CDMTCS Research Report Series

Complexity and Randomness

S. A. Terwijn
Technical University of Vienna

CDMTCS-212
March 2003

Centre for Discrete Mathematics and
Theoretical Computer Science

Complexity and Randomness

Course notes, University of Auckland, March 2003[1]

Sebastiaan A. Terwijn

Institute for Algebra and Computational Mathematics
Technical University of Vienna
Wiedner Hauptstrasse 8-10
A - 1040 Vienna
Austria

Contents

[1]These notes were used in a series of lectures given at the University of Auckland. The author wishes to thank Bakhadyr Khoussainov and André Nies for inviting him. Financial support by the Marsden fund is gratefully acknowledged.

These course notes were compiled for a series of lectures on Complexity and Randomness at the University of Auckland, March 2003. We wish to thank Cris Calude, Bakh Khoussainov, Andre Nies, and Ludwig Staiger for hospitality and stimulating discussions.

Although this material contains more material than could be treated in 6 one-hour lectures, it is far from a complete overview of the subject. Planned sections on the structure of Δ^0_2, c.e. reals, computational depth, resource-bounded measure, and learning theory were cancelled due to lack of space and time. For a more comprehensive introduction to the subject the reader is referred to Calude [3], Downey [7] (a preliminary version of a forthcoming textbook by Downey and Hirschfeldt), and Li and Vitányi [30].

1 Introduction

1.1 Reals and Lebesgue measure

The topic of these notes is a mix of computability theory and measure theory. Our computability theory notation generally follows Odifreddi [41, 42] and Soare [48].

The Cantor space of all infinite binary sequences is denoted by 2^ω. An element $X \in 2^\omega$ is called a *real*. The set of finite initial segments of reals is denoted by $2^{<\omega}$. The space 2^ω is endowed with the tree topology, which has as basic open sets

$$[\sigma] = \{X \in 2^\omega : \sigma \sqsubset X\},$$

where $\sigma \in 2^{<\omega}$. The *uniform* or *Lebesgue measure* on 2^ω is defined as follows. Every basic open set $[\sigma]$ has the measure $\mu([\sigma]) = 2^{-|\sigma|}$, where $|\sigma|$ denotes the length of σ. (This corresponds to the *length* of the binary interval defined by σ, or alternatively by the probability that an infinite sequence chosen by random coin flips (whatever that may mean) ends up in $[\sigma]$.) The *Borel subsets* of 2^ω are defined by closing the basic open sets under unions and complements. The definition of the measure of basic opens extends in a natural way to a measure for all Borel sets. This is the *Borel measure* on 2^ω. Now if $\mathcal{B} \subset 2^\omega$ is a Borel set of measure 0, we think of $\mathcal{B}$ as being small, and it is natural to consider all subsets of $\mathcal{B}$ to be small also. So we extend the Borel measure by defining $\mu(\mathcal{A}) = 0$ whenever $\mathcal{A} \subseteq \mathcal{B}$ for some Borel $\mathcal{B}$ with $\mu(\mathcal{B}) = 0$. In this case we say that $\mathcal{A}$ is a *null set*. Now we say that $\mathcal{A}$ is *Lebesgue measurable* if $\mathcal{A} = \mathcal{B} \triangle \mathcal{C}$ is the symmetric difference of a Borel $\mathcal{B}$ and a null set $\mathcal{C}$, and in this case we define $\mu(\mathcal{A}) = \mu(\mathcal{B})$.

Now one may wonder which subsets of 2^ω are Lebesgue measurable. This turns out to be a difficult question, known as the measure problem. We will say some words about it in section 1.4.

1.2 Martingales

A different treatment of measure is the one of Ville using martingales. A *martingale* is a function $d : 2^{<\omega} \to \mathbb{R}^+$ that satisfies for every $\sigma \in 2^{<\omega}$ the averaging condition

$$2d(\sigma) = d(\sigma 0) + d(\sigma 1). \tag{1}$$

Similarly, d is a *supermartingale* if d satisfies

$$2d(\sigma) \geq d(\sigma 0) + d(\sigma 1). \tag{2}$$

A (super)martingale d *succeeds on* a set A if $\limsup_{n\to\infty} d(A\restriction n) = \infty$. We say that d succeeds on, or *covers*, a class $\mathcal{A} \subseteq 2^\omega$ if d succeeds on every $A \in \mathcal{A}$. The *success set* $S[d]$ of d is the class of all sets on which d succeeds. Below we prove that the class of sets of the form $S[d]$ coincides with the class of Lebesgue null sets.

Lemma 1.2.1 *Let d be a (super)martingale. For any string v and any prefix-free set $X \subseteq \{x : v \sqsubseteq x\}$ it holds that $2^{-|v|}d(v) \geq \sum_{x\in X} 2^{-|x|}d(x)$.*

Proof. It suffices to prove this for finite X (Bolzano-Weierstrass). Use induction on the cardinality of X. The base step $\|X\| = 1$ is immediate from (2). Suppose the lemma holds for all X of cardinality n. Let X be prefix-free and of cardinality $n+1$. Choose w of maximal length such that $X \subseteq \{x : w \sqsubseteq x\}$. Then both $X_0 = \{x \in X : w0 \sqsubseteq x\}$ and $X_1 = \{x \in X : w1 \sqsubseteq x\}$ have cardinality less than or equal to n. It follows by induction hypothesis that

$$\begin{aligned}\sum_{x\in X} 2^{|w|-|x|}d(x) &= \frac{1}{2}\sum_{x\in X_0} 2^{|w0|-|x|}d(x) + \frac{1}{2}\sum_{x\in X_1} 2^{|w1|-|x|}d(x)\\ &\leq \frac{1}{2}(d(w0)+d(w1))\\ &\leq d(w).\end{aligned}$$

Since any v with $X \subseteq \{x : v \sqsubseteq x\}$ satisfies $v \sqsubseteq w$ and by (2) it holds that $d(w) \leq 2^{|w|-|v|}d(v)$ the lemma follows by multiplying the above equations with $2^{-|w|}$. □

The following result is sometimes called "Kolmogorov's inequality for martingales".

Lemma 1.2.2 (Ville [56]) *Let d be a (super)martingale and define*

$$S^k[d] = \{X \in 2^\omega : (\exists \sigma \sqsubset X)[d(\sigma) \geq k]\}.$$

Then $\mu(S^k[d]) \leq d(\lambda)k^{-1}$.

Proof. Let $X \subseteq S^k[d]$ be prefix-free such that $\mu(X) = \mu(S^k[d])$. By Lemma 1.2.1 we have

$$k \cdot \mu(X) = k \sum_{x \in X} 2^{-|x|} \leq \sum_{x \in X} 2^{-|x|} d(x) \leq d(\lambda).$$

□

Theorem 1.2.3 (Ville [56]) *For any class $\mathcal{A} \subseteq 2^\omega$ the following statements are equivalent:*

(i) *$\mathcal{A}$ has Lebesgue measure zero,*

(ii) *There exists a martingale that succeeds on $\mathcal{A}$.*

Proof. (i)⇒(ii). Suppose $\mu(\mathcal{A}) = 0$. Then there are open sets $\mathcal{U}_k \subseteq 2^\omega$ such that $\mathcal{A} \subseteq \bigcap_k \mathcal{U}_k$ and $\mu(\mathcal{U}_k) \leq 2^{-k}$. Define the martingales d_k by

$$d_k(\sigma) = \mu(\mathcal{U}_k|\sigma) := \frac{\mu(\mathcal{U}_k \cap [\sigma])}{\mu([\sigma])},$$

and define

$$d(\sigma) = \sum_{k=0}^{\infty} d_k(\sigma).$$

Then $d(\sigma) \leq \sum_k 2^{|\sigma|-k} < \infty$ and d is a martingale because every d_k is. If $A \in \bigcap_{k\in\omega} \mathcal{U}_k$ then for all k there exists $\sigma \sqsubset A$ such that $\forall i = 1 \dots k.\ d_k(\sigma) \geq 1$, hence $d(\sigma) \geq k$, and thus $A \in S[d]$.
(ii)⇒(i). Suppose that martingale d succeeds on $\mathcal{A}$. Then by Lemma 1.2.2 the open sets $S^k[d]$ defined there have measure smaller than $d(\lambda)k^{-1}$, so $\mathcal{A}$ has measure zero. □

1.3 Three elementary theorems

A measurable set $\mathcal{A} \subseteq 2^\omega$ has *density d at X* if

$$\lim_{n\to\infty} \mu(\mathcal{A}|X{\restriction}n) := \lim_{n\to\infty} \mu(\mathcal{A} \cap [X{\restriction}n])2^n = d.$$

Define $\phi(\mathcal{A}) = \{X \in 2^\omega : \mathcal{A} \text{ has density 1 at } X\}$. Note that $\mathcal{A}$ has density 0 at each point of $\phi(\overline{\mathcal{A}})$.

We now prove a classical theorem of Lebesgue. The proof is essentially the proof given in Oxtoby [43, p17]. The proof below is somewhat simpler because the basic open sets $[x]$ have a more specific form than an arbitrary real interval.

