The prototypical application of Corollary 3.1 is $f(n) = \log n$ allowing us to conclude that $C(\alpha \upharpoonright n) \leq n - \log n$ infinitely often. Again we note that if we use a complexity whose interpretation is equivalent to bit complexity, then we remove the oscillations below n. This allows for the following definition.

Definition 3.2: (Levin(-Gács-Chaitin)) A real α is Levin-Gács-Chaitin random if for all n

$$K(A \upharpoonright n) \geq n - O(1).$$

The following fundamental theorem shows that the two notions of randomness coincide.

Theorem 3.4: (Schnorr) A real x is Levin-Gács-Chaitin random iff it is Martin-Löf random.

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

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

Since the universal machine is prefix-free, we can estimate the size of U_k.

$$\mu(U_k) = \sum\{2^{-|\sigma|} : K(\sigma) \leq n - k\}$$

$$\leq \sum_{n \in \mathbb{N}} 2^{-(n+k)} = 2^{-k}.$$

Hence the sets $\{U_k : k \in \mathbb{N}\}$ 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, $K(x \upharpoonright n) > n - k$.

For the converse direction, recall from Lecture 1 that K is a minimal information content measure so that for all σ, $K(\sigma) \leq K_k(\sigma) + \mathcal{O}(1)$. Now suppose that x is not Martin-Löf random, and hence $x \in \cap U_n$ with $\{U_n : n \in \mathbb{N}\}$ the universal Martin-Löf test (so that $\mu(U_n) \leq 2^{-n}$). We note that $\sum_{n \geq 3} 2^{-n^2+n} \leq 1$. We use Kraft-Chaitin to build a machine M. Whenever we see some $[\sigma]$ occur in U_{n^2} for $n \geq 3$, we enumerate an axiom for M of the form $|\sigma| - n$. The total cost of the M-axioms is found by the calculation:

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

Thus, if c is the coding constant for M in U, we have for all $\sigma \in U_{n^2}$ and $n \geq 3$,

$$K(\sigma) \leq |\sigma| - n + c.$$

Therefore, as $x \in \cap U_{n^2}$ for all $n \geq 3$ we see that $K(x \upharpoonright m) \leq m - n + c$, and hence it drops arbitrarily away from k. Hence, x is not Levin-Gács-Chaitin random. □

We can use Schnorr's Theorem to prove that there are many strings that are (weakly) Chaitin random yet are not Kolmogorov random.

Corollary 3.2: There are infinitely many n and strings x of length n such that

(i) $K(x) \geq n$ and
(ii) $C(x) \leq n - \log n$.

Proof: Let α be Martin-Löf random. Then by Schnorr's Theorem, Theorem 3.4, for all n, $K(\alpha \upharpoonright n) \geq n - O(1)$. But by Corollary 3.1, for infinitely many n, $C(\alpha \upharpoonright n) \leq n - \log n$. □

Schnorr's Theorem also allows us to define some *specific* kinds of random reals. For instance, the class

$$R = \cup_c R_c \text{ where } R_c = \{A : \forall n(K(A \upharpoonright n) \geq n - c\},$$

is the Σ^0_2 class of all Martin-Löf random reals. From some c onwards, the classes R_c are nonempty Π^0_1 classes of reals. By the Low Basis Theorem and Hyperimmunne-free Basis Theorem we have the following.

Theorem 3.5: (Kučera and others)

(i) There are low Martin-Löf random reals.
(ii) There are Martin-Löf random reals of hyperimmune-free degrees.

Actually, we can come up with a specific Martin-Löf random real. This is the famous example of Chaitin.

Theorem 3.6: (Chaitin [10], Chaitin's Ω) Let U be a universal prefix-free machine. Then Ω, the halting probability below, is Martin-Löf random.

$$\Omega = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|}.$$

Proof: We build a machine M and it has coding constant e given by the recursion theorem. (This means that if we put σ in $\mathrm{dom}(M)$, U *later* puts something of length $|\sigma| + e$ into $\mathrm{dom}(U)$.) Let $\Omega_s = \sum_{M(\sigma)\downarrow[s] \wedge |\sigma| \leq s} 2^{-|\sigma|}$. For $n \leq s$, if we see $K_s(\Omega_s \upharpoonright n) < n - e$, find some σ of $K_s(\Omega_s \upharpoonright n$ with

$U_s(\sigma) \mapsto \Omega_s \upharpoonright n$. Declare $M_s(\sigma)\downarrow$, which causes $\Omega_s \upharpoonright n \neq \Omega \upharpoonright n$. Note we cannot put more into the domain of M than U has in its domain and hence we may apply Kraft-Chaitin to build M. □

Solovay was the first to look at other computability-theoretical aspects of Ω. For instance, consider $D_n = \{x : |x| \leq n \wedge U(x)\downarrow\}$. Solovay proved that $K(D_n) = n + O(1)$, where $K(D_n)$ is the K-complexity for an index for D_n. Solovay also proved the following basic relationships between D_n and $\Omega \upharpoonright n$.

Theorem 3.7: (Solovay [84])

(i) $K(D_n|\Omega \upharpoonright n) = O(1)$. (Indeed $D_n \leq_{wtt} \Omega \upharpoonright n$ via a weak truth table reduction with identity use.)
(ii) $K(\Omega \upharpoonright n|D_{n+K(n)}) = O(1)$.

Proof: (i) is easy. We simply wait till we have a stage s where $\Omega_s =_{\rm def} \sum_{U(\sigma)\downarrow[s]} 2^{-|\sigma|}$ is correct on its first n bits. Then we can compute D_n.

The proof of (ii) is more involved. We follow Solovay [84]. Let $\hat{D} = D_{n+K(n)}$. Note that $K(n+K(n)|\hat{D}) = O(1)$. We can simply compute from $\hat{D}$, $K(j)$ for all $j \leq n+K(n)$, by looking for the length of the least $x \in D_n$ with $U(x) = j$. Hence we can find the least j such that $j+K(j) = n+K(n)$. Then we claim that $j - n = O(1)$. To see this note that

$$K(j) - K(n)| \leq K(|j - n|) + O(1).$$

Hence, $|j-n| \leq K(|j-n|)+O(1) \leq 2\log|j-n|+O(1)$. Therefore $|j-n| = O(1)$. Also this means $K(j|\hat{D}) = O(1)$, and hence $K(n|\hat{D}) = O(1)$.

We prove that there is a q such that $K(\Omega \upharpoonright n-q|\hat{D})O(1)$. We construct a machine M that does the following. $M(xy)$ is defined if

(i) $U(x) = n$.
(ii) $|y| = n$.
(iii) $\Omega \geq \frac{y}{2^n}$.

Here of course we are interpreting $y \in \{0, \ldots, 2^n - 1\}$. Now we can find q such that, for all n,

$$|\Pi_M| + K(n - q) + n - q \leq n + K(n).$$

But then,

$$\Omega \geq \frac{y}{2^{n-q}} \text{ iff } \Pi_M(n-q)^* y \in D_{n+K(n)}.$$

Therefore $K(\Omega \upharpoonright n-q|\hat{D}) = O(1)$, since $K(n|\hat{D}) = O(1)$. Clearly, $K(\Omega \upharpoonright n|\Omega \upharpoonright n-q) = O(1)$. Thus $K(\Omega \upharpoonright n|\hat{D}) = O(1)$, as claimed. □

In the light of Schnorr's Theorem, Solovay had asked whether $\liminf_s K(\Omega \upharpoonright n) - n \to \infty$. This was solved affirmatively by Chaitin. However, there is a very attractive generalization of this due to Miller and Yu who show that the complexity of a random real must be above n eventually by "quite a bit."

Theorem 3.8: (Ample Excess Lemma, Miller and Yu [63]) A real α is random iff

$$\sum_{n\in\mathbb{N}} 2^{n-K(\alpha\upharpoonright n)} < \infty.$$

Proof: One direction is easy. Suppose that α is not 1-random. Then we know that for all c, for infinitely many n, $K(\alpha \upharpoonright n) < n - c$. That means that $\sum_{n\in\mathbb{N}} 2^{n-K(\alpha\upharpoonright n)} = \infty$.

Now for the nontrivial direction. For the other direction, note that, for any $m \in \mathbb{N}$,

$$\sum_{\sigma\in 2^m}\sum_{n\le m} 2^{n-K(\sigma\upharpoonright n)} = \sum_{\sigma\in 2^m}\sum_{\tau\prec\sigma} 2^{|\tau|-K(\tau)}$$
$$= \sum_{\tau\in 2^{\le m}} 2^{m-|\tau|}2^{|\tau|-K(\tau)} = 2^m \sum_{\tau\in 2^{\le m}} 2^{-K(\tau)} \le 2^m,$$

by Kraft's inequality. Therefore, for any $p \in \mathbb{N}$, there are at most $2^m/p$ strings $\sigma \in 2^m$ for which $\sum_{n\le m} 2^{n-K(\sigma\upharpoonright n)} \ge p$. This implies that $\mu(\{\alpha \in 2^\omega : \sum_{n\le m} 2^{n-K(\alpha\upharpoonright n)} \ge p\}) \le 1/p$. Define $\mathcal{I}_p = \{\alpha \in 2^\omega : \sum_{n\in\mathbb{N}} 2^{n-K(\alpha\upharpoonright n)} \ge p\}$. We can express $\mathcal{I}_p$ as a nested union $\bigcup_{m\in\mathbb{N}}\{\alpha \in 2^\omega \mid \sum_{n\le m} 2^{n-K(\alpha\upharpoonright n)} \ge p\}$. Each member of the nested union has measure at most $1/p$, so $\mu(\mathcal{I}_p) \le 1/p$. Also note that $\mathcal{I}_p$ is a Σ^0_1 class. Therefore, $\mathcal{I} = \bigcap_{k\in\mathbb{N}} \mathcal{I}_{2^k}$ is a Martin-Löf test. Finally, note that $\alpha \in \mathcal{I}$ iff $\sum_{n\in\mathbb{N}} 2^{n-K(\alpha\upharpoonright n)} = \infty$. Now assume that $\alpha \in 2^\omega$ is 1-random. Then $\alpha \notin \mathcal{I}$, because it misses all Martin-Löf tests, so $\sum_{n\in\mathbb{N}} 2^{n-K(\alpha\upharpoonright n)}$ is finite. □

The following corollary was proven for f computable by Solovay.

Corollary 3.3: (Miller and Yu [64]) Suppose that f is an arbitrary function with $\sum_{m\in\mathbb{N}} 2^{-f(m)} = \infty$. Suppose that α is 1-random. Then there are infinitely many m with $K(\alpha \upharpoonright m) > m + f(m)$.

To finish this section we remark that it was a longstanding question whether there was a *plain complexity* characterization of 1-randomness. This was also solved by Miller and Yu, having been open for 40 years.

Definition 3.3: (Miller and Yu [63]) Define a computable function $G\colon \omega \to \omega$ by

$$G(n) = \begin{cases} K_{s+1}(t), & \text{if } n = 2^{\langle s,t\rangle} \text{ and } K_{s+1}(t) \neq K_s(t) \\ n, & \text{otherwise.} \end{cases}$$

Theorem 3.9: (Miller and Yu [63]) For $x \in 2^\omega$, the following are equivalent:

(i) x is 1-random.
(ii) $(\forall n)\ C(x \upharpoonright n) \geq n - K(n) \pm O(1)$.
(iii) $(\forall n)\ C(x \upharpoonright n) \geq n - g(n) \pm O(1)$, for every computable $g\colon \omega \to \omega$ such that $\sum_{n\in\omega} 2^{-g(n)}$ is finite.
(iv) $(\forall n)\ C(x \upharpoonright n) \geq n - G(n) \pm O(1)$.

3.3. *Martingales and the prediction paradigm*

The very earliest work on randomness was by von Mises [94] and involved *selection*, as we have already mentioned. This encapsulates the general view that random reals should be "unpredictable." Using computable functions, attempts were made to give a definition of randomness in terms of computable or partial computable selection procedures. This gives rise to notions of computable or partial computable stochasticity. It turned out that the correct way to formalize this notion of effective prediction was in terms of betting strategies.

Definition 3.4: (Levy [49]) A *martingale* is a function $f : 2^{<\omega} \to \mathbb{R}^+ \cup \{0\}$ such that for all σ,

$$f(\sigma) = \frac{f(\sigma 0) + f(\sigma 1)}{2}.$$

We say that the martingale *succeeds* on a real α if $\limsup_n F(\alpha \upharpoonright n) = \infty$.

Definition 3.5:

(i) A *supermartingale* is a function $f : 2^{<\omega} \to \mathbb{R}^+ \cup \{0\}$ such that for all σ,

$$f(\sigma) \geq \frac{f(\sigma 0) + f(\sigma 1)}{2}.$$

We say that the supermartingale *succeeds* on a real α if $\limsup_n F(\alpha \upharpoonright n) = \infty$.

(ii) Similarly we can define a *submartingale* and its success if we ask that

$$f(\sigma) \leq \frac{f(\sigma 0) + f(\sigma 1)}{2}.$$

Ville [95] proved that null sets correspond to success sets for martingales. They were used extensively by Doob in the study of stochastic processes.

The principal tool for using martingales is the classical result below. It says that the distribution of capital must be fair level by level.

Theorem 3.10: (Kolmogorov's inequality, see Ville [95])

(i) Let f be a (super-) martingale. For any string σ and prefix-free set $X \subseteq \{x : \nu \preceq x\}$,

$$2^{-|\nu|} f(\nu) \geq \sum_{x \in X} 2^{-|x|} f(x).$$

(ii) Let $S^k(f) = \{\sigma : f(\sigma) \geq k\}$, then

$$\mu(S^k(f)) \leq f(\lambda)\frac{1}{k}.$$

Schnorr showed that Martin-Löf randomness corresponded to effective (super-)martingales failing to succeed.

Definition 3.6: (Schnorr [78]) We will define a (super-, sub-)martingale f as being *effective* or *computably enumerable* if $f(\sigma)$ is a c.e. real, and at every stage we have effective approximations to f in the sense that $f(\sigma) = \lim_s f_s(\sigma)$, with $f_s(\sigma)$ a computable increasing sequence of rationals.

Theorem 3.11: (Schnorr [78]) A real α is Martin-Löf random iff no effective (super-)martingale succeeds on α.

Proof: We show that test sets and martingales are essentially the same. This effectivizes Ville's work. Firstly suppose that f is an effective (super-)martingale. Define open sets

$$V_n = \cup\{\beta : f(\beta) \geq 2^n\}.$$

Then V_n is clearly a c.e. open set. Furthermore, $\mu(V_n) \leq 2^{-n}$ by Kolmogorov's inequality. Thus $\{V_n : n \in \mathbb{N}\}$ is a Martin-Löf test. Moreover, $\alpha \in \cap_n V_n$ iff $\limsup_n f(\alpha \upharpoonright n) = \infty$, by construction. Hence f succeeds on α iff it fails the derived Martin-Löf test.

For the other direction, we show how to build a martingale from a Martin-Löf test. Let $\{U_n : n \in \mathbb{N}\}$ be a Martin-Löf test. We represent U_n by extensions of a prefix-free set of strings σ, and whenever such a σ is enumerated into $\cup_{n,s} U_n^s$, increase $F(\sigma)[s]$ by one. To maintain the martingale nature of F, we also increase F by 1 on all extensions of σ, and by 2^{-t} on the substring of σ of length $(|\sigma| - t)$. □

Corollary 3.4: (Levin [46,102], Schnorr [78])There is a universal effective martingale. That is there is an effective martingale f, such that for all martingales g, and reals α, f succeeds on α implies g succeeds on α.

Proof: Apply the proof above to the universal Martin-Löf test. □

Notice that any constant multiple of a martingale will succeed on a set exactly if the martingale does. The following strengthens Corollary 3.4 and is an analog to saying that K is a minimal information content measure.

Theorem 3.12: (Schnorr [78]) There is a *multiplicatively optimal* supermartingale. That is there is an effective supermartingale f such that for all effective supermartingales g, there is a constant c such that, for all σ,

$$cf(\sigma) \geq g(\sigma).$$

Proof: It is easy to construct a computable enumeration of all effective supermartingales, g_i for $i \in \mathbb{N}$. (Stop the enumeration when it threatens to fail the supermartingale condition.) Then we can define

$$f(\sigma) = \sum_{i \in \mathbb{N}} 2^{-i} g_i(\sigma).$$

□

3.4. *Supermartingales and continuous semimeasures*

In [48], Levin constructed a universal continuous semi-measure. This can be interpreted as Schnorr's result, as we now see.