Theorem 1.3.1 (Lebesgue Density Theorem) *If $\mathcal{A}$ is measurable then so is $\phi(\mathcal{A})$, and $\mu(\mathcal{A}\triangle\phi(\mathcal{A})) = 0$.*

Proof. It suffices to show that $\mathcal{A} - \phi(\mathcal{A})$ is a null set since $\phi(\mathcal{A}) - \mathcal{A} \subseteq \overline{\mathcal{A}} - \phi(\overline{\mathcal{A}})$ and $\overline{\mathcal{A}}$ is measurable. Define for every positive rational ε

$$\mathcal{B}_\varepsilon = \{X \in \mathcal{A} : \liminf_{n\to\infty} \mu(\mathcal{A} \cap [X{\restriction}n])2^n < 1 - \varepsilon\}.$$

Then $\mathcal{A} - \phi(\mathcal{A}) = \bigcup_\varepsilon \mathcal{B}_\varepsilon$, hence it suffices to prove that every $\mathcal{B}_\varepsilon$ is a null set. Suppose for a contradiction that for $\mathcal{B} = \mathcal{B}_\varepsilon$ we have that the outer measure $\mu^*(\mathcal{B}) := \inf\{\mu(\mathcal{U}) : \mathcal{B} \subseteq \mathcal{U} \wedge \mathcal{U} \text{ open}\} > 0$. Then there exists $\mathcal{G} \supseteq \mathcal{B}$ open with $\mu(\mathcal{G})(1 - \varepsilon) < \mu^*(\mathcal{B})$. Define

$$I = \{x \in 2^{<\omega} : [x] \subseteq \mathcal{G} \wedge \mu(\mathcal{A} \cap [x]) < (1 - \varepsilon)2^{-|x|}\}.$$

Then

(i) for any $X \in \mathcal{B}$, I contains $X{\restriction}n$ for some n, and

(ii) if $\{x_i\}_{i\in\omega}$ is a prefix-free set of elements of I then $\mu^*(\mathcal{B} - \bigcup_i [x_i]) > 0$.

The first statement holds since $\mathcal{G}$ is open and the second statement holds because $\mu^*(\mathcal{B} \cap \bigcup_i [x_i]) \leq \sum_i \mu(\mathcal{A} \cap [x_i]) < \sum_i (1 - \varepsilon)2^{-|x_i|} \leq (1 - \varepsilon)\mu(\mathcal{G}) < \mu^*(\mathcal{B})$.

Construct a sequence $\{x_i\}_{i\in\omega}$ as follows. Let x_0 in I be arbitrary, and if x_i, $i \leq n$ are defined such that $\{x_0, \dots, x_n\}$ is prefix-free, define $x_{n+1} \in I$ of minimal length such that the set $\{x_0, \dots, x_{n+1}\}$ is again prefix-free.

Now let $X \in \mathcal{B} - \bigcup_i [x_i]$. X exists by (ii). By (i), let $x \in I$ be such that $X \in [x]$. Let k be the smallest number with $[x] \cap [x_k] \neq \emptyset$. Note that k exists because there are only finitely many $y \in I$ of length shorter than x, so either $x = x_k$ or $x_k \sqsubset x$ for some k. In both cases $X \in [x] \subseteq [x_k]$, contradicting that X was not in $\bigcup_i [x_i]$. □

Next we prove a classical theorem from computability theory: Sacks' theorem on the measure of upper cones.

Theorem 1.3.2 (Sacks [45]) *For every noncomputable set $A \in 2^\omega$ the upper cone*

$$A^{\leq_T} = \{B : A \leq_T B\}$$

has measure zero.

Proof. Let A be an element of 2^ω such that $\mu(\{B : A \leq_T B\}) \neq 0$. Note that this set is measurable hence must have positive measure. We will show that A is computable. For two classes $\mathcal{C}$ and $\mathcal{D}$ define $\mu(\mathcal{C}|\mathcal{D}) = \mu(\mathcal{C} \cap \mathcal{D})/\mu(\mathcal{D})$ and for a formula P write $\mu(P(B))$ for $\mu(\{B \in 2^\omega : P(B)\})$. Since $\{B : A \leq_T B\} = \bigcup_e \{B : A = \{e\}^B\}$ has positive measure there exists $e \in \omega$ such that $\mu(\{B : A = \{e\}^B\}) > 0$. It follows from Theorem 1.3.1 that there is a point $X \in 2^\omega$ such that $\mathcal{A}$ has density 1 at X. From this follows the existence of a $\sigma \in 2^{<\omega}$ such that $\mu(A = \{e\}^B | [\sigma]) \geq 3/4$. Using σ we can compute A as follows. For any $x \in \omega$ the sets $T_n = \{X \sqsupset \sigma : \{e\}^X(x)\downarrow = n\}$ are uniformly c.e., so we can enumerate the T_n's, $T_n = \bigcup_s T_{n,s}$, until we find n with $\mu(T_{n,s}) \geq 3/4$. Then $A(x) = n$. □

Next we prove Kolmogorov's 0-1 law for measurable sets. As Sacks' theorem above, it can be proved directly, but it also follows very quickly from Lebesgues density theorem. (This was pointed out to us by Jack Lutz.)

Definition 1.3.3 $\mathcal{E} \subseteq 2^\omega$ is a *tail set* if $\mathcal{A}$ is closed under finite variances, i.e., if $v \in 2^{<\omega}$ and $X \in 2^\omega$ are such that $vX \in \mathcal{E}$ then $wX \in \mathcal{E}$ for every string w of length $|v|$.

Theorem 1.3.4 (Kolmogorov's 0-1 law) *If $\mathcal{A} \subseteq 2^\omega$ is a measurable tail set then either $\mu(\mathcal{A}) = 0$ or $\mu(\mathcal{A}) = 1$.*

Proof. Suppose $\mu(\mathcal{A}) > 0$. By Theorem 1.3.1, choose $X \in \mathcal{A}$ such that $\mathcal{A}$ has density 1 at X. Let $\varepsilon \in (0,1)$ be arbitrary. Choose n large enough such that $\mu(\mathcal{A} \cap [X{\restriction}n])2^n > 1 - \varepsilon$. Because $\mathcal{A}$ is a tail set we then have that $\mu(\mathcal{A} \cap [w])2^n > 1 - \varepsilon$ for *any* w of length n. So $\mu(\mathcal{A}) > 1 - \varepsilon$. Since ε was arbitrary it follows that $\mu(\mathcal{A}) = 1$. □

1.4 Measure and set theory

We do not give a full treatment of the measure problem here, but merely make some remarks about it. First, it is well-known that under AC there are nonmeasureable sets, using Vitali's construction. Solovay [50] proved that, assuming that there exists an inaccessible cardinal, there is a model of set theory in which all sets of reals are Lebesgue measurable. More precisely, Con(ZFC + ∃inaccessible) → Con(ZF + DC + all sets of reals measurable).

We now prove that under AD, the axiom of determinacy, every set of reals is Lebesgue measurable. Since AD is game theoretic, it is natural to use Ville's game theoretic characterization of measure from Theorem 1.2.3.

The proof below is a variant of the proof using Harringtons covering game [14, p552], [37, p424], [18, p307].

Given a set $\mathcal{A} \subseteq 2^\omega$, consider the following betting game $G(\mathcal{A})$:

$$\begin{array}{rllllll} \text{I}: & a_0 & & a_1 & & a_2 & \dots \\ \text{II}: & & (d(a_0 0), d(a_0 1)) & & (d(a_0 a_1 0), d(a_0 a_1 1)) & & \dots \end{array}$$

Here every $a_i \in \{0,1\}$, so player I plays $A = (a_i)_{i\in\omega} \in 2^\omega$, and for every n, $d(A{\restriction}n) \in \mathbb{Q}^{\geq 0}$, $d(\emptyset) = 1$, and

$$d(A{\restriction}n) \geq \frac{d(A{\restriction}n\hat{\ }0) + d(A{\restriction}n\hat{\ }1)}{2} \tag{3}$$

Player I wins if $A \in \mathcal{A}$ and $A \notin S[d] = \{X : \limsup_n d(X{\restriction}n) = \infty\}$.

A strategy for II is a martingale $d : 2^{<\omega} \to \mathbb{Q}^{\geq 0}$.

Lemma 1.4.1 *(Compare [14, p552]) (AD) When $\mathcal{A} \subseteq 2^\omega$ is such that every measurable $\mathcal{B} \subseteq \mathcal{A}$ is a null set, then $\mathcal{A}$ is also a null set.*

Theorem 1.4.2 *(AD) Every $\mathcal{A} \subseteq 2^\omega$ is measurable.*

Proof. Since every $\mathcal{A}$ always has an outer measure we always have a measurable $\mathcal{X} \supseteq \mathcal{A}$ such that $\mathcal{X} - \mathcal{A}$ does not contain any measurable subsets of measure 0. By Lemma 1.4.1 it follows that $\mathcal{X} - \mathcal{A}$ is null, hence $\mathcal{A}$ is measurable, with measure $\mu(\mathcal{X})$. □

Proof of Lemma 1.4.1. Let $\mathcal{A} \subseteq 2^\omega$ be as in the lemma.
Claim: I does not have a winning strategy for $G(\mathcal{A})$.
Proof of claim: Suppose I does have winning strategy σ. Consider $\mathcal{B} = \{\sigma * \tau : \tau \text{ is strategy for II }\}$. Then $\mathcal{B}$ is measurable (being $\mathbf{\Sigma}^1_1$, cf. [14, Thm 94], [37, p301]. Alternatively, directly construct a martingale that succeeds on $\mathcal{B}$), and because σ is winning we have $\mathcal{B} \subseteq \mathcal{A}$. Hence by hypothesis $\mu(\mathcal{B}) = 0$. By Theorem 1.2.3 there is a martingale d that wins on $\mathcal{B}$, but since such a d is a strategy that defeats σ this contradicts that σ is winning.

So by determinacy we have that II has a winning strategy. (AD says that every Gale-Stewart game is determined. It is easy to see that this implies also the determinacy of variants such as the betting game $G(\mathcal{A})$ above.) But such a strategy is a martingale that wins on $\mathcal{A}$, so again by Theorem 1.2.3 we have that $\mu(\mathcal{A}) = 0$. □

2 Random finite strings

According to classical probability theory, based on measure theory, every real is just as probable as another one. Also, for a fixed length n, every string of length n is just as probable as another. Yet we feel that there are great qualitative differences between strings. E.g. the sequence $000\dots 0$ consisting of 100 zeros appears to us to be special among all strings of length 100. This is part of the motivation of introducing a complexity measure for individual strings and reals. General introductions to this area are Calude [3] and Li and Vitányi [30]. Our notation in this section mainly follows [30].[2]

2.1 Plain Kolmogorov complexity

Fix a universal Turing machine U. Given a string $\sigma \in 2^{<\omega}$, define the *plain Kolmogorov complexity* of σ as

$$C(\sigma) = \min\{|\tau| : U(\tau) = \sigma\}.$$

Basic facts of C:

- The choice of U matters only an additive constant in the theory.
- For all σ, $C(\sigma) \leq |\sigma| + O(1)$.
- We can define σ to be *k-random* if $C(\sigma) \geq |\sigma| - k$. An easy counting argument shows that random strings exist: Given length n, there are

  $$\sum_{i=0}^{n-k-1} 2^{-i} = 2^{n-k} - 1$$

  programs of length $< n-k$, so there are $2^n - 2^{n-k} + 1$ k-random strings of length n.
- For every k, the set of k-random strings is an *immune* Π^0_1 set, i.e. it does not contain any infinite c.e. subsets. Namely suppose it is not immune. Then for every m we can compute a string $\psi(m)$ with $C(\psi(m)) \geq m$. But then $m \leq C(\psi(m)) \leq \log m + O(1)$, which can only be true for finitely many m, a contradiction.

[2] There are two traditions of notation in the theory of Kolmogorov complexity. One is the C/K tradition which uses C to denote the plain Kolmogorov complexity and K for the prefix-free complexity. The other tradition uses K and H. In these notes we will follow the first tradition.

- As a corollary to the previous item we obtain
  - C is not computable
  - If $m(x) = \min\{C(y) : y \geq x\}$, then m is unbounded (because we run out of short programs), but
  - m grows slower than any partial recursive function (since otherwise we could enumerate infinitely many high-complexity strings, which is impossible by immunity, see above).

We would like to extend the definition of randomness for finite strings to a definition for infinite strings. Naively, we could define a real A to be random if and only if for some k every $\sigma \sqsubset A$ would be k-random. However, such reals do not exist! We see this using the following argument by Katseff [16]. Suppose $A\restriction m$ is the n-th binary string. Then from the *length* of $A\restriction n$ we can recover $A\restriction m$, which is of length $\log n$. This gives

$$C(A\restriction n) \leq C(A\restriction m+1 \dots n) \leq n - \log n + O(1).$$

Namely first generate $C(A\restriction m+1 \dots n)$. Compute n from its length $n - \log n$. Then recover $A\restriction m$.

So we see that for any real A, infinitely often the length of $A\restriction n$ codes extra information. Chaitin and Levin argued that only the *bits* of A should count in measuring its complexity. This prompted them to introduce (different versions of) K, the prefix-free complexity of the next section.

2.2 Prefix-free complexity

Call a Turing machine T a *prefix machine* if $\text{dom}(T) \subseteq 2^{<\omega}$ is prefix-free. It is easy to construct a *universal* prefix machine U:

$$U(\langle m, \sigma \rangle) = T_m(\sigma),$$

for an effective enumeration $T_0, T_1, \dots$ of all prefix machines. Here $\langle m, \sigma \rangle$ denotes a prefix encoding of the pair (m, σ).

Now we can define the *prefix-free complexity* of a string σ as

$$K(\sigma) = \min\{|\tau| : U(\tau) = \sigma\}.$$

Basic facts of C:

- Again, the choice of U matters only an additive constant in the theory.

- The prefix encoding $\widehat{\sigma} = 1^{|\sigma|}0\sigma$ gives $K(\sigma) \leq 2|\sigma| + O(1)$.
- The prefix encoding $\widehat{|\sigma|}\sigma$ gives $K(\sigma) \leq |\sigma| + 2\log|\sigma| + O(1)$.
- Unlike C, K is *subadditive*:

  $$K(x, y) := K(\langle x, y \rangle) = K(x) + K(y) + O(1).$$

  (Simply concatenate programs for x and y. Because the set of programs is prefix-free, we do not need a special encoding to separate programs.)
- All facts about the computability of C and the immunity of the high-complexity strings also hold for K.
- Almost all σ have high K-complexity. This counting argument (which was easy for C) is now much harder! It will be proved in Theorem 2.6.3.

The naive approach to define a real to be random if and only if all its initial segments have high Kolmogorov complexity, which failed for C, does work for K, as we shall see in section 3.1.

2.3 Kraft inequality, Shannon-Fano code

In the following we will make extensive use of the next easy theorem. A *prefix code* is a prefix-free subset of $2^{<\omega}$. The elements of a prefix code are its *code words*.

Theorem 2.3.1 (Kraft [22]) *Let $l_1, l_2, l_3, \ldots$ be a sequence of natural numbers, possibly with repetitions. Then there is a prefix code with the l_i as the lengths of its code words if and only if $\sum_i 2^{-l_i} \leq 1$.*

Proof. For the 'only if' direction, note that a prefix code corresponds with an open subset of 2^ω, and that $\sum_i 2^{-l_i}$ is precisely the *measure* of this open set, and hence bounded by 1.

For the 'if' direction, enumerate a set of code words as follows. Set off intervals in 2^ω of length l_i, going from left to right. If the sequence l_i is nondecreasing, which we may assume here, then all these intervals are in fact of the form $[\sigma]$. Choose the σ as code words. $\square$

Chaitin [5] (see also [6, p113]) proved the following extension of Krafts theorem: Let a c.e. set of *requirements* (x_k, n_k), $k \in \omega$, be given. (Again there may be repetitions.) We think of (x_k, n_k) as saying that we want a code word of length n_k for x_k. Then, if $\sum_k 2^{-n_k} \leq 1$ one can construct a prefix machine M whose domain is a prefix code that satisfies all the requirements, i.e. such that for all x and n, $\big|\{\sigma : |\sigma| = n \wedge M(\sigma) = x\}\big| = \big|\{k : (x_k, n_k) = (x, n)\}\big|$. The enumeration of code words runs as follows. Initially all code words in $2^{<\omega}$ are available. If a code word is enumerated, it and all its prefixes and extensions become unavailable. Given code words of lengths $l_1, \ldots, l_n$, enumerate the lexicographically first available code word of length l_{n+1}. A full proof that in assigning code words one never runs out of available strings (under the condition $\sum_k 2^{-n_k} \leq 1$) is in Calude [3, p49 ff.].

The construction of M is sometimes referred to as "Chaitin-simulation", and the existence of M as the Kraft-Chaitin theorem.

Next we explain a similar result, the Shannon-Fano code [47]. (See also [30, p63,p224].) The idea of the Shannon-Fano code is that symbols with high probabilities receive short code words σ. The code word σ will be defined by the largest binary interval included in the interval of length the probability.

A *discrete semimeasure* is a function $P : \omega \to \mathbb{R}$ such that $\sum_x P(x) \leq 1$.

Theorem 2.3.2 (Shannon-Fano code [47]) *Given a discrete semimeasure P on ω, there is a prefix code E such that for the x-th code word $E(x)$ it holds that $|E(x)| \leq -\log P(x) + 2$.*

Proof. As in the proof of Krafts Theorem, set off intervals I_x of length $P(x)$ from left to right. Since the numbers $-\log P(n)$ need not be integers, we cannot assume the n-th interval to be a binary interval. Let i_x be the length of the longest binary interval included in I_x. If there are 3 consecutive binary intervals of size 2^{-n} in I_x there is also a binary interval of size $2 \cdot 2^{-n}$ in it. So $i_x \geq \frac{P(x)}{3}$, hence $-\log i_x \leq -\log P(x) + \log 3 \leq -\log P(x) + 2$. Now let $E(x)$ be the binary code word corresponding to the leftmost binary interval of length i_x. □

2.4 The universal semimeasure m

- Recall from the previous section that a *discrete semimeasure* is a function $P : \omega \to \mathbb{R}$ such that $\sum_x P(x) \leq 1$.
- P_0 is *universal* for a class of semimeasures $\mathcal{M}$ if P_0 multiplicatively dominates $\mathcal{M}$: $(\forall P \in \mathcal{M})(\exists c > 0)(\forall x \in \omega)\big[P_0(x) \geq cP(x)\big]$.

- A Σ_1-*function* is a function whose values are computably approximable from below. E.g. $-C$ and $-K$ are Σ_1-functions.

- There is a universal Σ_1-semimeasure $\mathbf{m}$ (Zvonkin and Levin [60]): Let $P_1, P_2, \dots$ be an effective enumeration of all Σ_1-semimeasures (such an enumeration is easily seen to exist: Effectively enumerate all Σ_1-functions P, and redefine P to be constant 0 from a point onwards if the sum $\sum_x P(x)$ becomes to large), and define $\mathbf{m}(x) = \sum_n 2^{-n} P_n(x)$. (We will construct universal objects in a similar way in Theorem 3.2.1 and section 3.5.) An alternative definition for $\mathbf{m}$ is $\mathbf{m}(x) = \sum_n 2^{-K(n)} P_n(x)$.

- Of course we are using Σ_1-semimeasures, since Σ_1-measures P with $\sum_x P(x) = 1$ are computable and the computable semimeasures have no universal element. (This last fact can be proved by a direct diagonalization: Suppose P is universal. Build Q such that $(\forall c > 0)(\exists x)\big[Q(x) > cP(x)\big]$. This works because $P(x) \to 0$.)

- We see that $\mathbf{m}$ is not computable and that $\sum_x m(x) < 1$.

2.5 A priori probability

- Let T be a prefix machine (see section 2.2). Define

$$Q_T(x) = \sum_{T(\sigma)=x} 2^{-|\sigma|},$$

  the probability that T computes x. (We will have to say more about such probabilities in section 3.3.)

- By taking for T a universal prefix machine U we obtain the *universal a priori probability* Q_U (Solomonoff [49]).