Definition 3.7: A *continuous semimeasure* is a function $\delta : [2^{<\omega}] \to \mathbb{R}^+ \cup \{0\}$ satisfying

(i) $\delta([\lambda]) \leq 1$, and
(ii) $\delta([\sigma]) \geq \delta([\sigma 0]) + \delta([\sigma 1])$.

This would seem an appropriate effective analog of normal Lebesgue measure treating the space as 2^ω rather than $2^{<\omega}$.

Levin [48] directly constructed an optimal minimal semimeasure. However, for any supermartingale F, we can define

$$\delta([\sigma]) = 2^{-|\sigma|}F(\sigma),$$

and conversely. Then Schnorr's optimal supermartingale is equivalent to Levin's optimal semimeasure. We can also associate a version of Kolmogorov complexity to a semimeasure.

$$KM(\sigma) = -\log \delta([\sigma]),$$

where δ is the optimal semimeasure. Notice that

$$KM(\sigma) = -\log F(\sigma) + |\sigma| + O(1),$$

where F is an optimal supermartingale.

A cornerstone of algorithmic information theory is the Coding Theorem as we have already seen. This directly shows that the probability a string is output is essentially the same as K. In the case of continuous semimeasures, it is natural to ask for a similar result.

It turns out that the relevant complexity measure is *monotone complexity*. The idea is that attempt to give a real itself a complexity. Thus since we are thinking of our space as 2^ω we are covering the segments of a real by rather than strings. Thus we can imagine a computable real as being output from a machine V in segments. (Here the machines can now have infinite output.) We ask that for all σ, τ if $\sigma \preceq \tau$ and $M(\sigma)\downarrow, M(\tau)\downarrow$, then $M(\sigma) \preceq M(\tau)$. Now we can again develop Kolmogorov complexity using monotone machine and the resulting measure is called Km. Clearly all prefix-free machines are monotone machines. Levin showed that a real α is random iff for all n,

$$Km(\alpha \upharpoonright n) = n + O(1).$$

Levin [48] conjectured that the analogous Coding Theorem held for KM vs Km. That is, that $Km(\sigma) = KM(\sigma) + O(1)$ for all σ.

This attractive conjecture fails.

Theorem 3.13: (Gács [28])

(i) There exists a function f with $\lim_s f(s) = \infty$, such that for infinitely many σ,

$$Km(\sigma) - KM(\sigma) \geq f(|\sigma|).$$

(ii) Indeed, we may choose f to be the inverse of Ackermann's function.

Gács proof is very difficult, and it would be nice to have an accessible proof.

3.5. *Schnorr and Computable Randomness*

Schnorr argued that Theorem 3.11 showed a flaw in the definition of Martin-Löf randomness. He argued that randomness should be concerned with defeating *computable* strategies rather than computably enumerable strategies, since the latter are fundamentally asymmetric, in the same way that a computably enumerable set is semi-decidable rather than decidable. He proposed two variants of the notion of Martin-Löf randomness.

Definition 3.8: (Schnorr randomness, Schnorr [78])

(i) We say that a Martin-Löf test $\{V_n : n \in \mathbb{N}\}$ is a *Schnorr test* iff for all n,

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

(ii) We say that a real α is *Schnorr random* iff for all Schnorr tests, $\alpha \notin \cap_n V_n$.

Note here 2^{-n} can easily be replaced by any uniformly computable sequence of computable reals effectively converging to 0.

Definition 3.9: (Schnorr [78])

(i) A martingale f is called computable iff $f : 2^{<\omega} \to \mathbb{R}^+ \cup \{0\}$ is a computable function with $f(\sigma)$ (the index of functions representing the effective convergence of) a computable real. (That is, we will be given indices for a computable sequence of rationals $\{q_i : i \in \mathbb{N}\}$ so that $f(\sigma) = \lim_s q_s$ and $|f(\sigma) - q_s| < 2^{-s}$.)

(ii) A real α is called *computably random* iff for no computable martingale succeeds on α.

It is possible to give machine characterizations of both of the notions above. The one for computable randomness is a little untidy, but Downey and Griffiths [17] gave a nice characterization of Schnorr randomness in terms of *computable* machines. Here we say that a machine M is computable if the measure of its domain is a computable real. Recall here that a real is called computable iff its dyadic expansion is computable. The domains of prefix-free machines are, in general, only *computably enumerable* or *left computable* in the sense that they are limits of computable nondecreasing

sequences of rations. (For example $\Omega = \lim_s \Omega_s = \sum_{U(\sigma)\downarrow[s]} 2^{-|\sigma|}$.) Computably enumerable reals play the same role in this theory as computably enumerable set do in classical computability theory, and will be deal with in more detail later.)

Theorem 3.14: (Downey and Griffiths [17]) A real α is Schnorr random iff for all computable machines M, there is a constant c such that, for all n, $K_M(\alpha \upharpoonright n) \geq n - c$.

Proof: (sketch) Begin by showing that Kraft-Chaitin works to give a computable machine if the measure of the requirements happens to be a computable real. Then run through the translations of tests to machines and conversely to make sure that things work. □

Incidentally, it is possible to look at time bounded variations here and to look at, say, polynomial time computable prefix-free complexity. (Randomness in polynomial time tends to be studied by martingales.) Kraft-Chaitin in this setting would seem to be related to things like $P, NP, PSPACE$, but this remains unexplored.

There is one other related notion of randomness we should mention. We define a *Kurtz test* to be a a Σ^0_1 class of measure 1. Then a real A is called *weakly random* or *Kurtz random*[c] iff it passes all Kurtz tests. That is $A \in U$ for all such U. There is an easy equivalent notion in terms of null tests, implicit in Kurtz's Thesis [45], and explicit in Wang's.

Definition 3.10: (Wang [96]) A *Kurtz null test* is a collection $\{V_n : n \in \mathbb{N}\}$ of c.e. open sets, such that

(i) $\mu(V_n) \leq 2^{-n}$, and
(ii) There is a computable function $f : \mathbb{N} \to (\Sigma^*)^{<\omega}$ such that $f(n)$ is a canonical index for a finite set of σ's, say, $\sigma_1, \ldots, \sigma_n$ and $V_n = \{[\sigma_1], \ldots, [\sigma_n]\}$.

Theorem 3.15: (Wang [96], after Kurtz [45]) A real α is Kurtz random iff it passes all Kurtz null tests.

Proof: We show how measure 1 open sets correspond to Kurtz null tests. Let U be a c.e. open set with $\mu(U) = 1$. We define V_n in stages. To define

[c]Now it could be argued that weak randomness is not really a randomness notion at all, but rather a genericity notion. As we will see, the higher level version is highly relevant to our story.

V_1, enumerate U until a stage s is found with $\mu(U_s) > 2^{-1}$. The let $V_1 = \overline{U_s}$. Note that V_1 is of the correct form, to be able to define f. Of course for V_n we enumerate enough of U to have $\mu(U_{s_n}) > 2^{-n}$. For the converse reverse the reasoning. □

There are nice martingale characterizations of both Kurtz and Schnorr randomness.

Theorem 3.16: (Wang [96]) A real α is Kurtz random iff there is no computable martingale F and nondecreasing computable function h, such that for *almost all* n,

$$F(\alpha \upharpoonright n) > h(n).$$

Definition 3.11: We say that a computable martingale *strongly* succeeds on a real x iff there is a computable unbounded nondecreasing function $h : \mathbb{N} \to \mathbb{N}$ such that $F(x \upharpoonright n) \geq h(n)$ infinitely often.

Theorem 3.17: (Schnorr [78]) A real x is Schnorr random iff no computable martingale strongly succeeds on x.

Finally, Downey, Griffiths and Reid [18] gave a machine characterization of Kurtz randomness in terms of "computably layered" machines. It is not hard to see that amongst randomness notions, Martin-Löf implies computable implies Schnorr implies Kurtz. Building on earlier work of Schnorr, Wang, Downey, LaForte, Reid etc, a complete determination of when degree had reals of the various kinds of which were not of others. Nies, Stephan and Terwijn established the following definitive result.

Theorem 3.18: (Nies, Stephan and Terwijn [70]) For every set A, the following are equivalent.

(I) A is high (i.e. $A'' \geq_T \emptyset''$).
(II) $\exists B \equiv_T A$, B is computably random but not Martin-Löf random.
(III) $\exists C \equiv_T A$, C is Schnorr random but not computably random.

Outside the high degrees, things collapse.

Theorem 3.19: (Nies, Stephan and Terwijn [70]) Suppose that a set A is Schnorr random and does not have high degree. Then A is Martin-Löf random.

Proof: Suppose that A is not of high degree and covered by the Martin-Löf test $A \subset \cap_i U_i$. Let f be the function that computes on argument n the stage by which U_n has enumerated a $[\sigma] \in U_{n,s}$ with $A \in [\sigma]$. Note that f is A-computable, and hence computable relative to an oracle which is not high. It follows that there is a computable function g such that $g(n) > f(n)$ for infinitely many n. Then consider the test $\{V_i : i \in \mathbb{N}\}$, found by setting $V_i = U_{i,g(i)}$. The $\cup_i V_i$ is a Schnorr-Solovay test (that is, a Solovay test whose measure is a computable real), and hence A is not Schnorr random. □

Finally we remark that for some degrees *all* the randomness notions coincide.

Theorem 3.20: (Nies, Stephan, Terwijn [70]) Suppose that A is of hyperimmune-free degree. Then A is Kurtz random iff A is Martin-Löf random[d].

Proof: Suppose that A has hyperimmune free degree, and A is Kurtz random. Suppose that A is not Martin-Löf random. Then there is a Martin-Löf test $\{V_n : n \in \mathbb{N}\}$, such that $A \in \cap_n V_n$. Using A we can compute A-computably compute a stage $g(n)$ such that $A \in V_{g(n)}$, and without loss of generality we can suppose that $V_{g(n+1)} \supseteq V_{g(n)}$. But as A has hyperimmune free degree, we can choose a computable function f so that $f(n) > g(n)$ for all n. Then if we define $W_n = V_{f(n)}$, being a Kurtz null test such that $A \in \cap_n W_n$, a contradiction. □

We remark that there has been a lot of work trying to see if there is a a possible refutation of Schnorr's criticism by looking at computable supermartingales, where now, we are allowed to bet on the bits of the real, but *nonmonotonically*. We refer the reader to the paper of Merkle et. al. [58] and [66], the latter being where Muchnik, An. A., A. Semenov, and V. Uspensky introduced the notion of nonmonotonic betting.

4. Lecture 3: Randomness in General

4.1. *The de Leeuw, Moore, Shannon, Shapiro Theorem, and Sacks' Theorem*

The first relationship of measure theory and computability theory was discovered by de Leeuw, Moore, Shannon, and Shapiro [13] in 1956. Its proof

[d]Actually, Yu Liang observed that the *same* proof shows that A is Kurtz random iff A is weakly 2-random, a notion we meet in the next lecture.

uses an important method called the "majority vote" technique. Recall that an index e (such as the standard construction of $\emptyset'$) is universal if for all indices f and all sets S, there is a finite string σ_f such that

$$W_f^S = W_e^{\sigma_f \hat{} S}.$$

Definition 4.1: Define the *enumeration probability* of A as

$$P(A) = \mu(\{X \in 2^\omega : W_e^X = A\}.$$

Theorem 4.1: (de Leeuw, Moore, Shannon, and Shapiro, [13]) If $P(A) > 0$ then A is computably enumerable.

Proof: If $P(A) > 0$ then for some e, $D_e = \{X : A = W_e^X\}$ has positive measure. By the Lebesgue Density Theorem, there is a string σ such that the relative measure of D_e above σ is greater than $\frac{1}{2}$. If we let the oracles extending σ vote on membership in D_e, then we get the right answer. That is, enumerate n into A whenever more than half (by measure) of the extensions X of σ put n into W_e^X. □

Corollary 4.1: (Sacks) If A is noncomputable, then

$$A^{\leq_T} =_{\text{def}} \{B : A \leq_T B\},$$

has measure 0.

Solovay [84] examined the relationship between $P(A) > 0$ and the least index for $W_i = A$. Let

$$H(A) = \lceil -\log P(A) \rceil \text{ and,}$$

$$I(A) = \min\{K(i) : W_i = A\}.$$

Theorem 4.2: (Solovay [84])

$$I(A) \leq 3H(A) + K(H(A)) + O(1).$$

The proof is combinatorial, definitely nontrivial, and uses a clever lemma of Martin. It is unknown if the constant 3 can be improved. The point here is that the original proof using majority vote relies on the Lebesgue Density Theorem, and hence is highly noneffective in obtaining the index for A.

There have been a lot of extensions of the results above. For instance, the same technique can be used to prove the following.

Theorem 4.3: (Stillwell [89]) Suppose that $\mu(\{C : D \leq_T A \oplus C\}) > 0$. Then $C \leq_T A$.

At this stage a good exercise to test your understanding is to prove this result. An easy corollary to this result is the following.

Corollary 4.2: (Stillwell [89]) For any $\mathbf{a}, \mathbf{b}$, $(\mathbf{a} \cup \mathbf{b}) \cap (\mathbf{a} \cup \mathbf{c}) = \mathbf{a}$, for almost all $\mathbf{c}$.

Proof: Take $D \leq_T A \oplus B$. Then by Theorem 4.3, if $D \leq_T A \oplus C$ for more than a measure 0 set of C, $D \leq_T A$. Hence for almost all C,

$$D \leq_T A \oplus B \wedge D \leq_T A \oplus C \rightarrow D \leq_T A. \qquad \square$$

Similarly it can be shown that almost all degrees obey

$$\mathbf{a}' = \mathbf{a} \cup \mathbf{0}',$$

That is, almost all degrees are GL_1. Indeed (Stillwell), for almost all $\mathbf{b}$, $(\mathbf{a} \cup \mathbf{b})' = \mathbf{a}' \cup \mathbf{b}$, and $\mathbf{a}^{(\mathbf{n})} = \mathbf{a} \cup \mathbf{0}^{(\mathbf{n})}$. Similarly, for almost all $\mathbf{a}$ and $\mathbf{b}$, $\mathbf{a} \cap \mathbf{b} = \mathbf{0}$. These kind of arguments can be assembled into a nice result of John Stillwell.

Theorem 4.4: The "almost all" theory of degrees is decidable.

Here, variables $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$ vary over arbitrary degrees. Terms are built from $'$ (jump), $\cup, \cap$. An atomic formula is one of the form $t_1 \leq t_2$ for terms t_1, t_2, and formulae in general are built from atomic ones and $\wedge, \neg$ and the quantifier $\forall$ interpreted to mean "for almost all.'

The proof is not difficult. For instance, the Corollary above allows us to compute the meet of two terms of the form $\mathbf{a_1} \cup \mathbf{a_2} \cup \cdots \cup \mathbf{0^{(f)}}$ and $\mathbf{a_1} \cup \mathbf{b_2} \cup \cdots \cup \mathbf{0^{(k)}}$ as $\mathbf{c_1} \cup \mathbf{c2} \cup \cdots \cup \mathbf{0}^{(\min\{\mathbf{f},\mathbf{k}\})}$, where $\mathbf{c_i}$ are variables common to both terms. For example $(\mathbf{a_1} \cup \mathbf{a_3} \cup \mathbf{0^{(4)}}) \cap (\mathbf{a_1} \cup \mathbf{a_5} \cup \mathbf{a_7} \cup \mathbf{0^{(6)}}) = \mathbf{a_1} \cup \mathbf{0^{(4)}}$.

These allow for giving normal forms for formulae, with Fubini's Theorem handling nested quantifiers. We refer to Stillwell [89] of Downey-Hirschfeldt [19] for full details.

4.2. *Coding into randoms*

The results above might lead us to suspect that it is not possible to code into random reals, in general. As we will see, this is not the case.

We begin with a famous result often attributed only to Gács [29], but whose first proof was by Kučera [37].

Theorem 4.5: (Kučera [37], Gács [29]) Every set is *wtt* reducible to a Martin-Löf random set.

It is by no means clear that this should be true. The problem is that a random real should not have information easily decodable, or else it would not be random. For instance, we could not expect that the reduction would be, say, an m-reduction. The most attractive proof of this result known to the author is due to Merkle and Mihailovic [57]. The following lemma is the key. It says that for any martingale d and any interval of length k, there are at least k paths extending v of length $\ell(\delta, k)$ where d cannot increase its capital more than a factor of δ while betting on I, no matter how d behaves.