- Q_U is very important for learning theory. Solomonoff proposed to use Q_U as a universal prior in Bayes' rule:

$$\Pr(x|y) = \frac{\Pr(y|x)\Pr(x)}{\Pr(y)}.$$

  This may be seen as a solution to the old philosophical problem of what to choose as a prior.

2.6 Coding, symmetry, and counting

The next theorem relates the subjects of the previous three sections:

Theorem 2.6.1 (Coding Theorem, Levin [29, 60], Chaitin [5]) *Up to an additive constant, for all x*

$$-\log \mathbf{m}(x) = -\log Q_U(x) = K(x).$$

Proof. To be provided during the course. □

Recall that $K(x, y)$ is defined as $K(\langle x, y\rangle)$.

Theorem 2.6.2 (Symmetry of Information, Levin)

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

Hence

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

Proof. To be provided during the course. □

Theorem 2.6.3 (Counting Theorem, Chaitin [5])

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

(ii) $\big|\{x : |x| = n \wedge K(x) \leq n+K(n)-r\}\big| \leq 2^{n-r+O(1)}$, *where the constant $O(1)$ does not depend on n and r.*

Proof. To be provided during the course. □

3 Random infinite strings

3.1 Various approaches in historical order

Among the oldest definitions of randomness are the definitions saying that a random sequence should have certain stochastic properties, such as being normal in the sense of Bernoulli. These approaches have been quite important for the subject, and many interesting and deep theorems have been proven about them, but we will not treat them here. For a discussion of stochasticity properties see we refer the reader to Ambos-Spies and Kučera [1].

Below, we restrict ourselves to those definitions of randomness that use a constructive version of Lebesgue measure or that use a constructive version of Ville's game-theoretic martingale framework.

$\mathcal{A} \subseteq 2^\omega$ is a Σ^0_1-class if there is a c.e. $A \subseteq 2^{<\omega}$ such that $\mathcal{A} = \bigcup_{\sigma\in A}[\sigma]$.

Definition 3.1.1 (Martin-Löf [35]) *A set of reals $\mathcal{A} \subseteq 2^\omega$ is Martin-Löf null (or* Σ_1-null*) if there is a uniformly c.e. sequence $\{\mathcal{U}_i\}_{i\in\omega}$ of Σ^0_1-classes (called a* Martin-Löf test*) such that $\mu(\mathcal{U}_i) \leq 2^{-i}$ and $\mathcal{A} \subseteq \bigcap_i \mathcal{U}_i$. $A \in 2^\omega$ is Martin-Löf random, or* Σ_1-random, *if $\{A\}$ is not Σ_1-null.*

Definition 3.1.2 (Schnorr [46]) *A* Schnorr test *is a Martin-Löf test $\{\mathcal{U}_i\}_{i\in\omega}$ with the additional property $\mu(\mathcal{U}_i) = 2^{-i}$. Equivalently, the sequence of reals $\mu(\mathcal{U}_i)$ is a uniformly computable sequence of computable reals. $\mathcal{A}$ is* Schnorr null *if $\mathcal{A} \subseteq \bigcap_i \mathcal{U}_i$ for some Schnorr test $\{\mathcal{U}_i\}_{i\in\omega}$, and A is* Schnorr random *if $\{A\}$ is not Schnorr null.*

Definition 3.1.3 (Solovay [51]) *A real A is* Solovay random *if for all uniformly c.e. sequences $\{\mathcal{U}_i\}_{i\in\omega}$ with $\sum_{i=0}^{\infty} \mu(\mathcal{U}_i) < \infty$, $A \in \mathcal{U}_i$ for only finitely many i. Note that the definition does not change if we replace the Σ^0_1-classes $\mathcal{U}_i$ by* intervals $[\sigma_i]$ *here.*

Definition 3.1.4 (Chaitin [5]) *A real A is* Chaitin random *(or Kolmogorov-Chaitin random) if there is a constant c such that $K(A\restriction n) \geq n - c$ for every n.*

Definition 3.1.5 (Schnorr [46], Lutz [31, 32]) *A real A is* computably random *if there is no computable martingale succeeding on A.*

There are more definitions of random reals in the literature (see e.g. [17, 26, 30, 57]), but we will not discuss these here. In the following, we will make use of some of the above definitions in relativized form, though. Relativizing computable randomness to K, the halting set, yields Δ_2*-randomness*, and relativizing Schnorr randomness to K yields *Schnorr* Δ_2*-randomness.* Relativizing Martin-Löf's Σ_1-randomness to K yields Σ_2*-randomness.*

In section 3.2 we will prove that a real A is Martin-Löf random if and only if it is Solovay random if and only if it is Chaitin random. Also, we will prove that the following sequence of measure zero notions is strictly increasing in strength.

(i) Schnorr null

(ii) computably null

(iii) Σ_1-null

(iv) Schnorr Δ_2-null

(v) Δ_2-null

(vi) Σ_2-null

From the definitions it is immediate that (i)$\Rightarrow$(ii)$\Rightarrow$(iii). (ii)$\not\Rightarrow$(i) was proved by Wang, (Theorem 3.2.8, see also Theorem 3.2.9), and (iii)$\not\Rightarrow$(ii) follows since the computable sets have Σ_1-measure zero. (This does not immediately imply that Σ_1-randomness is different from computable randomness. This will be proved in Theorem 3.2.7.) The strict implications (iv)$\Rightarrow$(v)$\Rightarrow$(vi) follow from relativizing this. (iii)$\Rightarrow$(iv) follows because given a Martin-Löf test $\{\mathcal{U}_i\}_{i\in\omega}$, with K we can exactly compute $\mu(\mathcal{U}_i)$ for every i, so $\{\mathcal{U}_i\}_{i\in\omega}$ is automatically a K-computable Schnorr test. Finally, (iv)$\not\Rightarrow$(iii) because, as noted above, there are $A \in \Delta_2$ such that $\{A\}$ is not Σ_1-null, whereas for every $A \in \Delta_2$ we have that $\{A\}$ is mod-Δ_2-null. So (i)$-$(vi) is indeed a sequence of notions of measure 0 increasing in strength.

A martingale characterization of Definition 3.1.2 will be given in section 3.5.

3.2 Several equivalences and separations

We start off by giving some basic facts about Martin–Löf randomness. The next theorem shows that there is a universal Martin-Löf null set:

Theorem 3.2.1 (Martin-Löf [35]) *There exists a universal Martin-Löf test. That is, there is a computable sequence of Σ^0_1 classes $\mathcal{U}_0,\mathcal{U}_1,\ldots$ such that*

- $\mathcal{U}_0 \supseteq \mathcal{U}_1 \supseteq \ldots$
- $\forall n\,(\mu(\mathcal{U}_n) < 2^{-n})$
- *for any Σ^0_1-approximable class $\mathcal{A}$ we have $\mathcal{A} \subseteq \bigcap_n \mathcal{U}_n$.*

Proof. Our presentation follows Kučera [23]. For every n construct a c.e. set $U_n \subseteq 2^{<\omega}$ as follows. For every $e > n$, U_n enumerates all the elements of $W_{\{e\}(e)}$ (where we take this set to be empty if $\{e\}(e)$ is undefined) as long as $\mu(W_{\{e\}(e)}) < 2^{-e}$. Define $\mathcal{U}_n = \mathrm{Ext}(U_n)$. Then $\mu(\mathcal{U}_n) < \sum_{e>n} 2^{-e} = 2^{-n}$, and if $\{e\}$ defines a Martin-Löf test then for every n there exists by padding $i \in \omega$ (in fact, infinitely many i) such that $W_{\{e\}(i)} \subseteq \mathcal{U}_n$ (if $i > n$ is an alternative code for e then $W_{\{e\}(i)} = W_{\{i\}(i)} \subseteq U_n$), so $\bigcap_i W_{\{e\}(i)} \subseteq \bigcap_n \mathcal{U}_n$. □

Definition 3.2.2 For every n, denote by $\mathcal{U}_n$ the Σ^0_1 class from the above proof. Define $\mathcal{P}_n$ to be the complement of $\mathcal{U}_n$.

Define the *left shift* $T : 2^\omega \to 2^\omega$ by $T(C)(n) = C(n+1)$. Let T^k denote the k-iteration of T.

Theorem 3.2.3 (Kučera) *For every Σ_1-random C there exists $k \in \omega$ such that $T^k(C) \in \mathcal{P}_0$.*

Proof. For a set of initial segments Σ and a class $\mathcal{A}$ define $\Sigma\hat{}\mathcal{A} = \{\sigma\hat{}A : \sigma \in \Sigma \wedge A \in \mathcal{A}\}$, where $\sigma\hat{}A$ denotes the concatenation of σ with the characteristic sequence of A. Fix a c.e. set U_0 that defines the Σ^0_1 class $\mathcal{U}_0$. By induction define $\mathcal{U}_0^1 = \mathcal{U}_0$ and $\mathcal{U}_0^{k+1} = U_0\hat{}\mathcal{U}_0^k$.
Now by $q = \mu(\mathcal{U}_0) < 1$ there is an $l \in \omega$ such that $q^l < 1/2$, so $\mu(\mathcal{U}_0^{kl}) = q^{kl} < 2^{-k}$. It follows that the sequence

$$\mathcal{U}_0,\ \mathcal{U}_0^l,\ \mathcal{U}_0^{2l},\ \ldots$$

constitutes a Martin-Löf test. Therefore, if C is Σ_1-random then either $C \notin \mathcal{U}_0$, i.e. $C \in \mathcal{P}_0$ and we are done, or for some $k > 0$ we have $C \in \mathcal{U}_0^{kl}$ and $C \notin \mathcal{U}_0^{(k+1)l}$. But the latter means that $T^{k'}(C) \notin \mathcal{U}_0$ for some k', so $T^{k'}(C) \in \mathcal{P}_0$. □

Theorem 3.2.4 (Solovay [51]) $A \in 2^\omega$ *is Solovay random if and only if it is Martin-Löf random,*