Lemma 4.1: (Folklore, see Merkle and Mihailovic [57]) Given a rational $\delta > 1$ and $k \in \mathbb{Z}^+$, we can compute a length $\ell(\delta, k)$, such that for any martingale d, and any word w,

$$|\{w \in 2^{\ell(\delta,k)} : d(vw) \leq \delta d(v)\}| \geq k.$$

Proof: For any martingale d word w, and k we have

$$d(v) = 2^{-k} \sum_{|u|=k} d(vu).$$

By Kolmogorov's inequality, for any given ℓ and v the average of $d(vw)$ over words of length ℓ is $d(v)$. Thus we have

$$\frac{|\{|w| = \ell : d(vw) > \delta d(v)\}|}{2^\ell} < \frac{1}{\delta}.$$

Since $\delta > 1$, $1 - \delta^{-1} > 0$ and hence it will suffice to have $\ell(\delta, k) \geq \log \frac{k}{1-\delta^{-1}} = \log k + \log \delta - \log(\delta - 1)$. □

Now we prove the Kučera-Gács Theorem. This proof is due to Merkle and Mihailovic [57]. Let $r_0 > r_1 > \dots$ be a collection of positive rationals where the sequence β_i $i \in \mathbb{N}$ converges, where

$$\beta_i = \Pi_{j \leq i} r_j.$$

Let $\ell_s = \ell(r_s, 2)$. Partition $\mathbb{N}$ into intervals $\{I_s : s \in \mathbb{N}\}$ with I_s of size ℓ_s. The by Lemma 4.1, there for any word v, and any martingale d, there are at least two words w of length ℓ_s with $d(vw) \leq r_s d(v)$.

We will construct a language R to which a given set X is wtt reducible. At step s we will specify R on I_s. Let d be a universal c.e. martingale. We say that w of length I_s is *admissible* if $s = 0$ and $d(w) \leq \beta_0$, and for $s > 0$, if

$$d(vw) \leq \beta_s \text{ where } v = R \upharpoonright (I_0 \cup \dots \cup I_{s-1})$$

We can argue that at every step there are at least 2 admissible extensions. This is easily seen by induction and the choice of the β_i as the product of the r_j for $j < i$. Now to specify R, armed with $R \upharpoonright (I_0 \cup \cdots \cup I_{s-1})$, we will choose the lexicographically least admissible extension if $s \notin X$ and the lexicographically greatest one if $s \in X$. That ends the proof.

4.3. *Kučera Coding*

Using similar coding with blocks, Kučera was able to prove the following.

Theorem 4.6: (Kučera [37]) Suppose that $\mathbf{a} \geq \mathbf{0}'$. Then $\mathbf{a}$ is Martin-Löf random.

There are several proofs of this result. The first is to derive it as a direct corollary of the Kučera-Gács Theorem.

Proof: (First proof) To derive this result from the proof of the Kučera-Gács Theorem. The point is that in that proof, if $\emptyset' \leq_T X$, then X can figure out R, by calculating the leftmost and rightmost paths. Hence $X \equiv_T R$. □

We will also give Kučera's original proof which is interesting and useful in its own right.

Kučera's proof uses an auxiliary construction of a universal Martin-Löf test which particularly Kučera has found ingenious applications of.

Kučera's Construction of a universal Martin-Löf test: Given $n \in \mathbb{N}$, consider all indices $e > n$. For each such e, enumerate all elements of $W_{\{e\}(e)}$ into U_n (where we understand that $W_{\{e\}(e)}$ is empty if $\{e\}(e)$ is undefined) as long as the condition

$$\sum_{w \in W_{\{e\}(e)}} 2^{|w|} < 2^{-e}$$

is satisfied. Then

$$\sum_{w \in U_n} 2^{|w|} \leq \sum_{e > n} 2^{-e} = 2^{-n}.$$

It is not difficult to show that this is indeed a universal Martin-Löf test. The key ingredient in the proof of Theorem 4.6 is a fact about intersections of fat classes which resembles that used in the proof of the Kučera-Gács Theorem.

Lemma 4.2: Let P_n denote the complement of the n-th set of the universal Martin-Löf test constructed above. If A is Π^0_1, then there exists a

computable function $\gamma : \Sigma^* \times \mathbb{N} \to \mathbb{Q}^{>0}$ such that for any $w \in \Sigma^*$ and any $n \in \mathbb{N}$ then

$$P_n \cap A \cap [w] \neq \emptyset \quad \rightarrow \quad \mu(A \cap [w]) \geq \gamma(w, n).$$

The critical thing, again, is that the function γ is *computable*. Hence, bound the measure of $A \cap [w]$ effectively from below.

The proof of Theorem 4.6 resembles the proof of the Friedberg Cupping Theorem. We construct a perfect tree $T \leq_T \emptyset'$ such that $[T] \subseteq \overline{U_0}$ and every path codes a set $B \subseteq \mathbb{N}$. This coding will be effective due to the preceding lemma, which allows us to compute an effective lower bound for the measure of $\overline{U_0}$.

We B into an infinite path of $\overline{U_0}$. Set $T(\epsilon) = \epsilon$. Assume now for $n \in \mathbb{N}$, $T(\sigma)$ where $\sigma = B \upharpoonright n$ has been constructed, such that $T(\sigma) \prec \overline{U_0}$. To define $T(B \upharpoonright n+1)$, compute (computably from $\emptyset'$) the smallest number n_σ such that the leftmost and the rightmost path of $[T(\sigma)] \cap \overline{U_0}$ differ (such an n_σ has to exist since a path in $\overline{U_0}$ cannot be isolated). Let these be L_σ and R_σ, respectively. Choose $T(B \upharpoonright n+1) = L_\sigma \upharpoonright n_\sigma$ if $B(n) = 0$, $T(B \upharpoonright n+1) = R_\sigma \upharpoonright n_\sigma$, otherwise.

Suppose $B \geq_T \emptyset'$. Claim $B \equiv_T T(B)$. $B \geq_T T(B)$ follows immediately from the construction, which is computable from $\emptyset'$. To show $B \leq_T T(B)$, we employ Lemma 4.2. For instance, to compute $B(0)$, Lemma 4.2 gives us a lower bound on $\mu(\overline{U_0})$, say 2^{-b_0}, $b_0 \in \mathbb{N}$. We know then that the leftmost and the rightmost path of $\overline{U_0} \upharpoonright b_0$ must differ (the tree must branch because its measure is too large). Given $T(B) \upharpoonright b_0$ we compute $\overline{U_0}$ till it turns out to be the left- or rightmost path. Obviously, using Lemma 4.2, this decision procedure can be continued inductively to decide $B(n)$ for any $n \in \mathbb{N}$. That concludes the proof of Theorem 4.6.

The reader will immediately notice the similar use of left and right blocks as in the proof of Kučera-Gács. By the generalized low basis theorem, it can be seen that since the class of random is perfect, there are random reals of all jumps. Below $\mathbf{0'}$ this is still true but requires more elaborate methods.

Theorem 4.7: (Kučera [39], Downey and Miller [25][e]) If $\mathcal{P}$ is a Π^0_1 class such that $\mu(\mathcal{P}) > 0$, then $S \geq_T \emptyset'$ is Σ^0_2 implies that there is a Δ^0_2 real $A \in \mathcal{P}$ such that $A' \equiv_T S$.

[e]This results was stated without proof in Kučera [39], where he had constructed a high incomplete 1-random real.

Frank Stephan has shown that these random reals above $\mathbf{0}'$ are in essence the only computationally powerful reals.

Theorem 4.8: (Stephan [88]) Suppose that $\mathbf{a}$ is PA and 1-random. Then $\mathbf{0}' \leq_T \mathbf{a}$.

4.4. *n-randomness*

In the same way that the arithmetical hierarchy provides a calibration of computational power, we can analogously calibrate randomness.

Definition 4.2:

(i) A Σ^0_n test is a computable collection $\{V_n : n \in \mathbb{N}\}$ of Σ^0_n classes such that $\mu(V_k) \leq 2^{-k}$.
(ii) A real α is Σ^0_n-random or n-random iff it passes all Σ^0_n tests.
(iii) One can similarly define Π^0_n, Δ^0_n etc tests and randomness.
(iv) A real α is called *arithmetically random* iff for any n, α is n-random.

We warn the reader that whilst we can use open sets to define Martin-Löf randomness, we apparently need to be careful to use classes for higher levels. For example, take the Σ^0_2 class consisting of reals that are always zero from some point onwards. This Σ^0_2 class is *not* equivalent to one of the form $\{[\sigma] : \sigma \in W\}$ for some Σ^0_2 set W. However for n-randomness, this apparent difference is illusory.

Open sets can be resurrected in the $n > 1$ cases also, as we now see.

Lemma 4.3: (Kurtz [45]) Let $q \in \mathbb{Q}$. The predicate

$$\text{“}\mu(S) > q''$$

is uniformly Σ^0_n where S is a Σ^0_n class. The predicate

$$\text{“}\mu(S) < q''$$

is uniformly Σ^0_n where S is a Π^0_n class.

This Lemma allows for the following, which says that we are able to use open sets and $\Sigma^{\emptyset^{(n)}}_1$ open classes in place of Σ^0_{n+1} classes.

Theorem 4.9: (Kurtz [45], Kautz [34]) Let $q \in \mathbb{Q}$.

(i) For S a Σ^0_n class, we can uniformly (i.e. uniformly in q and a Σ^0_n index for S) computably compute the index of a $\Sigma^{\emptyset^{(n-1)}}_1$ class which is also an open Σ^0_n class $U \supseteq S$ and $\mu(U) - \mu(S) < q$.

(ii) For T a Π^0_n class T, we can uniformly computably compute the index of a $\Pi^{\emptyset^{(n-1)}}_1$ class which is also a closed Π^0_n class $V \subseteq T$ and $\mu(T) - \mu(V) < q$.
(iii) For each Σ^0_n class S we can uniformly in $\emptyset^{(n)}$ compute a closed Π^0_{n-1} class $V \subseteq S$ such that $\mu(S) - \mu(V) < q$. Moreover, if $\mu(S)$ is a real computable from $\emptyset^{(n-1)}$ then the index for V can be found computably from $\emptyset^{(n-1)}$.
(iv) For a Π^0_n class T we can computably from $\emptyset^{(n)}$ obtain an open Σ^0_{n-1} class $U \supseteq T$ such that $\mu(U) - \mu(T) < q$. Moreover, if $\mu(S)$ is a real computable from $\emptyset^{(n-1)}$ then the index for U can be found computably from $\emptyset^{(n-1)}$.

The upshot is that a real is $n+1$-random iff it is 1-random relative to $\emptyset^{(n)}$. We remark that at least for 2-randomness, this characterization is implicit in Solovay's notes [84], where he passes from randomness relativized to $\emptyset'$, and 2-randomness without comment.

With other randomness notions care is needed. Similar relativization will work with Schnorr and computable randomness, but if we define a set to be weakly n-random iff it is in each Σ^0_n class of measure 1, this is *not* the same as being Kurtz random relative to $\emptyset^{(n-1)}$, which is a genericity notion. The best we can do is the following.

Lemma 4.4: (Kurtz [45], Kautz [34]) Let $n \geq 2$.

(i) Then for any Σ^0_n class C we can uniformly and computably obtain the index of a $\Sigma^{\emptyset^{(n-2)}}_2$-class $\widehat{C} \subseteq C$ with $\mu(\widehat{C}) = \mu(C)$.
(ii) For any Π^0_n class V we can uniformly and computably obtain the index of a $\Pi^{\emptyset^{(n-2)}}_2$-class $\widehat{V} \supseteq V$ with $\mu(\widehat{V}) = \mu(V)$.
(iii) Thus, for $n \geq 2$, α is Kurtz n-random iff α is in every $\Sigma^{\emptyset^{(n-2)}}_2$-class of measure 1.

Note that Kurtz 2-randomness is very natural. A real is weakly 2-random iff it avoids all Π^0_2 nullsets. This means that it is not in $\cap_n U_n$ for any computable collection of c.e. open sets with $U_n \to 0$. These are just Martin-Löf tests without the radius of convergence being effective. Similarly, α is Kurtz n-random iff for every $\emptyset^{(n)}$ computable sequence of open $\Sigma^{\emptyset^{(n-2)}}_1$ classes $\{S_i : i \in \mathbb{N}\}$, with $\mu(S_i) \leq 2^{-i}$, $\alpha \notin \cap_i S_i$. Weak 2-randomness was first studied by Gaifman and Snir [30].

The following is more or less immediate.

Theorem 4.10: (Kurtz [45])

(i) Every n-random real is Kurtz n-random.
(ii) Every Kurtz $n+1$-random real is n-random.

None of these implications can be reversed even for degrees. (Kurtz [45], Kautz [34]) The most difficult non-containment can be shown by constructing for each CEA($\emptyset^{(n)}$) degree $\mathbf{a} > \mathbf{0}^{(n)}$ a weakly $n+1$-random real X computably enumerable in ($\emptyset^{(n)}$, with $X \oplus \emptyset^{(n)}$ of degree $\mathbf{a}$. But then any such $n+1$ random real Y must have $Y \oplus \emptyset^{(n)}$ of degree $\mathbf{0}^{(n+1)}$. This method is due to Downey and Hirschfeldt [19], and is *not* a relativization of the fact that one can have Kurtz random c.e. reals in every nonzero c.e. degree, but rather a finite injury argument over $\mathbf{0}^{(n)}$ argument.

4.5. *Notes on 2-randoms*

Before we turn to the general theory, and 0-1 laws I would like to mention some beautiful results of Nies-Stephan-Terwijn and Miller relating "natural" randomness notions to 2-randomness. I should remark that Veronica Becher and Santiago Figueira have examples of somewhat natural n-random sets, along the lines of Post's Theorem for classical computability. But our concern in the present section are for some completely unexpected results relating plain complexity to 2-randomness.

We have seen that Martin-Löf showed that no real can have $C(\alpha \upharpoonright n) \geq n - d$ for all n, due to complexity oscillations. But it might be possible that some other natural C-condition might guarantee randomness. We have already met one in Theorem 3.9. There was, however, an earlier natural condition which had been analysed in this context. We need the following definitions.

Definition 4.3: We say that a real α is *strongly Chaitin random* iff

$$\exists^{\infty} n[(K(\alpha \upharpoonright n) > n + K(n) - O(1)].$$

Definition 4.4: We say that α is *Kolmogorov random*[f] iff $\exists^{\infty} n[(C(\alpha \upharpoonright n) > n - O(1)]$.

[f]There are some problems with terminology here. Kolmogorov did not actually construct or even name such reals, but he was the first more or less to define randomness for *strings* via initial segment plain complexity. The first person to actually construct what we are calling Kolmogorov random strings was Martin-Löf, whose name is already associated with 1-randomness. Schnorr was the first person to show that the notions of Kolmogorov randomness and Martin-Löf randomness were distinct. Again we can't use Schnorr randomness since Schnorr's name is associated with a randomness notion using tests of computable measure. Similar problems occur with our definition of strongly

We have seen that, should they exist, every strongly Chaitin random real is Kolmogorov random. This follows by Solovay's Theorem 2.11. Strongly Chaitin random reals do exist.

Lemma 4.5: (Yu, Ding, Downey [100], after Solovay [84])

(i) Suppose that α is 3-random. Then

$$\exists^\infty n(K(\alpha \upharpoonright n) = n + K(n) + O(1).$$

(ii) Suppose that α is 3-random. Then

$$\exists^\infty n(C(\alpha \upharpoonright n) = n + O(1).$$

Proof: Consider the test $V_c = \{\alpha : \exists m \forall n(n > m \rightarrow K(\alpha \upharpoonright n) \leq n + K(n) - c)\}$. Now $K \leq_T \emptyset'$, and hence V_c is $\Sigma_1^{\emptyset''}$, and hence Σ_3^0. Now we estimate the size of V_c. We show in fact $\mu(V_c) \leq O(2^{-c})$. Let $U_{c,n} = \{x| \ (\forall m \geq n)K(y \upharpoonright m) \leq m + K(n) - c\}$. It suffices to get an estimate $\mu(U_{c,n}) = O(2^{-c})$ uniform in n since $V_c \subseteq \cup_{n\in\omega} U_{c,n}$. But $\mu(U_{c,n}) \leq 2^{-m}|\{\sigma : |\sigma| = m \ \ \& K(\sigma) \leq m + K(n) - c\}$ for any $m > n$ and by the Counting Theorem this last expression is $O(2^{-c})$. Thus this is a 3-Martin-Löf test. Hence (i) and thus (ii) follow. □

Now contrary to claims in the literature, no Δ_2^0 real is Kolmogorov random. (Yu, Ding, Downey [100]) The following clever argument generalized the technique of [100], and proved something much stronger.

Theorem 4.11: (Nies, Stephan and Terwijn [70]) Suppose that α is Kolmogorov random. Then α is 2-random.

Proof: Recall that our universal prefix-free machines are prefix-free relative to *all* oracles. Suppose that α is *not* 2-random. Let K' denote $K^{\emptyset'}$. Then for all c, $\exists^\infty n(K'(\alpha \upharpoonright n) < n - c$. Let σ denote the string witnessing this,

Chaitin random reals. These were never defined by Chaitin, nor constructed by him. They were first constructed by Solovay who has yet another well-known notion of randomness associated with him which is equivalent to 1-randomness. Indeed, Chaitin did have a notion of strongly Chaitin random reals, which is the same as 1-randomness, and is not widely quoted. However, again Chaitin *did* look at the associated notion for *finite* strings, where he proved the fundamental lemma that $K(\sigma) \leq n + K(|\sigma|) + O(1)$ which allows for the definition of the reals. It is also known that Loveland in his 1969 ACM paper proposed equivalent notions via uniform Kolmogorov complexity. Again, Loveland's name is commonly associated with yet another notion of complexity : Kolmogorov-Loveland stochasticity.

so that $U^{\emptyset'}(\sigma) = \alpha \upharpoonright n$. Let s be sufficiently large that $U^{\emptyset'}(\sigma) \downarrow [s]$, with $\emptyset'$ correct use. Then consider the plain machine M which runs as follows. M looks at the input ν and attempts to parse it as $\sigma'\tau$, where it runs U with oracle $\emptyset'[t]$ for t steps, where $t = |\tau|$ steps, and for all such simulations, and σ if it gets a result it outputs $U^{\emptyset'}(\sigma')[t]\tau$. Then for inputs with $t > s$, we have $M(\sigma\tau) = \alpha \upharpoonright n + t$, and hence α is not Kolmogorov random. □

Notice that the machine we construct above actually runs (or at least) can run in time polynomial in the size of the input. This then gives to following useful and somewhat remarkable result.

Corollary 4.3: (Nies, Stephan and Terwijn [70]) A real α is 2-random iff for all computable g, with $g(n) > n^2$, $\exists^\infty n(C^g(\alpha \upharpoonright n) \geq n - O(1))$, where C^g denotes the plain complexity with time bound $g(n)$ for computations of length n.

Proof: Use the proof above, noting that the plain machine runs in linear time. For the other direction, we lose a quantifier because of the time bound g. □

Miller, then somewhat later, Nies, Stephan and Terwijn were able to prove the following equally remarkable result.

Theorem 4.12: (Miller [56], Nies, Stephan and Terwijn [70]) A real α is 2-random iff α is Kolmogorov random.

The point here is that there is no *a priori* reason that Kolmogorov randomness (defined totally in terms of plain complexity) should coincide with anything involving K, especially given the complex relationships between these two complexities. We recall in Definition 2.2, we defined a compression function which was a function emulating U^{-1}, was $1-1$ and for all x $|F(x)| \leq C(x)$. This notion was invented by Nies, Stephan, and Terwijn for the theorem we are now considering. (The Miller proof was different, and more complex.) For a compression function F we can define F-Kolmogorov complexity C_F: α is F-Kolmogorov random iff $\exists^\infty n(C_F(\alpha \upharpoonright n) > n - O(1))$.

The critical lemma was the following.

Lemma 4.6: (Nies, Stephan, and Terwijn [70]) If Z is 2-random relative a compression function F, then Z is Kolmogorov F-random.

The final result if then obtained by using a low compression function to same a quantifier.

4.6. *Kučera strikes again*

We have seen that most random reals are not below $\mathbf{0}'$ and hence are not PA. Thus they are computationally feeble. However, Kučera showed that randoms do have *some* computational power. Kučera [39] showed that they can compute FPF functions. Recall that this means that they can compute a function g with $g(e) \neq \varphi_e(e)$ for all e. The point, however, is that in a construction, the ability to compute a DNC $\{0,1\}$-valued function (i.e. being PA) is a *positive* thing in that by saying what something is *not* we will know what it *is*. In the general case, being FPF only allows us to say what something is not. So this computational power is *negative*.

Kučera was able to prove a significant generalization of the fact that random reals are FPF. We need the following definition.

Definition 4.5: (Jockusch, Lerman, Soare, and Solovay [33]) (a) We define a relation $A \sim_n B$ as follows.

(i) $A = B$ if $n = 0$.
(ii) $A =^* B$ if $n = 1$.
(iii) $A^{(n-2)} \equiv_T B^{(n-2)}$, if $n \geq 2$.

(b) A total function f is called *n-fixed point free* (n-FPF) iff for all x,

$$W_{f(x)} \not\sim_n W_x.$$

Kučera was able to extend his earlier result that random reals were FPF with the following.

Theorem 4.13: (Kučera [40]) Suppose that A is $n+1$ random. Then A computes an n-FPF function.

The proof is not really difficult, but is rather clever, and involves extensive use of Kučera's construction of a universal Martin-Löf test. We refer the reader to [40] or Downey and Hirschfeldt [19]. Strictly speaking the proof only uses weak $n+1$-randomness.

4.7. *van Lambalgen's Theorem*

In this section, we will study independence results for random reals. We begin with a *central* result concerning randomness, which has turned out to play a very important role in the theory.

We begin with a simple Lemma.

Theorem 4.14: (van Lambalgen, Kurtz, Kautz)

(i) If $A \oplus B$ is n-random so is A.
(ii) If A is n-random so is $A^{[n]}$, the n-th column of A.
(iii) If $A \oplus B$ is n-random, then A is $n - B-$random.

Proof: (i) (e.g. $n = 1$.) If A is not random, then $A \in [\sigma]$ for infinitely many $[\sigma]$ in some Solovay test V. Then $A \oplus B$ would be in $\widehat{V}$, where $[\sigma \oplus \tau] \in \widehat{V}$ for all τ with $|\tau| = |\sigma|$ and $\sigma \in V$. The measure of $\widehat{V}$ is the same as V. (iii) and (ii) are similar. □

Similar methods also who that if $A \oplus B$ is random, then $A \not\leq_T B$ and hence there are no minimal random degrees. The most important fact is that the *converse* of Theorem 4.14 is also true.

Theorem 4.15: (van Lambalgen's Theorem [93])

(i) If A n-random and B is $n - A-$random, then $A \oplus B$ is n-random.
(ii) Hence, $A \oplus B$ is n-random iff A n-random and B is $n - A-$random.

Proof: Suppose $A \oplus B$ is not random. We have $A \oplus B \in \bigcap_n W_n$ where W_n is uniformly Σ^0_1 with $\mu(W_n) \leq 1/2^n$. By passing to a subsequence we may assume that $\mu(W_n) \leq 1/2^{2n}$.

Put

$$U_n = \{X \mid \mu(\{Y \mid X \oplus Y \in W_n\}) > 1/2^n\}.$$

Note that U_n is uniformly Σ^0_1. Moreover $\mu(U_n) \leq 1/2^n$ for all n, because otherwise we would have

$$\mu(W_n) > \mu(U_n) \cdot \frac{1}{2^n} > \frac{1}{2^n} \cdot \frac{1}{2^n} = \frac{1}{2^{2n}},$$

a contradiction.

Since A is random, it follows that $\{n \mid A \in U_n\}$ is finite. Thus for all but finitely many n we have $A \notin U_n$, i.e.,

$$\mu(\{Y \mid A \oplus Y \in W_n\}) \leq 1/2^n.$$

Put $V^A_n = \{Y \mid A \oplus Y \in W_n\}$. Then $\mu(V^A_n) \leq 1/2^n$ for all but finitely many n, and V^A_n is uniformly $\Sigma^{0,A}_1$. Moreover $B \in \bigcap_n V^A_n$, contradicting the assumption that B is random over A. □

This result will be used extensively in the next Lecture. Here is a really pretty application of van Lambalgen's Theorem.

Theorem 4.16: (Miller and Yu [63]) Suppose that A is random and B is n-random. Suppose also that $A \leq_T B$. Then A is n-random.

Proof: (We do $n = 2$.) If B is 2-random, then B is 1-Ω-random (as $\Omega \equiv_T \emptyset'$.) Hence by van Lambalgen's Theorem, $\Omega \oplus B$ is random. Thus, again by van Lambalgen's Theorem, Ω is 1-B-random. But $A \leq_T B$. Hence, Ω is 1-A-random. Hence $\Omega \oplus A$ is random, again by van Lambalgen's Theorem. Thus, A is 1-Ω-random. That is, A is 2-random.

For the case $n + 1$, there is a 1-random Z with $Z \equiv_T \emptyset^{(n)}$ by Kučera's Coding Theorem. If B is n-random then B is n-Z-random. Thus $B \oplus Z$ is random. Hence Z is n-B-random. Hence Z is n-A-random, as $A \leq_T B$. Thus A is n-random. □

Actually, Miller and Yu [63] have also proven for any (not necessarily random Z), any random below a Z-random is itself Z-random. (Of course, this does not use van Lambalgen.)

A nice corollary of van Lambalgen's Theorem and Sacks' Theorem is the following.

Corollary 4.4: (Kautz [34]) Let $n \geq 2$. Then if **a** and **b** are relatively n-random, they form a minimal pair.

Proof: Suppose that $D \leq_T, A, B$. Then $A \in \{E : \Phi_e^E = D\}$. By Sacks' Theorem, this set is a Π_2^D-nullset, and hence A is not 2-D-random, and hence not 2-B-random. □

4.8. *Effective 0-1 Laws*

Classically we know that any measurable class of reals closed under finite translations has measure 0 or measure 1. Stillwell's Theorem and other consideration suggest that there should be refined computability-theoretical analogs of this.

The following lemma is the real basis of these results.

Lemma 4.7: (Kučera-Kurtz, [34], Lemma IV.2.1) Let D be a real, and $n \geq 1$. Let T be a Π_n^D class of positive measure. Then T contains a member of every n-D-random degree. Moreover, if A is any n-D-random, then there is some string σ and real B such that $A = \sigma B$ and $B \in T$.

Proof: For simplicity, we do $n = 1$ with D computable, the general case being analogous. We let T be a Π_1^0 class of positive measure, and $S = \overline{T}$, so that there is a c.e. set of strings W with $S = \cup\{[\sigma] : \sigma \in W\}$. Moreover we can assume W is prefix-free.

Choose rational $r < 1$ with $\mu(S) < r$. We define tests. Let $E_0 = S$ and $E_{s+1} = \{\sigma\tau : \sigma \in E_s \wedge \tau \in W\}$. Then $\mu(E_s) \leq r^s$ by induction on s. Now suppose that for every B with $A = \sigma B$, $A \in S$. Then $A \in \cap_s E_s$, and hence A is not random. Thus for any random B, there is some σ with $\sigma B \in \overline{S} = T$. □

I remark that this can also be gotten from the lemma for Kučera Coding. The following is an immediate Corollary to this Lemma.

Corollary 4.5: (Kurtz [45], also Kautz [34])

(i) Every degree invariant Σ^0_{n+1}-class or Π^0_{n+1} either contains all n-random sets or no n-random sets.
(ii) In fact the same is true for any such class closed under translations, and such that for all A, if $A \in S$, then for any string σ, $\sigma A \in S$.

Here are some examples of results proven using this fact.

Corollary 4.6: (Kurtz and others)

(i) The class $\{A : A$ has non-minimal degree $\}$ has measure 1, and includes every 1-random set.
(ii) The class $\{A \oplus B : A, B$ form a minimal pair $\}$ has measure 1, and includes all 2-random but not every 1-random set.
(iii) The class $\{A : \deg(A)$ is hyperimmune $\}$ has measure 1 and includes all 2-random but not every 1-random set.

The proofs of (i) and (ii) are done by analyzing the proofs of almost everywhere behaviour. For instance (i) follows since no random real has minimal degree, and the part for 2-randoms follows by Corollary 4.4 We will prove (iii) in Lecture 5, where we will look at measure-theoretical injury priority arguments.

The second part of (ii) is trickier. It uses a result of Kučera.

Theorem 4.17: (Kučera [38]) If A and B are 1-random with $A, B <_T \emptyset'$ then A and B do not form a minimal pair.

Proof: If $\mathbf{a}$ is random then we have already seen that it is DNC. Choose a low random below $\mathbf{0}'$ and using van Lambalgen's Theorem, get another Turing incomparable with it Choose a low random below $\mathbf{0}'$ and using van Lambalgen's Theorem, get another Turing incomparable with it. It is a consequence of Kučera's priority free solution to Post's Problem (in [38]) that no pair of Δ^0_2 of FPF degrees form a minimal pair. □

Hirschfeldt, Nies, and Stephan [32] have shown that the degrees below such pairs are *K-trivial*.

4.9. *Omega operators*

Unfortunately, I don't have time to discuss the interesting results looking at Ω, or, rather, *Omegas* as operators on Cantor Space. Here we push the possible analogy that Ω looks like the halting problem. The first question was whether it was degree invariant.

In fact there are reals $A =^* B$ such that Ω^A and Ω^B are relatively random!

There are many other very interesting results such as the fact that that Omega operators are lower semicontinuous but not continuous, and moreover, that they are continuous exactly at the 1-generic reals. These results will hopefully be presented by one of the other co-authors at this conference, and we otherwise refer the reader to Downey, Hirschfeldt, Miller and Nies [21] for details.

5. Lecture 4: Calibrating Randomness

Our goal is to try to calibrate levels of randomness and the vehicle we will use is comparing initial segment complexities. The idea is that if the initial segment complexity of a real determines whether it is random, then it also should determine *how* random the relevant real is. Naturally, other approaches suggest themselves, supermartingale growth rates, etc. More on this later.

5.1. *Measures of relative randomness and the Kučera-Slaman Theorem*

One of the operators in classical computability theory is the jump operator. In some sense Ω, the halting *probability*, is a kind of analog to $\emptyset'$, the halting *set*. The fact that $\emptyset'$ is computably unique is Myhill's Theorem. Solovay [84] realized that Ω was apparently machine dependent, and proposed an analytic version of m-reducibility that he showed preserved randomness.

Definition 5.1: (Solovay [84]) 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 up to a constant factor. Solovay reducibility is particularly relevant to the measure-theoretical analog of the computably enumerable sets, the computably enumerable *reals*, which may be defined as the measures of the domains of prefix-free machines. If $\alpha \leq_S \beta$, then given a sequence of rationals converging to some β and f we can generate a sequence converging to α. We then get the following characterization of Solovay reducibility.

Lemma 5.1: (Calude, Hertling, Khoussainov, Wang [8]) For c.e. reals, $\alpha \leq_S \beta$ iff for all c.e. $q_i \to \beta$ and c.e. $r_i \to \alpha$, there exists a total computable g, and a constant c, such that, for all m,

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

The proof of this result applies equally well to a β computable sequence $q_i \to \beta$, and hence this lemma means that the ability to compute a close approximation to β (say the first n bits) allows us to compute α to within some close approximation (say 2^{-n+d}) means that the following holds.

Proposition 5.1: (Folklore) For any reals α and β, if $\alpha \leq_S \beta$, then $\alpha \leq_T \beta$.

Since there are only $O(2^{2d})$ many reals within a radius of 2^{-n+d} of a string representing a rational whose dyadic expansion has length n, it follows that $\leq_S$ has the *Solovay Property*

Proposition 5.2: (Solovay [84]) If $\alpha \leq_S \beta$ then there is a c such that, for all n,

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

The same also holds for C in place of K.

Thus we will regard $\leq_S$ as an initial segment *measure of relative randomness*. We can compactly write the facts expressed in Proposition 5.2 as

$$\leq_S \text{ implies } \leq_C, \text{ and,}$$

$$\leq_S \text{ implies } \leq_K .$$

Notice that, by Schnorr's Theorem, if $\Omega \leq_S \beta$, then β is Martin-Löf random.

There is a particularly nice characterization of $\leq_S$ in terms of $+$ for c.e. reals.

Lemma 5.2: (Downey, Hirschfeldt, Nies) $\alpha \leq_S \beta$, with α and β c.e. reals, iff there is a constant c and a c.e. real γ such that $c\beta = \alpha + \gamma$.

The proof is fairly easy. Roughly, the proof works by synchronizing the enumerations so that the approximation to α is "covered" by one for β, (i.e. $\alpha_{s+1} - \alpha_s$ generates a change in $c\alpha$ of the same order. Then we use the amount needed for this covering for α and the excess goes into $\gamma_{s+1} - \gamma_s$.

The formal statement of the lemma being used is the following.