Proof. It is immediate from the definitions that every Solovay random real is Martin-Löf random. For the other direction, suppose that X is Martin-Löf random and that $\{I_n\}_{n\in\omega}$ is a computable sequence of intervals such that $\sum_{n=0}^{\infty} |I_n| < \infty$. Without loss of generality, $\sum_{n=0}^{\infty} |I_n| < 1$. Define

$$\mathcal{V}_k = \big\{Y : Y \in I_n \text{ for } \geq 2^k \text{ many } I_n\big\}.$$

Then $2^k\mu(\mathcal{V}_k) \leq \sum_{n=0}^{\infty} |I_n| < 1$. (It suffices to prove this for any finite collection of I_n's, with induction on the number of I_n's.) It follows that $\{\mathcal{V}_k\}_{k\in\omega}$ is a Martin-Löf test, and thus $X \notin \bigcap_k \mathcal{V}_k$. □

Theorem 3.2.5 (Schnorr, see Chaitin [5]) $A \in 2^\omega$ *is Martin-Löf random if and only if it is Chaitin random, i.e. there is a constant c such that $K(A{\restriction}n) \geq n - c$ for every n.*

Proof. (Only if) Define $\mathcal{U}_k = \big\{X : \exists n\ K(X{\restriction}n) \leq n - k\big\}$. That this is a test follows from the Counting Theorem 2.6.3. Namely, by Theorem 2.6.3 we have for all n and k that

$$\mu\big(\big\{X : K(X{\restriction}n) \leq K(n) + n - k\big\}\big) \leq 2^{-k+O(1)},$$

where the $O(1)$ does not depend on n and k. Subtracting $K(n)$ from k we obtain,

$$\mu\big(\{X : K(X\restriction n) \leq n - k\}\big) \leq 2^{-K(n)-k+O(1)},$$

Hence $\mu(\mathcal{U}_k) \leq 2^{-k+O(1)} \sum_n 2^{-K(n)} \leq 2^{-k+O(1)}$, so $\{\mathcal{U}_k\}_{k\in\omega}$ is a test. So if A is Martin-Löf random then there is k such that $A \notin \mathcal{U}_k$.

(If) Suppose that $\{\mathcal{U}_k\}$ is a Martin-Löf test. Define

$$L = \big\{|\sigma| - k : \sigma \in \mathcal{U}_{2k}, k > 1\big\}.$$

L is c.e., and L satisfies Kraft:

$$\sum_{k>1} \sum_{\sigma\in\mathcal{U}_{2k}} 2^{-|\sigma|+k} = \sum_{k>1} 2^k \mu(\mathcal{U}_{2k}) \leq \sum_{k>1} 2^k 2^{-2k} = \sum_{k>1} 2^{-k} \leq 1.$$

So by Kraft-Chaitin (page 9) there is a prefix code assigning strings of length $|\sigma| - k$ to σ, i.e. there is prefix-free machine T such that

$$K_T(\sigma) \leq |\sigma| - k$$

for all $\sigma \in \mathcal{U}_{2k}$, $k > 1$. Since K is additively optimal, if $A \in \bigcap_k \mathcal{U}_k$ then for all k there is n such that $A\restriction n \in \mathcal{U}_{2k}$, so

$$K(A\restriction n) \leq K_T(A\restriction n) + O(1) \leq n - k + O(1).$$ □

Recall that a real A is computably random if and only if there is no computable martingale d such that $\limsup_n d(A\restriction n) = \infty$. The next lemma says that the definition does not change if we replace 'limsup' by 'lim.'

Lemma 3.2.6 (Savings Lemma, Lutz) *For every computable martingale d there is a computable martingale d' such that $S[d] \subseteq \{A : \lim_n d'(A\restriction n) = \infty\}$.*

Proof. Without loss of generality suppose $d(\lambda) = 1$. Define d' by using the same betting percentages $\dfrac{d(\sigma i)}{d(\sigma}$, $i \in \{0, 1\}$, at every point in the tree, but by letting d' *save* one dollar every time its value becomes bigger than 2, and use the other dollar for betting. If d becomes infinitely large, d' will become bigger than 2 infinitely often, since it is using the same betting strategy, and hence d' will be saving infinitely many dollars. □

Theorem 3.2.7 (Schnorr [46, Satz 7.2]) *There is a computably random real that is not Martin-Löf random.*

Proof. We follow some notes of Lutz and Gasarch from around 1991. This proof is essentially the same as Schnorr's proof. We use Lemma 3.2.6 saying that that randomness using "lim sup" in the definition of success of a martingale is equivalent to randomness defined using just "lim". Let $\mathcal{U}_n$ be a sequence of c.e. open sets such that $\mathcal{U}_n \supseteq \mathcal{U}_{n+1}$ and $\text{ML-RAND}^c = \bigcap_{n=0}^{\infty} \mathcal{U}_n$ (see Theorem 3.2.1). Let $d_0, d_1, d_2, \dots$ be a (necessarily noneffective) enumeration of all computable martingales d such that $d(\lambda) = 1$. We construct $A \in \text{compRAND} \setminus \text{ML-RAND}$ as a union of initial segments $A = \bigcup_{k=0}^{\infty} w_k$. We define w_k and numbers l_k with the properties

(i) $w_k \sqsubset w_{k+1}$,

(ii) $[w_k] \subseteq \mathcal{U}_k$,

(iii) $\sum_{j=0}^{k} 2^{-l_j} d_j(w_k) \leq 1 - 2^{-k}$.

Item (ii) guarantees that for every k it holds that $A \in \mathcal{U}_k$, hence $A \notin$ ML-RAND, and item (iii) guarantees that $\lim_{n\to\infty} d_j(A{\upharpoonright}n) < \infty$ for every j, so $A \in$ compRAND.

Define l_k and w_k with induction as follows. Let $l_{-1} = 0$ and $w_{-1} = \lambda$. Suppose that l_k and w_k satisfying (i), (ii), and (iii) are defined. Let $l_{k+1} = |w_k| + k + 2$ and define $\tilde{d} = \sum_{j=0}^{k+1} 2^{-l_j} d_j$. Then

$$
\begin{aligned}
\tilde{d}(w_k) &\leq 1 - 2^{-k} + 2^{-l_{k+1}} d_{k+1}(w_k) \\
&\leq 1 - 2^{-k} + 2^{-l_{k+1}} 2^{|w_k|} \\
&= 1 - 2^{-k} + 2^{-(k+2)} \\
&< 1 - 2^{-(k+1)}.
\end{aligned}
$$

By direct diagonalization there exists $Y \in [w_k] \cap \text{COMP}$ such that $\tilde{d}(w) \leq 1 - 2^{-(k+1)}$ for every w with $w_k \sqsubseteq w \sqsubset Y$. Because $Y \in \text{COMP} \subseteq \text{ML-RAND}^c \subseteq \mathcal{U}_{k+1}$ and this last set is open there exists $w_k \sqsubset w_{k+1} \sqsubset Y$ such that $[w_{k+1}] \subseteq \mathcal{U}_{k+1}$. This w_{k+1} clearly satisfies (i), (ii), and (iii). □

Theorem 3.2.8 (Wang [58]) *There exists a Schnorr random real that is not computably random.*

Theorem 3.2.9 (Terwijn [53]) *There exists a subset $\mathcal{A}$ of* COMP *such that $\mathcal{A}$ has computable measure 0 but not Schnorr measure 0.*

Proof. For every number $n = \langle e, f\rangle$ recursively define a set of numbers $\{\langle y_m^n, z_m^n\rangle : m \in \omega\}$ as follows. Let $y_0^n = z_0^n = n$. If $\langle y_{m-1}^n, z_{m-1}^n\rangle$ is defined let $\langle y_m^n, z_m^n\rangle$ be the smallest number such that $y_m^n \geq z_m^n$, and

$$2^{y_{m-1}^n + 1} < \varphi_{f, y_m^n}(z_m^n)\downarrow \tag{4}$$

if this exists and let $\langle y^n_m, z^n_m \rangle$ be undefined otherwise.
Call a number $\langle e, f \rangle$ a Schnorr-test if φ_e is a martingale with $\varphi_e(\lambda) = 1$ and φ_f is a monotonic unbounded function. For every Schnorr-test $n = \langle e, f \rangle$ define a computable set A_n that escapes n: Let $A_n{\restriction}n = \emptyset{\restriction}n$ and define $A_n(n) = 1$, so that $0^n1 \sqsubset A_n$ and the number n is coded in this way into the initial segment of A_n. Since φ_e is a martingale and φ_f is unbounded we can recursively define the rest of A_n as follows. Given $A_n{\restriction}y^n_{m-1}$, define $A_n{\restriction}y^n_m$ to be the (lexicographically) first string σ of length y^n_m such that $(A_n{\restriction}y^n_{m-1})1 \sqsubseteq \sigma$ and

$$(\forall j)[\ y^n_{m-1} < j < |\sigma| - 1 \rightarrow \varphi_e(\sigma{\restriction}j) \geq \varphi_e(\sigma{\restriction}j+1)\ ] \tag{5}$$

i.e. the martingale φ_e does not grow along σ. For every A_n defined in this way we have

$$\begin{array}{rcll} \varphi_e(A_n{\restriction}y^n_m) & \leq & \varphi_e((A_n{\restriction}y^n_{m-1})1) & (\varphi_e \text{ does not grow}) \\ & \leq & 2^{y^n_{m-1}+1} & (\forall w(\varphi_e(w) \leq 2^{|w|})) \\ & < & \varphi_{f,y^n_m}(z^n_m)\downarrow & (\text{by } (4)) \\ & \leq & \varphi_f(y^n_m) & (y^n_m \geq z^n_m \text{ and } \varphi_f \text{ is monotone}) \end{array}$$