Lemma 5.3: (Calude, Hertling, Khoussainov, Wang, [8]) 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,

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

Solovay reducibility is particularly relevant to computably enumerable reals as we soon see. Recall that such reals are the measures of the domains of prefix-free machines. Of course, if M is prefix-free, then $x = \mu(\mathrm{dom}(M))$ is the limit of the following computable increasing sequence of rations.

$$x = \lim_s x_s \text{ where } x_s = \mu(\mathrm{dom}(M_s)) = \sum_{M_s(\sigma)\downarrow} 2^{-|\sigma|}.$$

Equivalently, that is, we can define a c.e. real as the limit of a nondecreasing sequence of rationals. Solovay called a real β Ω-*like* if β was computably enumerable and $\Omega \leq_S \beta$. He remarked that he thought it was very interesting that many of the properties of Ω (which seems machine dependent) also held for Ω-like reals. The first piece of the puzzle was found by Calude, Hertling, Khoussainov, and Wang.

Theorem 5.1: (Calude, Hertling, Khoussainov, Wang [8]) Suppose that β is a c.e. real and that $\Omega \leq_S \beta$. Then β is a halting probability. That is, there is a universal machine $\widehat{U}$ such that $\mu(\mathrm{dom}(\widehat{U})) = \beta$.

Proof: Here we use Lemma 5.3. Suppose that we are given monotone enumerations $\Omega = \lim_s \Omega_s$ and $\beta = \lim_s \beta_s$, and f and c witnessing $\Omega \leq_S \beta$ so that for all rationals $q < \beta$, $f(q) \downarrow < \Omega$ and $2^c(\beta - q) > \Omega - f(q)$. We will build our machine M in stages using KC-axioms.

It is not hard to use c and f to speed up the enumeration of β so that such that for all s, $2^c(\beta_{s+1} - \beta_s) > \Omega_{s+1} - \Omega_s$. Then at stage s, suppose

that $U(\sigma)\downarrow$, so that σ enters the domain of U, and hence $\Omega_{s+1} - \Omega_s \geq 2^{-|\sigma|}$. We can assume that exactly on string enters the domain of U. Then $\beta_{s+1} - \beta_s \geq 2^{-(|\sigma|+c)}$. Hence we build M via the KC-axioms $\langle |\sigma| + c, U(\sigma)\rangle$. The result follows. □

The final piece of the puzzle was provided by the following lovely result of Kučera and Slaman.

Theorem 5.2: (Kučera and Slaman [41]) 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 $\beta_s \to \beta$ be a computable sequence of rationals converging to β monotonically. We assume that $\beta_s < \beta_{s+1}$. At stage s if $\alpha_s \in F_n^s$, do nothing, else put $(\alpha_s, \alpha_s + 2^{-n}(\beta_{s+1} - \beta_{t_s}))$ into F_n^{s+1}, where t_s denotes the last stage we put something into into F_n. 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. □

Corollary 5.1: For c.e. reals α the following are equivalent:

(i) α is Martin-Löf random.
(ii) For all c.e. reals, β, for all n, $K(\beta \upharpoonright n) \leq K(\alpha \upharpoonright n) + O(1)$.
(iii) For all c.e. reals, β, for all n, $C(\beta \upharpoonright n) \leq C(\alpha \upharpoonright n) + O(1)$.
(iv) For any version of Ω, for all n, $C(\Omega \upharpoonright n) \leq C(\alpha \upharpoonright n) + O(1)$ and $K(\Omega \upharpoonright n) = K(\alpha \upharpoonright n) + O(1)$.
(v) For all c.e. reals β, $\beta \leq_S \alpha$.
(vi) α is the halting probability of some universal machine.

Whilst we know that all reals have complexity oscillations, the Kučera-Slaman Theorem says that for c.e. random reals, they all happen in the same places.

By all of this, if a real is both random and c.e. it must be Solovay complete and hence Turing complete. Actually, it has to be Turing complete in a very strong way.

Theorem 5.3: (Downey and Hirschfeldt [19]) Suppose that A is a c.e. set and α is a 1-random c.e. real. Then $A \leq_{wtt} \alpha$, and this is true with identity use.

Proof: Given A and α as above we must construct $\Gamma^\alpha = A$, where $\gamma(x) = x$. Fix a universal prefix-free machine U and using Kraft-Chaitin, and the Recursion Theorem, we will be building a part of U, so that if we enumerate a Kraft-Chaitin axiom $\langle 2^n, \sigma\rangle$ we will know that some τ, σ enters U for some τ of length $e+n$. Since α is 1-random we know that for all n, $K_U(\alpha \upharpoonright n) \geq n - c$ for a fixed c, which we will know for the sake of this construction.

Let $\alpha_s \to \alpha$ be a computable sequence converging to α and let $A = \cup_s A_s$. Initially, we will define $\Gamma^{\alpha_s}(x) = 0$ for all x, and maintain this unless x enters $A_{s+1} - A_s$. As usual at such a stage, we would like to change the answer from 0 to 1. To do this we will need $\alpha \upharpoonright x \neq \alpha_s \upharpoonright x$. Should we see a stage $t \geq s$ with $\alpha_t \upharpoonright x \neq \alpha_s \upharpoonright x$ then we can so change the answer. For $x > e + c + 2$, we can force this to happen. We simply enumerate an axiom $\langle 2^{x-c-e-1}, \alpha_s \upharpoonright x\rangle$ into our machine, causing a description of $\alpha_s \upharpoonright x$ of length $x - c - 1$ to enter $U - U_s$, and hence $\alpha \upharpoonright x \neq \alpha_s \upharpoonright x$. We can simply wait for this to happen, correct Γ and move to the next stage. □

Similar methods can be used to prove the following (the first being originally established by Arslanov's Completeness Criterion).

Theorem 5.4: (Kučera [37]) Suppose that A is a random set of c.e. degree. Then A is Turing complete.

Theorem 5.5: (Downey and Hirschfeldt [19]) Suppose that A is a random set of c.e. wtt-degree. Then A is wtt-complete.

Downey, Hirschfeldt and Nies [22], and Downey, Hirschfeldt and LaForte [20] were motivated to look at the structure of c.e. reals under Solovay reducibility. They proved several results, but the structure remains largely unexplored.

Theorem 5.6: (Downey, Hirschfeldt and Nies [22]) The Solovay degrees of c.e. reals forms a distributive upper semilattice, where the operation of join is induced by $+$, arithmetic addition (or multiplication) (namely $[x] \vee [y] \equiv_S [x + y]$.)

Theorem 5.7: (Downey, Hirschfeldt and Nies [22]) If $[\Omega] = \mathbf{a} \vee \mathbf{b}$ then either $[\Omega] = \mathbf{a}$ or $[\Omega] = \mathbf{b}$.

Theorem 5.8: (Downey and Hirschfeldt [19]) There exist c.e. *sets* A and B such that the Solovay degrees of A and B have no infimum in the (global) Solovay degrees.

To prove (i) note that $x, y \leq_S z$ implies there is a triple c, p, q such that $cz = x + p = y + q$. So $2cz = (x + y) + (p + q)$. So $x + y \leq_S z$. Clearly $x, y \leq x + y$. Similarly to prove (ii), roughly, we work as follows. Suppose $z \leq_S x_1 + y_1$. Use Lemma 5.3 to run the enumerations of and cover the $z_{s+1} - z_s$ using bits of $x_{1,s+1} - x_s, y_{s+1} - y_s$.

The proof of density and join inaccessibility are significantly more intricate.

5.2. *The Density Theorem*

Theorem 5.9: (Downey, Hirschfeldt and Nies [22]) The Solovay degrees of c.e. reals are dense. Indeed the following hold.

(i) If $\mathbf{a}$ is incomplete and $\mathbf{b} <_S \mathbf{a}$, then there exist $\mathbf{a_1}|_S\mathbf{a_2}$ 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.

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

Proof: (ii) is a straightforward finite injury argument. (i) is a finite injury argument with some quite novel features. 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 $i < 2$:

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

There are very interesting timing problems and these can be seen with a two requirement scenario, which we discuss below.

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

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. We have

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

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 5.2: 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 5.4: 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. □

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 R_1 will, in turn, be satisfied.

The problem is that R_1 *cannot tell when such an s arrives.* If R_1 is too quick, 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 5.5: 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. □

Downey and Hirschfeldt [19] have shown that the proof can be made to work for any Σ^0_3 measure of relative randomness where + is a join, the 0 degree includes the computable reals, and the top degree is Ω.

5.3. *Other measures of relative randomness*

We remark that there are a number of other interesting measures of relative randomness, aside from $\leq_S$ and the fundamental initial segment ones $\leq_C$ and $\leq_K$. They include

(i) $A \leq_{sw} B$ iff there is a c and a wtt procedure Γ with use $\gamma(n) = n+c$, and $\Gamma^B = A$. (We met this in Theorem 5.3.) If $c = 0$, then this is called ssw-reducibility and is the one used by Soare and Csima in differential geometry, such as Soare [82].

(ii) $A \leq_{rK} B$ means that there there is a c such that for all n,

$$K((A \upharpoonright n)|(B \upharpoonright n + c)) = O(1).$$

I don't really have room to discuss all the results but will try to give a flavour. *sw*-reducibility says that not only is the case that the initial segments converge at more of less the same rate, but there is an *efficient* way to convert the *bits* of B into those of A.

Thus in spite of the fact that the Kučera-Slaman Theorem says that all versions of Ω are the same in terms of their S-degrees, Yu and Ding [98] established the following.

Theorem 5.10: (Yu and Ding [98])

(i) There is no *sw*-complete c.e. real.

(ii) There are two c.e. reals β_0 and β_1 so that there is no c.e. real α with $\beta_0 \leq_{sw} \alpha$ and $\beta_1 \leq_{sw} \alpha$.

The proof roughly works by picking two long intervals $\beta_0 \upharpoonright [n, n+t], \beta_1 \upharpoonright [n, n+t]$, to diagonalize against some α and sw reduction Γ_e with use $n+e$. Initially the reals have $\beta_i(k) = 0$ on this interval. Our procedure will work by alternating between β_0 and β_1 adding $2^{-(n+t)}$ each time, where time here means "expansionary stages."

The key observation of Yu and Ding here is that this simple procedure can drive α to be large. This is proven by induction, the nicest proof being due to Bamparlias and Lewis [4]. The main lemma is to show that α's best strategy is the obvious one of *least effort* (nomenclature of Bamparlias and Lewis [4]) where α changes as far right as it can. You argue that if α' works then so would α given by this least effort strategy. This is proven by induction.

Here is an example which would show why the least effort strategy won't work.

stage 1: $\beta_{0,1} = 0.001$, $\beta_{1,1} = 0$ and $\alpha_1 = 0.001$
stage 2: $\beta_{0,2} = 0.001$, $\beta_{1,2} = 0.001$ and $\alpha_2 = 0.010$
stage 3: $\beta_{0,3} = 0.010$, $\beta_{1,3} = 0.001$ and $\alpha_3 = 0.100$
stage 4: $\beta_{0,4} = 0.010$, $\beta_{1,4} = 0.010$ and $\alpha_4 = 0.110$
stage 5: $\beta_{0,5} = 0.011$, $\beta_{1,5} = 0.010$ and $\alpha_5 = 0.111$
stage 6: $\beta_{0,6} = 0.011$, $\beta_{1,6} = 0.011$ and $\alpha_6 = 1.000$
stage 7: $\beta_{0,7} = 0.100$, $\beta_{1,7} = 0.011$ and $\alpha_7 = 1.100$
stage 8: $\beta_{0,8} = 0.100$, $\beta_{1,8} = 0.100$ and $\alpha_8 = 10.000$
Similar arguments show the following.

Theorem 5.11: (Bamparlias and Lewis [3, 4]) There is a c.e. real α such that for any random c.e. real β, $\alpha \not\leq_{sw} \beta$.

An argument of a different kind shows the following.

Theorem 5.12: (Hirschfeldt, unpubl) There is a real α such that for all random reals β, $\alpha \not\leq_{sw} \beta$.

We have seen that if W is a c.e. set the $W \leq_{sw} \Omega$. Also on the c.e. sets, S and sw coincide. Little else is known about $\leq_{sw}$.

The reducibility rK is implied by either of sw and S. It has many of the best features. By unpublished work of Downey, Greenberg, Hirschfeldt, and Miller it is not implied by $\leq_C$ even on the c.e. reals. It is an appropriate Σ^0_3 reducibility and hence it is dense on the c.e. reals. It implies $\leq_T$. Little else is known about $\leq_{rK}$.

Other reducibilities include $\leq_{Km}$, $\leq_{KM}$ (i.e. supermartingale reducibility), but these are more or less completely unexplored, save the fact that

$\leq_{SM}$ is dense on the c.e. reals.

5.4. $\leq_C$ *and* $\leq_K$

Recall $A \leq_K B$ means that, for all n, $K(A \upharpoonright n) \leq K(B \upharpoonright n) + O(1)$, and similarly $\leq_C$.

Thanks mainly to the work of Miller and Yu, we know some basic facts about the $\leq_K$ degrees of *random reals*. The first thing we discover about $\leq_C$ and $\leq_K$ is that they are not really "reducibilities" though we will confusingly call them such.

Theorem 5.13: (Yu, Ding, Downey [100]) For $Q \in \{K, C\}$, $\{X : X \leq_Q Y\}$ has size $2^{\aleph_0}$ and has members of each degree, whenever Y is random.

The proof is relatively easy. Take a sufficiently computable sparse set X. Then it's complexity is eventually always well below a random real. But any degree can be coded into a really sparse set. The replacement for this theorem is a measure-theoretical one:

Theorem 5.14: (Yu, Ding, Downey [100]) For any real A, $\mu(\{B : B \leq_K A\}) = 0$. Hence there are uncountably many K degrees.

Yu and Ding improved this result to construct $2^{\aleph_0}$ many K-degrees directly ([99]), but this can also be obtained by observing that $\leq_K$ is Borel, and hence a theorem of Silver can be used. Using direct analysis of the the fluctuations of initial segment complexities Yu, Ding, and Downey obtained the following.

Theorem 5.15: (Yu, Ding, Downey [100]) For all c and $n < m$,

$$(\exists^\infty k)\big[\, K(\Omega^{(n)} \upharpoonright k) < K(\Omega^{(m)} \upharpoonright k) - c\big].$$

For $n = 0, m = 1$ Theorem 5.15 was proven by Solovay [84], using totally different methods. Using van Lambalgen's Theorem as a base. more powerful results have recently been obtained by Miller and Yu. Recall that van Lambalgen's Theorem states: *B n-random and A is B-n-random iff $A \oplus B$ is n-random.*

Definition 5.3: (Miller and Yu [63]) We say that $\alpha \leq_{vL} \beta$, α is *van Lambalgen*[g] reducible to β if for all $x \in 2^\omega$, $\alpha \oplus x$ is random implies $\beta \oplus x$ is random.

[g]This is closely related to a relation introduced by Nies: He defined $A \leq_{LR} B$ if for all Z,

Theorem 5.16: (Miller and Yu [63]) For all random α, β,

(i) α n-random and $\alpha \leq_{vL} \beta$ implies β is n-random.
(ii) If $\alpha \oplus \beta$ is random then α and β have no upper bound in the vL-degrees.
(iii) If $\alpha \leq_T \beta$ and α is 1-random, then $\beta \leq_{vL} \alpha$.
(iv) There are random $\alpha \equiv_{vL} \beta$ of different Turing degrees.
(v) There are no maximal or minimal random vL-degrees, and no join.
(vi) If $\alpha \oplus \beta$ is random then $\alpha \oplus \beta <_{vL} \alpha, \beta$.
(vii) The Σ^0_1 theory of the vL-degrees is decidable.

The proofs of most of these are relatively easy once you figure out what to do. For instance, suppose that α n-random and $\alpha \leq_{vL} \beta$. Use Kučera's Theorem that there is a random z with $z \equiv_T \emptyset^{(n-1)}$. Then $\alpha \oplus z$ is random, and hence $\beta \oplus z$ is random and hence β is 1-z-random, that is β is n-random.

Furthermore, Miller and Yu show that $\Omega^{(n)}$ and $\Omega^{(m)}$ have no upper bound in the vL degrees for $n \neq m$. This improves the Yu, Ding, Downey (Theorem 5.15) result above.

All of this is filters through an interesting relationship between $\leq_{vL}$ and $\leq_C, \leq_K$.

Lemma 5.6: (Miller and Yu [63]) For random α, β,

(i) Suppose that $\alpha \leq_K \beta$. Then $\alpha \leq_{vL} \beta$.
(ii) Suppose that $\alpha \leq_C \beta$. Then $\alpha \leq_{vL} \beta$.

We state the following for $\leq_K$ but they hold equally for $\leq_C$. (Most of the proofs are in this area work equally well for $\leq_C$ and $\leq_K$. There are occasional cases where the proof needs considerably more work in the $\leq_C$ case, such as the proof of Lemma 5.6(ii) above.)

Corollary 5.2: (Miller and Yu [63])

(i) Suppose that $\alpha \leq_K \beta$, and α is n-random and β is random. Then β is n-random.
(ii) If $\alpha \oplus \beta$ is 1-random, then $\alpha|_K \beta$ and have no upper bound in the K-degrees.

Z is 1-B-random implies Z is 1-A-random. If A and B are both random then $A \leq_{LR} B$ iff $B \leq_{LR} A$. Note that $\leq_{vL}$ is really only interesting on the randoms, but there are a number of possible extensions which also make sense on the non-randoms. These have yet to be explored.

(iii) For all $n \neq m$, the K-degrees of $\Omega^{(n)}$ and $\Omega^{(m)}$ have no upper bound.

Miller and Yu provided a natural way to demonstrate that the vL-degree and the K-degrees differ on randoms. The following result should be compared with Theorem 5.16 (vi).

Theorem 5.17: (Miller and Yu [63]) If $\alpha \oplus \beta$ is 1-random, then $\alpha|_K \alpha \oplus \beta$.

A simple application yields Theorem 5.14, that $\mu\{\beta : \beta \leq_K \alpha\}$ for random α is zero. Namely, if β is 1-α-random, then $\beta \not\leq_{vL} \alpha$ and hence, since $\mu(\{\beta : \beta \text{ is 1-}\alpha\text{-random }\}) = 1$, we get $\mu(\{\beta : \beta \leq_K \alpha\}) = 0$, since $\leq_K$ implies $\leq_{vL}$.

Using new techniques and extensions of the above, Miller has proven the following.

Theorem 5.18: (Miller [59])

(i) If α, β are random, and $\alpha \equiv_K \beta$, then $\alpha' \equiv_{tt} \beta'$. As a consequence, every K-degree of a random real is countable.
(ii) If $\alpha \leq_K \beta$, and α is 3-random, then $\beta \leq_T \alpha \oplus \emptyset'$.

Notice that (ii) implies that the cone of K-degrees above a 3-random is countable. Miller and Yu have constructed a 1-random whose K-upper cone is uncountable. This last result uses their method of constructing K-comparable reals. Its proof uses the following clever lemma. The current proof of Lemma 5.19 is quite difficult.

Theorem 5.19: (Miller and Yu) Suppose that $\sum_n 2^{-f(n)} < \infty$, then there is a 1-random Y with

$$K(Y \upharpoonright n) < n + f(n),$$

for almost all n.

Then to get K-comparable reals, use the result taking $g(n) = K(B \upharpoonright n) - n$ for random B. This function is convergent by the Ample Excess Lemma. Now we use Theorem 5.19 on some convergent function f with $g - f \to \infty$.

We remark that Miller has also constructed an uncountable (non-random) K-degree.

Finally Miller has shown that if α is 3-random then its often useless as an oracle. We will call α *weakly-low for* K if $(\exists^\infty n)[K(n) \leq K^\alpha(n) + O(1)]$.

Thus in a weakly-low real, the information in α is so useless that it cannot help to compress n. The following result echoes the theme articulated by Stephan that most random reals have little *usable* information in them.

Theorem 5.20: (Miller [59])

(i) If α is 3-random it is weakly-low.
(ii) If α is weakly-low, and random, then α is strongly Chaitin random in that

$$(\exists^\infty n)\big[K(\alpha \upharpoonright n) \geq n + K(n) - O(1)\big].$$

5.5. *Outside of the randoms*

Little is known about $\leq_C$ and $\leq_K$ outside of the random reals. On the c.e. reals $\leq_C$ and $\leq_K$ are appropriate Σ^0_3 measures of relative randomness, and hence the following is true.

Theorem 5.21: (Downey and Hirschfeldt [19]) The C- and K- degrees of c.e. reals form dense uppersemilattices.

We remark that this needs the result of Downey, Hirschfeldt, Nies, Stephan [23] that $+$ is a join. To see this, given $x, y < z$, run the enumerations, and have one z-program if $x_s \upharpoonright n$ stops first, and one if $y_s \upharpoonright n$ first.

Other than this, Frank Stephan has shown that $\leq_C$ implies $\leq_T$ on the c.e. reals. (see [19]). This generalizes earlier theorems of Loveland and of Chaitin.

Theorem 5.22: (Loveland [51]) Suppose that for all n, $C(X \upharpoonright n|n) = O(1)$. Then X is computable.

Theorem 5.23: (Chaitin [9]) $A \leq_C 1^\omega$ iff A is computable.

Proof: (Sketch) All of these use the "Π^0_1 class method" each time. They use the fact that a Π^0_1 class with a finite number of paths has computable computable paths. Take Loveland's Theorem, for instance. Since there are only finitely many programs to consider for the $C(X \upharpoonright n|n) = O(1)$. Knowing these and the maximum hit infinitely often will allow for the construction of the Π^0_1 class.

Chaitin's Theorem uses the same method but needs the combinatorial fact below.

Lemma 5.7: (Chaitin [9]) $|\{\sigma : C(\sigma) \leq C(n) + d \wedge |\sigma| = n\}| = O(2^d)$.

Since we know that between n and 2^n there are C-random lengths with $C(n) = \log n$, we can then apply the Lemma to construct the Π^0_1 class. Finally, Stephan's result is similar, but uses a relativization plus enumeration argument. □

5.6. $\leq_K$ and $\leq_T$

This naturally leads us to ask whether $\leq_K$ implies $\leq_T$ for c.e. reals. As it turns out the implication fails at the very first place it can.

Definition 5.4: We say that A is *K-trivial* iff there is a constant d such that for all n, $K(A \upharpoonright n) \leq K(n) + d$. We would write $A \in KT(d)$.

Theorem 5.24: (Solovay [84]) There are noncomputable K-trivial reals.

As we will see, such reals can even be c.e. sets. The reader might well ask, "what about the Π^0_1 class method?" The Π^0_1 class method kind of works, except to construct the tree, we don't know the K-complexity of any n, like we do for C. For C, we know "$\log n$" is the answer in long enough interval. (That is, between m and 2^m there is a random length and its C-complexity will be $\log n$.) But in the prefix-free case, the tree is only Δ^0_2 since $\emptyset'$ can construct it. Now the same methods work (this time using the Coding Theorem to bound the width). We get the following.

Theorem 5.25: (Chaitin [10], Zambella [101]) There are only $O(2^d)$ members of $KT(d)$. They are all Δ^0_2.

The reader might wonder with the nice computable bound how many K-trivial reals there are. Let $G(d) = |\{X : X \in KT(d)\}$. Then there is a crude estimate that $G(d) \leq_T \emptyset'''$. This is the best upper bound known. In unpublished work, Downey, Miller and Yu have shown that $G(d) \not\leq_T \emptyset'$, using the fact that $\sum_d \frac{G(d)}{2^d}$ is convergent. This is all related to the Csima-Montalbán functions. We say that f is a *Csima-Montalbán function* if f is nondecreasing and

$$K(A \upharpoonright n) \leq K(n) + f(n) + O(1)$$

implies that $A \upharpoonright n$ is K-trivial. Such functions can be constructed from $\emptyset'' \oplus G$. We define f to be *weakly* Csima-Montalbán, if we weaken the hypothesis to be that $\liminf_n f(n) \to \infty$. Little is known here. It is not known if the arithmetical complexity of f depends upon the universal machine chosen.

Returning to our story, it is very easy to construct a K-trivial real, using the "cost function" method. This construction has been well-reported, and we note it below.

Let

$$A_{s+1} = A_s \cup \{x : W_{e,s} \cap A_s = \emptyset \wedge x \in W_{e,s}$$

$$\wedge \sum_{x \leq j \leq s} 2^{-K(1^j)[s]} < 2^{-(e+1)}\}.$$

Then A is noncomputable and K-trivial. Work of Nies shows that, basically, this is the *only* way to construct such sets.

The K-trivial reals form a fascinating class of reals and has many unexpected properties. The first such property to be established was the following.

Theorem 5.26: (Downey, Hirschfeldt, Nies, Stephan [23]) If A is K-trivial then A is Turing incomplete.

The proof of this result is far from easy, and uses the "decanter" method. This decanter/golden run method has been refined and elaborated through the deep work of Nies, and Hirschfeldt-Nies, (especially [67, 69]) and later Hirschfeldt-Nies-Stephan to establish a number of amazing results, using "golden run" constructions. For example:

Theorem 5.27:

(i) (Nies) Every K-trivial is tt-bounded by a K-trivial c.e. set.
(ii) (Nies) Every K-low is superlow, and "traceable".
(iii) (Nies) K-trivial = low for randomness, meaning that A-random iff random.
(iv) (Hirschfeldt-Nies) K-trivial=low for K, meaning that $K^A(\sigma) = K(\sigma) + O(1)$, for all σ.
(v) (Nies) K-trivials are closed under T-reducibility and form the only known natural Σ^0_3 ideal in the Turing degrees.
(vi) (Nies) They are bounded above by a low_2 degree.

Hirschfeldt, Nies and Stephan [32] have shown that if A and B are Δ^0_2 random then there are K-trivials are T-below both of them. I simply don't have time in these lectures to tell the "trivial story" which is still being worked out.

I remark that there are many open questions about this amazing class. Here is one of my favourites. Is there a low (necessarily non-c.e.) degree

above all the K-trivials. The reason that this is of interest is that if such a real could be random then it would be a genuinely new strategy for coding into randoms, as has been pointed out by Kučera.

5.7. *Hausdorff Dimension*

We return to the theme of calibrating randomness. This time we will try another approach. Consider Ω. It is random. What about $a_0 0 a_1 0 \dots$ where $\Omega = a_0 a_1 \dots$. Then probably we'd expect it to be "half random."

There is an an effectivization of a well-known theory that makes this correct. A refinement of the class of measure zero sets is given by the theory of Hausdorff Dimension. In 1919 Hausdorff [31] generalized earlier work of Carathéodory to define a notion of an s-dimensional measure to include non-integer values.

The basic idea is that you replace measure by a kind of generalized measure, where $\mu([\sigma])$ is replaced by $2^{-s|\sigma|}$ where $0 < s \leq 1$. With $s = 1$ we get normal Lebesgue measure. For $s < 1$ we get a refinement of measure zero. Very informally, it can be shown that there is some limsup where the s-measure is not zero, and this is called the Hausdorff dimension of the set. One can translate this cover version into a s-gale (a version of martingales) definition in the same way that it is possible to frame Lebesgue measure in terms of martingales.

In any case, for the effective version through the work of Lutz, Mayordomo, Hitchcock, Staiger and others we find that the notion corresponds to $\liminf_n \frac{K(A\upharpoonright n)}{n}$, and can take that as a *working definition* of effective Hausdorff dimension. (This sentence does not do justice to the work done by these and other authors in this area.) With this definition, one can easily see that the thinned version of Ω above gets dimension $\frac{1}{2}$. Actually it is $\frac{1}{2}$-random in the sense of Tadaki [90].

In these lectures I don't have the space to talk about all the nice results developed concerning effective Hausdorff dimension (and effective packing and box counting dimension). I simply want to point out that there are other ways to calibrate randomness. One very nice question here is the following. Is there a degree $\mathbf{a}$ which has a member of nonzero dimension, and yet bounds no random degree?

I would like to remark that Lutz [52, 53] has even developed a notion of dimension for individual strings. Again we see that it is immediately related to prefix-free complexity. The approach is to replace s-gales by "termgales" which are the analogues of s-gales for terminated strings. (You have a third

bet that you have reached the end of the string.) One of the results he has proven is the following.

Theorem 5.28: (Lutz [52, 53]) Let d denote the discrete dimension obtained using "termgales" as alluded to above. There is a constant $c \in \mathbb{N}$ such that for all $\sigma \in 2^{<\omega}$,

$$|K(\sigma) - |\sigma| \dim(\sigma)| \leq c.$$

I refer the reader to Lutz [52, 53], Staiger [85, 86], Terwijn [91], Reimann [75, 76], Downey, Merkle, Reimann [26], Tadaki [90], and Downey and Hirschfeldt [19], for more details.

6. Lecture 5 : Measure-theoretical injury arguments

6.1. *Risking measure*

In the last section we met the effective 0-1 laws. These laws can be exploited to prove various results about random degrees by making constructions which work on sets of positive measure. This basic idea goes back to unpublished work of Martin (as we see below) and of Paris [73,74]. The idea was beautifully exploited by Kurtz in the later chapters of his PhD Thesis [45]. These results tend to give theorems that hold for almost all degrees. With more care, we can calculate exactly the level needed to make the constructions work and deduce that they hold for all, for example, 2-random reals, as in Kautz [34].

6.2. *2-random degrees are hyperimmune*

We begin this section with the proof of Martin's Theorem 6.1 The main idea is called "risking measure," in the words of Kurtz [45], and results in a measure-theoretical version of the priority method. The idea is that if we *fail* to meet some requirement then we will fail to define some object under construction (typically, a Turing functional) on some small measure of Cantor space. However, things are arranged that this is small enough that we only fail on a set whose measure is bounded, and then after the fact argue that the result holds for almost all reals by the effective 0-1 laws.

Theorem 6.1: (Martin, unpubl.) Almost every degree is a hyperimmune degree.

Proof: By the zero-one law it is enough to prove that $\mu(\{A : A$ bounds a hyperimmune degree $\}) > 0$. To achieve this we construct a partial computable functional Ξ so that

$$\mu(\{A : \Xi^A \text{ is total and not dominated by any computable function}\} \geq \frac{1}{2}.$$

For this construction, it is convenient to consider Ξ as a partial computable function from strings to strings. This will be a reduction provided that $\Xi(\nu)\downarrow$, $\nu \preceq \widehat{\nu}$ and $\Xi(\widehat{\nu})\downarrow$, then $\Xi(\nu) \subseteq \Xi(\widehat{\nu})$. We remark that it is not necessarily true that if $\Xi(\nu)\downarrow$ then $\Xi(\gamma)\downarrow$ for all $\gamma \subseteq \nu$.

On a set of positive measure, we will meet the requirements :

$$R_e : \varphi_e \text{ total } \rightarrow \Xi^A \text{ is not majorized by } \varphi_e.$$

Now suppose that we *knew* whether φ_e was total. Then we could proceed as follows. We could begin with λ, the empty string. If φ_0 was not total, then we would need to do nothing else and could proceed to treating R_1. Otherwise, we could select some witness n_0, compute $\varphi_0(n_0)$ and then set $\Xi^\lambda(n_0) = \varphi_0(n_0) + 1$. Then, of course, φ_0 cannot majorize Ξ^A for any A. We could then use a new witness for φ_1, etc.

The trouble is that we cannot decide whether φ_0 is total, and of course even for a witness n_0, we can't decide if $\varphi_0(n_0)\downarrow[s]$ for some s.

The idea then is to try to implement this process in such a way that should we fail to meet some R_e then the overall cost (in terms of measure) will be small. (Here small will be $2^{-(e+2)}$.)

For the sake of R_0 we will work as follows. Initially, we will devote the string 00 to trying to force φ_0 not to be total. By this we mean that we first pick a witness $n_0 = n_0^{00}$, for the cone [00] of strings σ extending 00. We will not define $\Xi^\sigma(n_0)$, or indeed Ξ^σ at all for such σ until we see some stage s where $\varphi_0(n_0^{00})\downarrow[s]$. At this stage we will then define

$$\Xi^{00}(n_0) = \varphi_0(n_0) + 1.$$

The *point* is that now for any strings σ extending 00, $\Xi^\sigma(n_0) = \varphi_0(n_0) + 1$. (And we would make sure that $\Xi^{00}(m)$ is defined for all $m \leq n_0^{00}$ so as to make Ξ^α total on a set of α of positive measure.) Hence R_0 is met within the cone [00] no matter how else we define Ξ, provided that it is done in a way consistent with Ξ^{00}.

Notice that if we *fail* to define Ξ^{00}, then n_0^{00} is a witness to the fact that φ_0 is not total. R_0 is therefore met globally. The cost of meeting R_0 this way is that Ξ^A will not be defined on a set of measure $2^{-|00|} = 2^{-2}$.

Now whilst we are devoting [00] to testing R_0, we cannot stop Ξ^ν being defined for strings *not* extending 00. Thus, for instance, by the stage s that we get to define $\Xi^{00}(n_0) \downarrow [s] = \varphi(n_0) + 1$, we might well have defined $\Xi^\sigma(m)$ for various σ extending 01.