Thus, by (5) we have

$$(\forall i > n)[\ \varphi_e(A_n{\restriction}i) < \varphi_f(i)\ ],$$

and hence $A_{\langle e,f \rangle} \notin S_{\varphi_f}[\varphi_e]$. Now define $\mathcal{A} = \{A_n : n \text{ is a Schnorr-test}\}$ Then there is no Schnorr-test $\langle e, f \rangle$ such that $\mathcal{A} \subseteq S_{\varphi_f}[\varphi_e]$, and hence $\mathcal{A}$ is not Schnorr null. On the other hand, $\mathcal{A}$ does have computable measure zero. Namely, define a computable martingale d that succeeds on $\mathcal{A}$ as follows. Let $d(\lambda) = 1$, and for $w = 0^n1v$ define $d(w1) = 2d(w)$ if and only if $|w| \in \{y^n_m : m \in \omega\}$, and $d(w1) = d(w)$ otherwise. In any case define $d(w0) = 2d(w) - d(w1)$, so that d is a martingale. Note that the sets $\{y^n_m : m \in \omega\}$ are computable uniformly in n: to test whether a number k is one of the numbers y^n_m we only have to perform the finite number of computations $\varphi_{f,k}(l)$, where $n = \langle e, f \rangle$ and $l \leq k$. So d is indeed computable. Also, $\mathcal{A} \subseteq S[d]$ because if $A_n \in \mathcal{A}$ then the set $\{y^n_m : m \in \omega\}$ is infinite. $\square$

3.3 Chaitins Ω

Let U be a universal prefix machine (see section 2.2). Chaitin defined the real

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

Note that the definition of Ω depends on the choice of U. We state some interesting facts about Ω.

- Note that $\Omega = \sum_{x\in\omega} Q_U(x)$, see section 2.5.
- From its definition it is immediate that Ω is a c.e. real. Furthermore, $0 < \Omega < 1$, because U halts on some, but not on every program.
- Ω is sometimes called "the number of wisdom", because it has the property that $\Omega\restriction n$ can compute whether $U(\sigma)\downarrow$ for all σ with $|\sigma| \leq n$. To see this, first note that

$$\Omega\restriction n \leq \Omega \leq \Omega\restriction n + 2^{-n}. \tag{6}$$

  Given σ of length $\leq n$, compute s such that $\Omega_s > \Omega\restriction n$. Then, if $U_s(\sigma)\uparrow$, U will not halt on σ at a stage later than s, because σ would contribute an extra amount of $2^{-|\sigma|} \geq 2^{-n}$ to Ω, which would contradict the upper bound (6).
- Ω is incompressible in the sense of Chaitin (Chaitin random, see Definition 3.1.4), hence Σ_1-random. To see this, let ϕ be a computable function such that for all n, $\phi(\Omega\restriction n) = x$, with $K(x) \geq n$. Such ϕ exists by the previous item: any x not among all the $U(\sigma)\downarrow$ with $|\sigma| < n$ will do. Then

$$K(\Omega\restriction n) \geq K(\phi(\Omega\restriction n)) - c \geq n - c$$

  for some constant c depending only on ϕ.
- By the previous items, Ω can be seen as a very compact version of the halting problem K. Its first 10,000 bits contain a solution to all interesting open problems in mathematics that can be formulated as an effective search problem, such as Goldbachs conjecture (every even $n > 2$ is the sum of two primes).
- However, to compute these solutions would take an unreasonable amount of time: To compute as above from $\Omega\restriction n$ which σ, $|\sigma| < n$, have $U(\sigma)\downarrow$, would take time $t(n)$, where t is a function growing faster than any computable function.

More on Ω-numbers in section 3.4.

3.4 Complexity of Σ_1-random sets

In this section we will say a few words on the complexity of Martin-Löf random sets. Recall that a set A is *low* if $A' \leq_T K \oplus A$, i.e. the jump of A is as low as possible. The Low Basis Theorem of Jockusch and Soare [41, Theorem V.5.32] says that every nonempty Π^0_1-class (i.e. a class that consists of the infinite branches of a computable tree) contains a low set. Now consider the first level $\mathcal{U}_0$ of the universal Martin-Löf test, see Theorem 3.2.1. The complement $\mathcal{P}_0$ of $\mathcal{U}_0$ is a nonempty Π^0_1-class consisting purely of Σ_1-random sets. Therefore, by the Low Basis Theorem we have that there is a low Σ_1-random set.[3] However, there are no Σ_1-random sets of low *c.e.* degree, by the following theorem.

Theorem 3.4.1 (Kučera [23, p249]) *Let A be c.e., $A <_T K$. Then ${}^{\leq_T}A$ has Σ_1-measure 0. Equivalently, A does not bound a Σ_1-random set.*

Recently Kučera and Slaman [24] characterized the Σ_1-random sets of c.e. degree exactly in terms of Solovay reducibility, see also Downey's survey paper [7]: A real is an Ω-*number* if it is equal to Chaitins Ω from section 3.3 for some choice of a universal prefix machine (see also section 2.2). Chaitin and Solovay both showed that Ω-numbers are random. By Theorem 3.4.1 these are all T-complete c.e. reals. A real A is Ω-*like* if it has a universal approximation, which is the same as saying that A is Solovay-complete for all c.e. reals. Any Ω-number is Ω-like (Solovay), and Calude, Hertling, Khoussainov, and Wang [4] proved that any Ω-like real is an Ω-number. Finally, Kučera and Slaman [24] showed that every Σ_1-random c.e. real is Ω-like, thus proving that the random c.e. reals are precisely the Solovay-complete ones.

We will come back to Theorem 3.4.1 in section 4.4.

3.5 Martingales and orders

Martingales are a convenient way of introducing various effective measures by varying the complexity of the martingales. This approach was first taken by Schnorr, and later applied with much success in complexity theory by Lutz.

Next we discuss Σ_1-martingales. Recall that a Σ_1-function is a function whose values are computably approximable from below.

[3] Nies [38] observed that the Low Basis Theorem actually gives a *super*low Σ_1-random set. A set A is superlow if $A' \leq_{tt} K$. That there are Σ_1-randoms *tt*-below K, but none that are *btt*-below K was observed in Terwijn [53].

It is often convenient to have all martingales be $\mathbb{Q}$-valued. Namely, by identifying $\mathbb{Q}$ with ω in an appropriate way, one can then directly speak about computability, without having to use approximations. However, for Σ_1-martingales d, if $d(\lambda) \in \mathbb{Q}$ then in particular $d(\lambda)$ is computable, but this implies that all of d is computable. So either one uses Σ_1-martingales with values in $\mathbb{R}$, or one relaxes the martingale property (1) to the *super*martingale property (2).

Schnorr proved the following effective version of Ville's Theorem 1.2.3:

Theorem 3.5.1 (Schnorr [46, Satz 5.3]) *$\mathcal{A} \subseteq 2^\omega$ is Martin-Löf null if and only if there is a Σ_1-supermartingale d such that $\mathcal{A} \subseteq S[d]$.*

Proof. This is a direct effectivization of the proof of Theorem 1.2.3. Note that d in the proof of Theorem 1.2.3 is a Σ_1-martingales if the $\mathcal{U}_k$ are uniformly c.e. Since in general d cannot be computable, by the discussion above this implies that $d(\lambda)$ cannot be a computable real. □

Now Σ_1-supermartingales are Σ_1 objects, so it comes as no surprise that we can effectively list all of them in an enumeration d_0, d_1, ... The sum $d = \sum_i 2^{-i} d_i$ is then again a Σ_1-supermartingale, and the success set $S[d]$ is the maximal Martin-Löf null set, so d is a *universal* Σ_1-supermartingale. (Alternatively, we could have used the existence of a universal Martin-Löf test, Theorem 3.2.1.)

We now give a characterization of the Schnorr null sets in terms of martingales.

Definition 3.5.2 (Schnorr [46]) An *order* is a nondecreasing unbounded function $h : \omega \to \omega$. (N.B. An "Ordnungsfunktion" in Schnorr's terminology is always computable, whereas we prefer to leave the complexity of orders unspecified in general.) For a martingale d and an order h we define

$$S_h[d] := \{X : \limsup_{n\to\infty} \frac{d(X{\upharpoonright}n)}{h(n)} \geq 1\}.$$

Schnorr pointed out that the rate of success of a Σ_1-martingale d can be so slow that it cannot be computably detected. Thus rather than working with Σ_1 null sets of the form $S[d]$ with $d \in \Sigma_1$, he worked with null sets of the form $S_h[d]$, where both d and h are computable. He showed that these null sets are the same as the Schnorr null sets from Definition 3.1.2. For the proof of this, we isolate the following lemma, which will also be useful later on when we discuss Hausdorff dimension.

Lemma 3.5.3 *Suppose that f is a computable order and that $\{\mathcal{U}_n\}_{n\in\omega}$ is a Martin-Löf test, where the $\mathcal{U}_n$ are defined by prefix-free sets $U_n \subseteq 2^{<\omega}$, such that*

$$\sum_{\sigma\in U_n} 2^{-|\sigma|}2^{f(|\sigma|)} \leq 2^{-n}.$$

Then there is a Σ_1-martingale d such that $\bigcap_n \mathcal{U}_n \subseteq S_{2^{f(n)}}[d]$. Furthermore, if $\{\mathcal{U}_n\}_{n\in\omega}$ is a Schnorr test then d is a computable martingale.