The idea is that once we succeed for R_0 in [00] we will process R_0 in the cone [01] (and then [10], then [11], always risking 2^{-2} each time). Thus R_1 will assert control of [01] taking control of all extensions of 01 of length s. There will be 2^{s-2} such extensions $\nu_1 \dots \nu_{2^{s-2}}$ and note that

$$\sum_{i \leq i \leq 2^{s-2}} 2^{-|\nu_i|} = 2^{-2}.$$

Then the idea is that R_0 will pick a new (large, fresh) witness n_0^{01} which will serve for *all* of the ν_i's. Diagram 1 below might be helpful here.

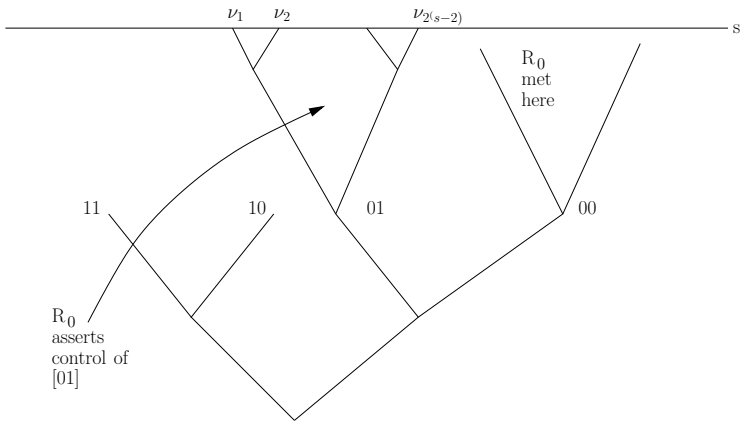

Fig. 1. R_0 changes to the next cone

Then if we ever see a stage $t > s$ such that $\varphi_0(n_0^{01}) \downarrow [t]$, we will be free to define $\Xi^{\nu_i}(n_0^{01}) \downarrow [t] = \varphi_0(n_0^{01}) + 1$, for *all* ν_i simultaneously.

Then R_0 could assert control of [10], via all strings of length t and take a new witness for this cone, etc.

The point is that either R_0 will eventually get stuck on one of $[00], [01], [10], [11]$ at a cost of $\frac{1}{4}$, or we will diagonalize φ_0 in each cone via the cone's witness, in which case R_0 has *no* effect on the measure where Ξ is defined.

The inductive strategies are defined similarly. For R_e choose the collection of strings $\sigma_1, \dots, \dots, \sigma_{2^{2+e}}$, the antichain of strings of length $e + 2$

to take the role of $00, 01, 10, 11$ as above. The goal would be, first process $R - e$ in $[\sigma_1]$ then $[\sigma_2]$, etc. Of course we would let the priorities sort this out. Whilst some R_j is asserting control of some $[\nu] \supset [\sigma_i]$ for $j < e$, we would let R_e assert control of the first available $[\sigma_k]$. In this way, we see that at any stage each R_e has exactly $2^{-(e+2)}$ of measure risked because of it, of $R - e$ is completely met. Thus the overall measure where Ξ is not defined is bounded by $\sum_{e \in \mathbb{N}} 2^{-(e+2)} = \frac{1}{2}$. □

This result can also be obtained by the following elegant argument of Nies, Stephan, and Terwijn.

Proof: (Nies, Stephan, and Terwijn [70]) Recall that in Lemma 4.3, it is shown that *A is 2-random iff for all computable time bounds g with $g(n) \geq n^2$,*

$$\exists d \exists^\infty n (C^g(A \upharpoonright n) \geq n - d).$$

Define

$$f(k) = \mu n [\exists p_1, \ldots, p_k \leq n] (C^g(A \upharpoonright p_i) \geq p_i - d).$$

Then f is A computable. We claim that f is not dominated by any computable function. Suppose that $f(k) \leq h(k)$ for all k. Define the Π^0_1 class

$$P = \{Z : \forall k [\exists p_1, \ldots, p_k \leq h(k)] (C^g(Z \upharpoonright p_i) \geq p_i - d)\}.$$

Then $P \neq \emptyset$, and every member of P is 2-random. But then there is a 2-random real that is, for instance, of low degree. □

6.3. *Almost every degree is CEA*

We use the ideas of the Martin's proof above to establish the following remarkable result of Kurtz, with the observation of Kautz that 2-randomness is enough for the proof.

Theorem 6.2: (Kurtz [45], Kautz [34]) Suppose that A is 2-random. Then A is CEA.

Proof: As in Theorem 6.1, we satisfy things on a set of positive measure. Here, we construct an operator Ξ so that

$$\mu(\{A : \Xi(A) \text{ total and } \Xi(A) \not\leq_T A\}) \geq \frac{1}{4},$$

and A is c.e. in $\Xi(A)$ whenever $\Xi(A)$ is total. The calculation that weak 2-randomness is enough comes from again analyzing the method of satisfaction of the requirements.

To make A c.e. in $\Xi(A)$ we will ask that $n \in A$ iff $\langle n, m\rangle \in \Xi(A)$ for some m. Thus, in fact A is enumeration reducible to $\Xi(A)$. Now whilst doing this we must meet requirements of the form

$$R_e : A \neq \Phi_e^{\Xi(A)},$$

there Γ_e denotes the e-Turing procedure.

Definition 6.1: We say that a string ξ is *acceptable* for a string σ iff

$$\xi(\langle m, n\rangle) = 1 \to \sigma(n) = 1.$$

Remember we are trying to make A c.e. in Ξ^A. Thus we will always require that $\Xi^\sigma[s]$ is acceptable. We will also try, whenever possible, to use ξ to represent string in the range of $\Xi[s]$.

The principal difficulty with this proof is that it is very difficult for us to actually force

$$A \neq \Phi_e^{\Xi(A)}.$$

The reason is that our opponent is playing Φ_e.

The main idea is the following. In this proof, we will inductively be working above some string β, to which Kurtz assigns a *state* via a colour blue$_e$. This more or less indicates that we are presently happy with the situation up to this string. Now we consider the action in the cone $[\beta]$. As in the previous construction, we will willfully be not defining Ξ on some cone of small measure in the cone $[\beta]$. In this case, the test string will be $\beta^\frown 1^{e+2}$. We will only ever define Ξ^σ for σ extending $\beta^\frown 1^{e+2}$, should it be possible for us to actually perform some kind of diagonalization.

For those reading the account of Kurtz [45] or Kautz [34], this testing is signaled by assigning the string $\beta^\frown 1^{e+2}$ the state red$_e$.

While we are waiting for suitable conditions for diagonalization to occur, we will devote $[\nu_1], \ldots, [\nu_{2^{(e+2)}-1}]$ (the length $e+2$ extensions of β) to the rest of the construction in this cone $[\beta]$. Note that we will only be defining Ξ^τ for τ extending ν_i in this cone, with priority e. In Kurtz's construction, this part of the current inductive module satisfying R_e is given the state/colour yellow$_e$. Diagram 2 below might be helpful here.

Now, in the background, the construction is running along, gradually defining Ξ^σ for various θ extending ν_i in the cone $[\beta]$.

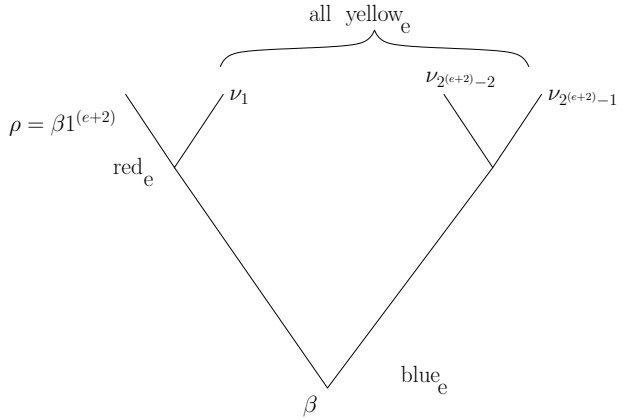

Fig. 2. R_e's basic module

Question: Under what circumstances would a string θ look bad from R_e's point of view?
Answer: It would look bad if it looked like the initial segment of a real α with $\Phi_e^{\Xi(\alpha)} = \alpha$.

This threatening situation can be detected as by looking at strings which might approximate such reals.

Definition 6.2: We say that a string θ is *threatening* a requirement R_e is there is a yellow$_e$ strings ν extending its blue$_e$ predecessor β with $\nu \preceq \theta$, and a strings ξ acceptable to θ such that

(i) $|\theta| \leq s$
(ii) $|\xi| = s$
(iii) $\Xi^{\nu}[s] \preceq \xi$
(iv) $\Phi_e^{\xi}(k) = \nu(k) = 0[s]$ for some k such that $|\beta| < k \leq |\nu|$, and
(v) no initial segment of θ has colour purple$_e$.

Item (v) is a mystery at present, but is simply a minimality condition now to be described, and can presently be ignored. If we see a threatening string θ, then it looks bad for us to continue to define Ξ on strings extending θ. Thus we will do the following. In the construction we will give any string θ which is threatening R_e colour purple$_e$. While this situation holds, we will not define Ξ on any extension of θ.

Now it might be that above β, the measure of the strings coloured red$_e$ (namely $2^{-(|\beta|+e+2)}$) *plus* the measure of purple$_e$ strings remains small

enough. That is, we don't kill too much measure above $[\beta]$ by this process. Then we would be safe to continue out construction, and R_e would only have measure-theoretically small effect. Then R_e will be met, and the string $\beta^\frown 1^{(e+2)}$ draws attention to this fact.

What about if the amount of measure killed by threatening strings becomes too great. Then we risk defining Ξ only on a set of measure zero above β. The key thing to notice is that the collection of strings ν_i are chosen so that they each differ from 1^{e+2} in at least one place where they are a 0. That is, the reader should note that item (iv) in Definition 6.2 means that if $\rho = \beta 1^{e+2}$ denotes the unique red_e extension of β at stage s, for some k with $\rho(k) = 1$ we must have $\Phi_e^{\xi}(k) = \nu(k) = 0 \neq \rho(k) = 1$, by fact that $\rho = \beta 1^{e+2}$. That means if we chose to define Ξ^α on extensions α of ρ to emulate Ξ^ν, then it *cannot be* that $\Phi_e^{\Xi^\alpha} = \alpha$ as it must be wrong on ρ.

For each purple_e string θ, let θ' denote the unique string of length $|\theta|$ extending the red_e string ρ with $\theta(m) = \theta'(m)$ for all $n \geq |\rho|$. The idea is that we will be able to give these θ' the colour green_e, and bound their density away from 0, if the density of purple_e strings grows too much.

Specifically, when the density of purple_e strings above the blue_e string β exceeds $2^{-(e+3)}$, there must be some yellow_e string ν such that the density of purple_e strings above ν must also exceed $2^{-(e+3)}$, by the Lebesgue Density Theorem. Let $\{\theta_1, \ldots, \theta_n\}$ list the purple_e strings above ν, where for definiteness ν is chosen lexicographically least. For each θ_i, let ξ_i be the least string which witnesses the threat to R_e according to Definition 6.2.

Thus,

(i) ξ_i is acceptable for θ_i,
(ii) $\Xi^\nu \preceq \xi_i$, and
(iii) $\Phi_e^{\xi_i}(k) = 0 = \theta_i(k)$ for some k with $\rho(k) = 1$.

Now we are in a position to win R_e in the cone above ρ, and on a set of large measure. In the construction, we will now define Ξ to mimic the action of Ξ on the θ_i above ν, so that $\Xi^\nu[s] = \Xi^\rho[s]$. The action is that

(a) Any string extending β loses its colour.
(b) β loses colour blue_e.
(c) Each string θ_i' is given colour green_e.
(d) We define $\Xi^{\theta_i'} = \xi_i$, which will then force $\Phi_e^{\xi_i}(k) \neq \theta'(k)$ for some k with $|\beta| < k \leq |\nu|$.

Notice that (d) above justifies the use of the colour green_e for the strings θ_i'. Diagram 3 might be helpful here.

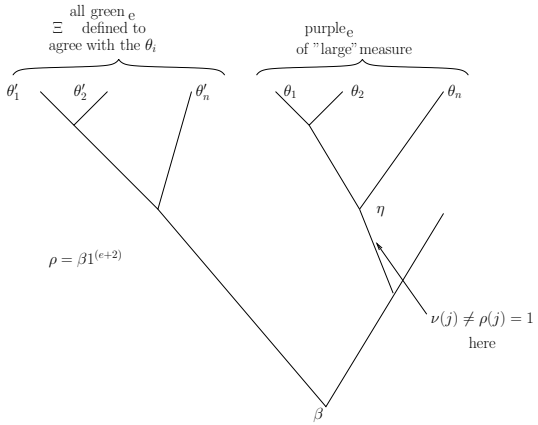

Fig. 3. R_e's acts under purple$_e$ pressure

The reader should note that each time we are forced to use the red$_e$ string ρ, we are guaranteed to succeed on set of measure at least $2^{-(e+5)}$ above β, and hence we will succeed on a set of positive measure. Notice also that since we remove all colours from the purple strings then we will be able to replicate this construction on strings extending those that have lost their colour. Finally, we remark that the fact that we only consider acceptable strings will mean that some subset of A is computably enumerable in Ξ^A. This will be fixed via a "catch up" when we assign blue$_e$ colours. It is also why we chose 1^{e+2} as the extension for β since all strings of interest will remain acceptable, and we can always find an extension to make the enumeration reduction work.

To see that 2-randomness is enough for the result, we have made sure that $\{\Xi^A$ is total $\}$ is a Π^0_2 class of positive measure and contains at least one 2-random real. Thus by the effective 0-1 law, it contains members of every 2-random degree.

Full details can be found in Downey and Hirschfeldt [19], and Kautz [34]. □

In Kautz's Thesis [34], Kautz mistakenly claims that weak 2-randomness is enough. His error is to assume that the effective 0-1 law holds for weak 2 randomness. In fact for hyperimmune free degrees Martin-Löf randomness is the same as weak 2-randomness, as we have already seen.

6.4. *Variations and marginalia*

Kurtz proved that almost every degree bounds a 1-generic degree. He remarks that this result can also be deduced from the theorem above, via the following result which was known to several authors in the 70's. P The proof below is an unpublished one due to Richard Shore (also found in Soare's book [81], Exercise VI, 3.9).

Theorem 6.3: Suppose that A is CEA(B) with $B <_T A$. Then A bounds a 1-generic degree.

Proof: Let $A = \cup_s A_s$ be a B-computable enumeration of A. Let $c(n)$ denote the computation function of A:

$$c(n) = \mu s(A_s \upharpoonright n = A \upharpoonright n).$$

We construct the 1-generic set $G = \lim_s G_s$ via a finite extension argument. Let V_e denote the e-th c.e. set of strings. At stage s we let $G_{s+1} = G_s$ unless (for some least e) we see some extension $\gamma \in V_{e,c(s+1)}$ with $G_s \prec \gamma$. In this latter case, let $G_{s+1} = \gamma$.

Suppose that G is not 1-generic. We claim that $A \leq_T B$. Let e such that G does not meet V_e and every initial segment of G is extended by one in V_e. Let s_0 be a stage after which e has priority. It suffices to compute $c(n)$ from B, since B enumerates A. Using simultaneous induction on s and G_s, for $s > s_0$.

Now assume that G_s is known. Compute a minimal stage t such that some extension γ_s of G_s occurs in $V_{e,t}$. The it must be that $t > c(s+1)$, lest we would act for e. This allows us to compute $c(s+1)$, and hence G_{s+}□

Corollary 6.1: (Kurtz [45])Suppose that **a** is 2-random. Then **a** bounds a 1-generic degree.

Actually, Kurtz proved an even more surprising result in [45]. Recall that we say that a class $\mathcal{C}$ of degrees is *downward dense* below a degree **a** iff for all nonzero $\mathbf{b} < \mathbf{a}$ there is a degree $\mathbf{c} \leq \mathbf{b}$ with $\mathbf{c} \in \mathcal{C}$

Theorem 6.4: (Kurtz [45]) The 1-generic degrees are downward dense below any 2-random degree.

.

Again the methods of proof are elaborations of the measure risking ones. Roughly speaking, a key ingredient is the de Leeuw, Moore, Shannon, and Shapiro-Sacks result that the cone of degrees above a noncomputable real

has measure zero. However, this time the argument is much more delicate, since, in particular, we need to recognize when we are dealing with a computable real where the de Leeuw, Moore, Shannon, and Shapiro-Sacks result might fail. The proof of this result is beyond the scope of the present lecture and we refer the reader to Kurtz [45] and Downey-Hirschfeldt [19].