Proof. Define

$$d_k(\sigma) = \begin{cases} 2^{f(|\tau|)} & \text{if } \tau \sqsubset \sigma \text{ and } \tau \in U_k, \\ \displaystyle\sum_{\sigma\tau\in U_n} 2^{-|\tau|}2^{f(|\sigma\tau|)} & \text{otherwise.} \end{cases}$$

One can easily verify that d_k is a martingale. Note that the expression $\sum_{\sigma\tau\in U_n} 2^{-|\tau|}2^{f(|\sigma\tau|)}$ is like the $\mu(\mathcal{U}_k|\sigma)$ used in the proof of Theorem 1.2.3, except that now every $\sigma\tau \in U_k$ counts for $2^{-|\tau|+f(|\sigma\tau|)}$ rather than just $2^{-|\tau|}$. Again we define the sum martingale

$$d(\sigma) = \sum_{k=0}^{\infty} d_k(\sigma).$$

Note that $d_k(\lambda) = \sum_{\tau\in U_k} 2^{-|\tau|}2^{f(|\tau|)} \leq 2^{-k}$ by assumption, so $d(\lambda) \leq \sum_k 2^{-k}$ is finite, and hence by the martingale property all $d(\sigma)$ are finite. The computability claims on d are easily verified. (Note that, given σ, there can be only finitely many $\mathcal{U}_k$ σ can be in.) Finally, note that if $\sigma \in U_k$ then $d_k(\sigma) \geq 2^{f(|\sigma|)}$. So if $A \in \bigcap_{k\in\omega} \mathcal{U}_k$ then $A \in S_{2^{f(n)}}[d]$. □

Theorem 3.5.4 (Schnorr [46, Satz 9.4, 9.5]) *$\mathcal{A} \subseteq 2^\omega$ is Schnorr null if and only if there are computable d and h such that $\mathcal{A} \subseteq S_h[d]$.*

Proof. (Only if) Let $\{\mathcal{V}_n\}_{n\in\omega}$ be a Schnorr test. By Lemma 3.5.3 it suffices to show that there are a computable order f and a Schnorr test $\{\mathcal{U}_n\}_{n\in\omega}$ such that

$$\bigcap_n \mathcal{V}_n \subseteq \bigcap_n \mathcal{U}_n \text{ and } \sum_{\sigma\in U_n} 2^{-|\sigma|}2^{f(|\sigma|)} \leq 2^{-n}. \quad (7)$$

Let $V \subseteq 2^{<\omega}$ be prefix-free and computable such that $[V] = \bigcup_n \mathcal{V}_n$. ($V$ exists because $\{\mathcal{V}_n\}_{n\in\omega}$ is a Schnorr test.) Construct f computable order such that

$$\sum_{\sigma\in V,\, |\sigma|\geq n} 2^{-|\sigma|} \leq 2^{-2f(n)}.$$

Then

$$\begin{aligned}\sum_{\sigma\in V,\, f(|\sigma|)=m} 2^{-|\sigma|}2^{f(|\sigma|)} &\leq 2^m \sum_{\sigma\in V,\, f(|\sigma|)=m} 2^{-|\sigma|} \\ &\leq 2^m 2^{-2m} \\ &= 2^{-m},\end{aligned}$$

so $\sum_{\sigma\in V} 2^{-|\sigma|}2^{f(|\sigma|)} \leq \sum_m 2^{-m}$ is finite. Let g be computable such that

$$\sum_{\sigma\in V,\, |\sigma|\geq g(n)} 2^{-|\sigma|}2^{f(|\sigma|)} \leq 2^{-n},$$

and define $U_n = \big\{\sigma \in V : |\sigma| \geq g(n)\big\}$. Then the U_n define a Schnorr test $\mathcal{U}_n$ with the properties (7).

(If) Let the Σ^0_1-classes $\mathcal{U}_k$ be defined by the sets of strings

$$U_k = \big\{\sigma : |\sigma| \text{ minimal such that } d(\sigma) \geq h(|\sigma|) \wedge d(\sigma) \geq 2^k\big\}.$$

Then $\mu(\mathcal{U}_k) \leq 2^{-k}$ and $\mu(\mathcal{U}_k)$ is computable: To compute it to within precision 2^{-r}, compute n such that $h(n) \geq 2^r d(\lambda)$. Let $A_n = U_k - \{\sigma : |\sigma| > n\}$. Then $\sigma \in U_k - A_n \Longrightarrow d(\sigma) \geq h(|\sigma|) \geq h(n) \geq 2^r d(\lambda)$, so $\mu(U_k - A_n) \leq 2^{-r}$ by Ville's Lemma 1.2.2. □

3.6 A sufficient condition for computable randomness

The material in this section is taken from Terwijn [53]. For notational convenience, in this section we denote the initial segment of length n of an infinite sequence $x \in 2^\omega$ by x_n. We abbreviate the phrases 'infinitely often' and 'almost everywhere' by 'i.o.' and 'a.e.', respectively.

Ko [21] investigated the relations between polynomial time and space bounded versions of Martin-Löf randomness. His notion of pspace-randomness is obtained by defining a sequence to be non-pspace-random if it is covered by a pspace-computable Martin-Löf test *sufficiently fast*. The extra condition on the speed with which the set is covered is necessary, since otherwise the defined notion equals that of Martin-Löf. The following sufficient condition for pspace-randomness was proved by Ko.

Theorem 3.6.1 (K.-I. Ko [21]) *Let p be a polynomial. Let C^s denote the s-space bounded generating complexity. If for all polynomials q it holds that $C^q(x_n) > n - p(\log n)$ a.e. then x is pspace-random.*

We now turn our attention to computable randomness. The next lemma is analogous to [30, Claim 2.2, p122], with the time bounded Kolmogorov complexity instead of the plain Kolmogorov complexity.

Lemma 3.6.2 *For any infinite sequence $x \in 2^\omega$ the following are equivalent:*

(i) *For every computable function t there is a constant c such that $C^t(x_n) \geq n - c$ for infinitely many n.*

(ii) *For every computable function t there is a constant c such that $C^t(x_n|n) \geq n - c$ for infinitely many n.*

Proof. The implication from (ii) to (i) is trivial since always $C^t(x|n) \leq C^t(x)$. For the other implication note that

$$C^{2t}(x_n) \leq C^t(x_n|n) + 2 \cdot C^t(n - C^t(x_n|n)) + O(1).$$

For if we have a minimal program p that generates x_n given n, and a program q for $n - C^t(x_n|n)$, then we can reconstruct n from the length of p together with q. If p and q run both in time t then this new program takes time $2t + O(1)$.

Now fix any computable t. From (i) it follows that infinitely often $n - c \leq C^{2t}(x_n)$ for some constant c. For all the n for which this holds we then have

$$\begin{aligned} n - c &\leq C^t(x_n|n) + 2 \cdot C^t(n - C^t(x_n|n)) + O(1) \\ &\leq C^t(x_n|n) + 2 \cdot |n - C^t(x_n|n)| + O(1). \end{aligned}$$

Hence $n - C^t(x_n|n) \leq 2 \cdot |n - C^t(x_n|n)| + O(1)$, but this is only possible if $n - C^t(x_n|n)$ is bounded, i.e. for the infinitely many n such that the above inequalities hold we must have that $n - C^t(x_n|n) \leq c'$ for some constant c'. □

Proposition 3.6.3 *For any sequence $x \in 2^\omega$ and any superlinear computable time bound t it holds that $C^t(x_n) \leq n - \log n$ infinitely often.*

The unbounded version of Proposition 3.6.3 prevents a definition of randomness like: "An infinite sequence x is random if there is a constant c such that for all n it holds that $C(x_n) \geq n - c$." (This was discussed in section 2.)

Schnorr's characterization of Martin-Löf randomness (Theorem 3.2.5) was obtained by considering prefix-complexity instead of plain Kolmogorov complexity. We now give an 'infinitely often' criterion for computable randomness. Since we use 'i.o.' rather than 'a.e.' we have no need for prefix-complexity at this point.

Theorem 3.6.4 *Let x be an infinite sequence. If for every computable function t there is a constant c such that it holds that infinitely often $C^t(x_n) \geq n - c$ then x is computably random.*

Proof. We prove this by contraposition. Suppose that x is a sequence that is not computably random. By Lemma 3.6.2 it suffices to prove that there is a computable t such that for every constant c it holds that $C^t(x_n|n) \leq n - c$ a.e. First we prove that for every constant c there exists a computable function t such that $C^t(x_n|n) \leq n - c$ a.e. At the end of the proof we show that this proof can be made uniform. Fix c and let d be a computable martingale such that $x \in S[d]$ and $d(\lambda) = 1$. Without loss of generality we may assume that $d(x_n) \geq 2^c$ a.e. n. By Lemma 1.2.2 we have that

$$\mu(\{w \in 2^{<\omega} : w \text{ of minimal length such that } d(w) \geq 2^c\}) \leq 2^{-c}. \tag{8}$$

Let M be a machine that, given i and n, outputs the i-th initial segment w of length n with $d(w) \geq 2^c$, or outputs zero if such w does not exist. Let $t_c(i, n)$ be the number of computation steps in the computation $M(i, n)$. Fix n such that $d(x_n) \geq 2^c$. Let i be such that x_n is the i-th string w of length n with $d(w) \geq 2^c$. Note that by (8) there can be at most $2^{-c}/2^{-n}$ strings w of length n with $d(w) \geq 2^c$, so $i \leq 2^{n-c}$, and thus $|i| \leq n - c$. Therefore,

$$\begin{aligned} C^{t_c}(x_n|n) &\leq |i| + C(c) + C(d) + |M| \\ &\leq n - c + \log c + C(d) + |M| \end{aligned}$$

Here by $C(d)$ we mean the Kolmogorov complexity of a program for the computable martingale d. So for every c there is a computable function t_c such that $C^{t_c}(x_n|n) \leq n - (c - \log c - b)$ a.e., where $b = C(d) + |M|$. Hence, given a constant c' we can choose c so large that $c - \log c - b \geq c'$ to obtain $C^{t_c}(x_n|n) \leq n - (c - \log c - b) \leq n - c'$ a.e.

It is now easy to see that the above construction can be done *uniformly*, yielding a function t that works for all c. We simply set $t(i, n) = \max_{c \leq n} t_c(i, n)$ and note that this t majorizes every t_c. □

Lathrop and Lutz proved the following two results relating computable randomness and Kolmogorov complexity. The first result shows that computably random sequences have very high time-bounded Kolmogorov complexity, and the second result shows that this is no longer true in the absence of time bounds.