We remark that there has been a reasonable amount of work pursuing analogs of these results for other classes, such as the generic reals. For instance, Yu Liang [97] has proven an analog of van Lambalgen's Theorem:

Theorem 6.5: (Yu [97]) $x \oplus z$ is n-generic iff x is n-z-generic and z is n-generic.

This allowed Yu to prove a number of interesting results about generics. We can also ask whether reals x can be low for, say, 1-genericity meaning that y is x-generic iff y is generic.

Theorem 6.6: (Greenberg, Miller, Yu [97]) No noncomputable real is low for 1-genericity.

We remark that Miller and Yu have shown that there are reals low for weak genericity. One question is whether the class of low for weakly generic reals is the same class as the computably traceable reals.

7. Acknowledgement

Downey's research is supported by the Marsden Fund of New Zealand. Parts of this paper were prepared whilst the author was visiting the University of Chicago, and he thanks the members of the seminar there for being excellent guinea pigs. Additional support provided by the Institute for Mathematical Sciences, Singapore, as part of their programme *Computational Prospects of Infinity.* Also thanks to both Carl Jockusch and Joe Miller for providing much needed correction to earlier drafts.

References

1. Allender, E., H. Buhrman, M. Koucký, D. van Melkebeek, and D. Ronneburger, *Power from Random Strings,* in *FOCS 2002,* IEEE (2002), 669-678.
2. Allender, E., H. Buhrman, and M. Koucký, *What Can be Efficiently Reduced to the Kolmogorov-Random Strings?,* Annals of Pure and Applied Logic, 2006 to appear.
3. Bamparlias, G., and A. Lewis,
4. Bamparlias, G., and A. Lewis, *On a question of Yu and Ding*, submitted.

5. Calude, C., *Information Theory and Randomness, an Algorithmic Perspective,* Springer-Verlag, Berlin, 1994. Second revised edition 2002.
6. Calude, C., and Coles, R. *Program size complexity of initial segments and domination relation reducibility,* in *Jewels are Forever*, (J. Karhümaki, H. Mauer, G. Paŭn, G. Rozenberg, eds.) Springer-Veralg, New York, 1999, 225-237.
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. Chaitin, G., *A theory of program size formally identical to information theory*, Journal of the Association for Computing Machinery 22 (1975), pp. 329-340.
10. Chaitin, G. *Information-theoretical characterizations of recursive infinite strings,* Theoretical Computer Science, vol. 2 (1976), 45-48.
11. Chaitin, G. *Incompleteness theorems for random reals,* Adv. in Appl. Math Vol. 8 (1987), 119-146.
12. Chaitin, G., *Information, Randomness & Incompleteness*, 2nd edition, Series in Computer Science 8, World Scientific, River Edge, NJ, 1990.
13. de Leeuw, K., Moore, E. F., Shannon, C. E., and Shapiro, N. *Computability by probabilistic machines,* Automata studies, pp. 183–212. Annals of mathematics studies, no. 34. Princeton University Press, Princeton, N. J., 1956.
14. Downey, R., *Some recent progress in algorithmic randomness,* in *Proceedings of the 29 th Annual Conference on Mathematical Foundations of Computer Scence, Prague, August 2004* (invited paper) (J. Fiala, V. Koubek and J. Kratochvil eds), Springer-Verlag, Lecture Notes in Computer Science, Vol. 3153 (2004), 42-81.
15. Downey, R., *Some Computability-Theoretical Aspects of Reals and Randomness,* to appear *The Notre Dame Lectures* (P. Cholak, ed) *Lecture Notes in Logic*, Association for Symbolic Logic, 2005.
16. Downey, R., Ding Decheng, Tung Shi Ping, Qiu Yu Hui, Mariko Yasuugi, and Guohua Wu (eds), *Proceedings of the 7th and 8th Asian Logic Conferences*, World Scientific, 2003, viii+471 pages.
17. Downey, R. and E. Griffiths, *On Schnorr randomness*, Journal of Symbolic Logic, Vol 69 (2) (2004), 533-554.
18. Downey, R., E. Griffiths, and S. Reid, *On Kurtz randomness*, Theoretical Computer Science Vol. 321 (2004), 249-270.
19. Downey, R., and D. Hirschfeldt, *Algorithmic Randomness and Complexity*, Springer-Verlag Monographs in Computer Science, to appear.
20. Downey, R., D. Hirschfeldt, and G. LaForte, *Undecidability of Solovay degrees of c.e. reals*, in preparation.
21. Downey, R., D. Hirschfeldt, J. Miller, and A. Nies, *Relativizing Chaitin's halting probability*, submitted.
22. Downey, R., D. Hirschfeldt, and A. Nies, *Randomness, computability and density* SIAM Journal on Computing, 31 (2002) 1169–1183 (extended abstract

in proceedings of STACS 2001 January, 2001. Lecture Notes in Computer Science, Springer-Verlag, (Ed A. Ferriera and H. Reichel, 2001, 195-201)).

23. Downey, R., D. Hirschfeldt, A. Nies, and F. Stephan, *Trivial reals*, extended abstract in *Computability and Complexity in Analysis* Malaga, (Electronic Notes in Theoretical Computer Science, and proceedings, edited by Brattka, Schröder, Weihrauch, FernUniversität, 294-6/2002, 37-55),July, 2002. Final version appears in [16] 2003, 103-131.
24. Downey, R., D. Hirschfeldt, A. Nies, and S. Terwijn, *Calibrating randomness,* to appear, Bulletin Symbolic Logic.
25. Downey, R., and J. Miller, *A basis theorem for Π^0_1 classes of positive measure and jump inversion for random reals*, to appear, *Proceedings of the American Math. Society.*
26. Downey, R., J. Reimann, and W. Merkle, *Schnorr dimension*, to appear, Proceedings *Computability in Europe.*
27. Gács, P., *On the symmetry of algorithmic information*, Soviet Mat. Dolk., Vol. 15 (1974), 1477-1480.
28. Gács, P., *On the relation between descriptional complexity and algorithmic probability,* Theoretical Computer Science, Vol. 22 (1983), 71-93.
29. Gács, P., *Every set is reducible to a random one,* Information and Control, Vol. 70, (1986), 186-192.
30. Gaifmann, H., and M. Snir, *Probabilities over rich languages*, J. Symb. Logic, Vol. 47, (1982), 495-548.
31. Hausdorff, F., *Dimension und äußeres Maß*, Mathematische Annalen 79 (1919) 157–179.
32. Hirschfeldt, D, A. Nies, and F. Stephan, *Martin-Löf oracles*, in preparation.
33. Jockusch, C. G. , M. Lerman, R. I. Soare, and R. Solovay, *Recursively enumerable sets modulo iterated jumps and extensions of Arslanov's completeness criterion,* J. Symb. Logic, Vol. 54 (1989), 1288-1323.
34. Kautz, S., *Degrees of Random Sets,* Ph.D. Diss. Cornell, 1991.
35. Kolmogorov, A.N., *Three Approaches to the Quantitative Definition of Information*, in *Problems of Information Transmission (Problemy Peredachi Informatsii)*, 1965, Vol. 1, 1-7.
36. Kraft, L. G., *A device for quantizing, grouping, and coding amplitude modulated pulses*, M.Sc. Thesis, MIT, 1949.
37. Kučera, A., *Measure, Π^0_1 classes, and complete extensions of PA,* in *Springer Lecture Notes in Mathematics,* Vol. 1141, 245-259, Springer-Verlag, 1985.
38. Kučera, A., *An alternative priority-free solution to Post's Problem, Proceedings, Mathematical Foundations of Computer Science,* (Ed. J. Gruska, B. Rovan, and J. Wiederman), Lecture Notes in Computer Science, Vol. 233, Springer-Verlag, (1986).
39. Kučera, A., *On the use of diagonally nonrecursive functions,* in *Logic Colloquium, '87*, North-Holland, Amsterdam, 1989, 219-239.
40. Kučera, A., *Randomness and generalizations of fixed point free functions,* in *Recursion Theory Week, Proceedings Oberwolfach 1989,* (K. Ambos-Spies, G. H. Müller and G. E. Sacks, eds.) Springer-Verlag, LNMS 1432 (1990), 245-254.

41. Kučera, A. and T. Slaman, *Randomness and recursive enumerability,* SIAM Journal of Computing, Vol. 31 (2001), 199-211.
42. Kučera, A., and S. Terwijn, *Lowness for the class of random sets,* Journal of Symbolic Logic, vol. 64 (1999), 1396-1402.
43. Kummer, M., *Kolmogorov complexity and instance complexity of recursively enumerable sets,* SIAM Journal of Computing, Vol. 25 (1996), 1123-1143.
44. Kummer, M., *On the complexity of random strings*, (extended abstract) in *STACS, '96*, Springer-Verlag Lecture Notes in Computer Science, Vol 1046 (11996), 25-36.
45. Kurtz, S., *Randomness and Genericity in the Degrees of Unsolvability*, Ph. D. Thesis, University of Illinois at Urbana, 1981.
46. Levin. L., *On the notion of a random sequence*, Soviet Math. Dokl. 14 (1973) 1413–1416.
47. Levin, L., *Laws of information conservation (non-growth) and aspects of the foundation of probability theory,* Problems Informat. Transmission, Vol. 10 (1974), ' 206-210.
48. Levin, L., *Measures of complexity of finite objects (axiomatic description),* Soviet Mathematics Dolkady, vol. 17 (1976), 552-526.
49. Levy, P., *Theorie de l'Addition des Variables Aleantoires,* Gauthier-Villars, 1937.
50. Li, Ming and Vitanyi, P., *Kolmogorov Complexity and its Applications*, Springer-Verlag, 1993.
51. Loveland, D. *A variant of the Kolmogorov concept of complexity*, Information and Control, vol. 15 (1969), 510-526.
52. Lutz, J., *The dimensions of individual strings and sequences*, Information and Computation, Vol 187 (2003), pp. 49-79. (Preliminary version: *Gales and the constructive dimension of individual sequences*, in: U. Montanari, J. D. P. Rolim, E. Welzl (eds.), Proc. 27th International Colloquium on Automata, Languages, and Programming, 902–913, Springer, 2000.)
53. Lutz, J., *Effective fractal dimensions,* Mathematical Logic Quarterly Vol. 51 (2005), pp. 62-72.
54. Martin-Löf, P., *The definition of random sequences*, Information and Control, 9 (1966), 602-619.
55. Martin-Löf, P., *Complexity oscillations in infinite binary sequences,* Z. Wahrscheinlichkeittheorie verw. Gebiete, Vol. 19 (1971), 225-230.
56. Miller, J., *Kolmogorov random reals are 2-random*, Journal of Symbolic Logic,
57. Merkle W., and N. Mihailovic, *On the construction of effective random sets*, in Proceedings MFCS 2002, (ed. Diks and Rytter) Springer-Verlag LNCS 2420.
58. Merkle, W., J. Miller, A. Nies, J. Reimann, and F. Stephan, *Kolmogorov-Loveland randomness and stochasticity*, to appear, Annals of Pure and Applied Logic.
59. Miller, J., *The K-degrees, low for K degrees, and weakly low for K oracles,* in preparation.
60. Miller, J., *Solution to the question of whether* $\{x : K(x) < |x| + K(|x|) - c\}$ *is* Σ^0_1, e-mail communication, 13th January, 2005.

61. Miller, J. *Contrasting plain and prefix-free Kolmogorov complexity,* in preparation.
62. Miller, J., *A hyperimmune-free weakly 2 random real* , e-mail communication, 14th April, 2005.
63. Miller, J., and L. Yu, *On initial segment complexity and degrees of randomness*, to appear, Trans. Amer. Math. Soc.
64. Miller, J., and L. Yu, *Oscillation in the initial segment complexity of random reals,* in preparation.
65. Muchnik, An. A., and S. P. Positelsky, *Kolmogorov entropy in the context of computability theory*, Theor. Comput. Sci., Vol. 271 (2002), 15-35.
66. Muchnik, An. A., A. Semenov, and V. Uspensky, *Mathematical metaphysics of randomness,* Theor. Comput. Sci., Vol 207(2), (1998), 263-317.
67. Nies, A., *Reals which compute little*, to appear.
68. Nies, A., *Lowness properties and randomness*, to appear.
69. Nies, A., *Each Low(CR) set is computable*, typeset manuscript, January 2003.
70. Nies, A., F. Stephan and S. A. Terwijn, *Randomness, relativization, and Turing degrees*, to appear, Journal of Symbolic Logic.
71. Odifreddi, P., *Classical Recursion Theory,* North-Holland, 1990.
72. Odifreddi, P., *Classical Recursion Theory, Vol. 2,* North-Holland, North-Holland, 1999.
73. Paris, J., *Measure and minimal degrees,* Annals of Mathematical Logic, Vol. 11 (1977), 203-216.
74. Paris, J., *Survey of Results on Measure and Degrees,* unpublished notes.
75. Reimann, J, PhD Thesis, University of Heidelberg, in preparation.
76. Reimann, J., *Computability and Dimension,* unpublished notes, University of Heidelberg, 2004
77. G. Sacks, *Degrees of Unsolvability*, Princeton University Press, 1963.
78. Schnorr, C. P., *A unified approach to the definition of a random sequence,* Mathematical Systems Theory, 5 (1971), 246-258.
79. Schnorr, C. P., *Zufälligkeit und Wahrscheinlichkeit*, Springer-Verlag Lecture Notes in Mathematics, Vol 218, 1971, Springer-Verlag, New York.
80. Schnorr, C. P., *Process complexity and effective random tests*, Journal of Computer and System Sciences, vol. 7 (1973), 376-388.
81. Soare, R., *Recursively enumerable sets and degrees* (Springer, Berlin, 1987).
82. R. Soare, *Computability Theory and Differential Geometry*, bulletin Symbolic Logic, to appear.
83. Solomonoff, R., *A formal theory of inductive inference, part 1 and part2,* Information and Control, 7 (1964), 224-254.
84. Solovay, R., *Draft of paper (or series of papers) on Chaitin's work*, unpublished notes, May, 1975, 215 pages.
85. Staiger, L., *Kolmogorov complexity and Hausdorff dimension,* Information and Computation, Vol. 103 (1993), 159-194.
86. Staiger, L., *A tight upper bound on Kolmogorov complexity and uniformly optimal prediction,* Theory of Computing Sciences, Vol. 31 (1998), 215-229.
87. Staiger, L., *Constructive dimension equals Kolmogorov complexity*, Research Report CDMTCS-210, University of Auckland, January 2003.

88. Stephan, F., *Martin-Löf random sets and PA-complete sets,*to appear.
89. Stillwell, J., *Decidability of "almost all" theory of degrees,* J. Symb. Logic, Vol. 37 (1972), 501-506.
90. Tadaki, K., *A generalization of Chaitin's halting probability* Ω *and halting self-similar sets,* Hokkaido Math. J., Vol. 32 (2002), 219-253.
91. Terwijn, S. *Computability and Measure*, Ph. D. Thesis, University of Amsterdam, 1998.
92. van Lambalgen, M., *Random Sequences,* Ph. D,. Diss. University of Amsterdam, 1987.
93. van Lambalgen, M., *The axiomatization of randomness,* JSL.
94. von Mises, R., *Grundlagen der Wahrscheinlichkeitsrechnung*, Math. Z., vol. 5 (1919), 52-99.
95. Ville, J., *Ětude critique de la concept du collectif*, Gauthier-Villars, 1939.
96. Wang, Y., *Randomness and Complexity*, PhD Diss, University of Heidelberg, 1996.
97. Yu, Liang, *Degrees of generic and random reals,* to appear.
98. Yu Liang and Ding Decheng, *There is no sw-complete c.e. real*, *J. Symbolic Logic* Vol. 69 (2004), no. 4, 1163-1170.
99. Yu Liang and Ding Decheng, *The initial segment complexity of random reals*, *Proc. Amer. Math. Soc.,* Vol. 132 (2004), no. 8, 2461–2464.
100. Yu Liang, Ding Decheng, and R. Downey, *The Kolmogorov complexity of the random reals*, *Annals of Pure and Applied Logic* Volume 129, Issues 1-3 , (2004), 163-180
101. Zambella, D., *On sequences with simple initial segments*, ILLC technical report, ML-1990-05, University of Amsterdam, 1990.
102. Zvonkin A. K., and L.A. Levin, *The complexity of finite objects and the development of concepts of information and randomness by the theory of algorithms*, Russian Math. Surveys, 25(6):83-124 (1970).

INDEX