Theorem 3.6.5 (Lathrop and Lutz [28]) *Suppose that $x \in 2^\omega$ is computably random and that $t, g : \omega \to \omega$ are computable functions with g nondecreasing and unbounded. Then $K^t(x_n) > n - g(n)$ for infinitely many n.*

Call a sequence $x \in 2^\omega$ *ultracompressible* if for every nondecreasing unbounded computable function $g : \omega \to \omega$ it holds that $K(x_n) < K(n) + g(n)$ for almost every n.

Theorem 3.6.6 (Lathrop and Lutz [28]) *There exists a computably random sequence x that is ultracompressible.*

It would be interesting to find a precise characterization of the notion of computable randomness in terms of Kolmogorov complexity.

4 Hausdorff dimension

4.1 Classical Hausdorff dimension

First we repeat the definition of classical Hausdorff dimension [12]. For comments and discussion the reader can consult e.g. Falconer [11].

Definition 4.1.1

- $C \subseteq 2^{<\omega}$ is an *n-cover* if $\sigma \in C \to |\sigma| \geq n$.
- C *covers* $\mathcal{A} \subseteq 2^\omega$ if $\mathcal{A} \subseteq \bigcup_{\sigma \in C}[\sigma]$.
- Define $H_n^\varepsilon(\mathcal{A}) := \inf\Big\{\sum_{\sigma \in C} 2^{-\varepsilon|\sigma|} : C \text{ is } n\text{-cover of } \mathcal{A}\Big\}$.
- Define $H^\varepsilon(\mathcal{A}) := \lim_{n\to\infty} H_n^\varepsilon(\mathcal{A})$. This is the *$\varepsilon$-dimensional outer Hausdorff measure* of $\mathcal{A}$.

Lemma 4.1.2 *There exists $\varepsilon \in [0,1]$ such that*

- $\forall \varepsilon' > \varepsilon.\ H^{\varepsilon'}(\mathcal{A}) = 0,$
- $\forall\, 0 \leq \varepsilon' < \varepsilon.\ H^{\varepsilon'}(\mathcal{A}) = \infty.$

Proof. First note that for all n and $\delta > 0$,

$$\begin{aligned} H_n^{\varepsilon+\delta}(\mathcal{A}) &= \inf\Big\{\sum_{\sigma\in C} 2^{-\varepsilon|\sigma|}2^{-\delta|\sigma|} : C \text{ } n\text{-cover of } \mathcal{A}\Big\} \\ &\leq \inf\Big\{2^{-\delta n}\sum_{\sigma\in C} 2^{-\varepsilon|\sigma|} : C \text{ } n\text{-cover of } \mathcal{A}\Big\} \\ &= 2^{-\delta n} H_n^\varepsilon(\mathcal{A}). \end{aligned}$$

Now suppose that $H^\varepsilon(\mathcal{A}) < \infty$. Then $H_n^{\varepsilon+\delta}(\mathcal{A}) \leq \lim_{n\to\infty} 2^{-\delta n} H_n^\varepsilon(\mathcal{A}) = 0$. □

The ε from Lemma 4.1.2 is called the *Hausdorff dimension* of $\mathcal{A}$:

Definition 4.1.3

$$\dim(\mathcal{A}) := \inf\{\varepsilon : H^\varepsilon(\mathcal{A}) = 0\}$$

4.2 Effectivizations of Schnorr and Lutz

We now discuss effectivizations of Hausdorff dimension. Recall from section 3.5 the null sets of of the form $S_h[d]$. Schnorr also addressed null sets of the form $S_h[d]$ with $h(n) = 2^{\varepsilon n}$, $\varepsilon \in (0, 1]$, of *exponential* order. Although he did not make explicit reference to Hausdorff dimension, it turns out that the theory of Hausdorff dimension can be cast precisely in terms of such null sets of exponential order.

Lutz constructivized Hausdorff dimension in [33, 34], using what he called *s-gales* (a generalization of martingales). Let $s \in [0, \infty)$. An *s-gale* is a function $d : 2^{<\omega} \to \mathbb{R}^+$ that satisfies the averaging condition

$$2^s d(w) = d(w0) + d(w1) \tag{9}$$

for every $w \in 2^{<\omega}$. Similarly, d is an *s-supergale* if (9) holds with $\geq$ instead of equality. The success set $S[d]$ is defined exactly as was done for martingales in section 1.2.

Although Theorem 4.2.1 shows that we do not really need s-gales for the treatment of Hausdorff dimension, it will be convenient to use them at some points.

Theorem 4.2.1 *For any class $\mathcal{A}$ the following are equivalent:*

(i) *$\mathcal{A}$ has dimension α (as defined in Definition 4.1.3),*

(ii) $\alpha = \inf\big\{s \in \mathbb{Q} : \exists d$ *s-(super)gale* $\big(\mathcal{A} \subseteq S[d]\big)\big\}$.

(iii) $\alpha = \inf\{s \in \mathbb{Q} : \exists d$ *(super)martingale* $(\mathcal{A} \subseteq S_{2^{(1-s)n}}[d])\}$.

Proof. For the equivalence of (ii) and (iii), note that d' is an s-gale if and only if $d(w) = 2^{(1-s)|w|} d'(w)$ is a martingale. For $s' < s$ we have $2^{(1-s')n} > 2^{(1-s)n}$ so

$$S_{2^{(1-s')n}}[d] \subseteq S\Big[\frac{d}{2^{(1-s)n}}\Big] \subseteq S_{2^{(1-s)n}}[d]. \tag{10}$$

Now the equivalence of (ii) and (iii) is immediate.

The equivalence of (i) and (ii) is due to Lutz [33, Theorem 3.6]. This proof is similar to the proof of Theorem 3.5.4.

Note that the implication (i)$\Longrightarrow$(iii) follows from Lemma 3.5.3, with $f(n) = (1-s)n$. So we see that the theory of (effective) Hausdorff dimension falls out as a special case of Schnorr's treatment of effective measure theory. □

Theorem 4.2.1 motivates the following definition:

Definition 4.2.2 For a complexity class $\mathcal{C}$, $\mathcal{A}$ has $\mathcal{C}$*-dimension* α if

$$\alpha = \inf\{s \in \mathbb{Q} : \exists d \in \mathcal{C}\ (\ d \text{ supermartingale and } \mathcal{A} \subseteq S_{2^{(1-s)n}}[d]\ )\}.$$

4.3 Picture of implications

The relations between these notions are as follows:

$$\begin{array}{ccc}
\Delta_2\text{-random} & & \\
\Downarrow & & \\
\text{Schnorr } \Delta_2\text{-random} & \Longrightarrow & \Delta_2\text{-dimension } 1 \\
\Downarrow & & \Downarrow \\
\Sigma_1\text{-random} & \Longrightarrow & \Sigma_1\text{-dimension } 1 \\
\Downarrow & & \\
\text{computably random} & & \Downarrow \\
\Downarrow & & \\
\text{Schnorr random} & \Longrightarrow & \text{computable dimension } 1
\end{array}$$

No other implications hold than the ones indicated. The strictness of the implications was discussed in section 3.1. That there are no more implications between the first and the second column follows from the next proposition. The strictness of the two implications in the second column follows by similar means. (It is easy to see (cf. [34]) that COMP has Σ_1-dimension 0, but is not computably null, so in particular COMP has computable dimension 1. Also, Lutz [34] has shown that there are sets in Δ^0_2 of any Σ_1-dimension α, but it is elementary that every set in Δ^0_2 has Δ^0_2-dimension 0.)

Proposition 4.3.1 *There are sets A such that A is not Schnorr random and A has Δ_2-dimension 1.*

Proof. Let R be Δ_2-random, and let $D = \{2^x : x \in \omega\}$ be an exponentially sparse computable domain. Then $A = R \cup D$ is not Schnorr random, since no Schnorr random contains an infinite computable subset, and no Δ_2-martingale can succeed on A exponentially fast. □

Clearly, the "Δ_2-dimension 1" in Proposition 4.3.1 can be improved to "Δ_n-dimension 1" by the same proof, if one is considering higher orders of randomness.

4.4 Σ_1-Dimension

Write $\mu^\varepsilon(C) := \sum_{\sigma\in C} 2^{-\varepsilon|\sigma|}$. Note that since H_n^ε is monotone in n,

$$\begin{aligned} H^\varepsilon(\mathcal{A}) = 0 &\iff (\forall\delta > 0)(\forall n)(\exists C \ n\text{-cover })\big[\mu^\varepsilon(C) < \delta\big] \\ &\iff (\forall n)(\exists C \ n\text{-cover })\big[\mu^\varepsilon(C) < 2^{-n}\big] \\ &\iff (\forall n)(\exists C \text{ cover })\big[\mu^\varepsilon(C) < 2^{-n}\big]. \end{aligned}$$

Definition 4.4.1 Let $\varepsilon \in (0,\infty)$. An ε-*test* is a uniform sequence of Σ_1^0-classes $\{\mathcal{U}_n\}_{n\in\omega}$ such that for all n and every prefix-free $C \subseteq \mathcal{U}_n$ it holds that $\mu^\varepsilon(C) < 2^{-n}$.

An ε-test $\{\mathcal{U}_n\}$ with $\mathcal{A} \subseteq \bigcap_n \mathcal{U}_n$ shows that $H^\varepsilon(\mathcal{A}) = 0$ in an effective way.

Theorem 4.4.2 (Calude, Staiger, Terwijn) *For any class $\mathcal{A} \subseteq 2^\omega$ the following three statements are equivalent:*

(i) *α is minimal such that for all $\varepsilon > \alpha$ there is an ε-test $\{\mathcal{U}_n\}_{n\in\omega}$ such that $\mathcal{A} \subseteq \bigcap_n \mathcal{U}_n$.*

(ii) *Lutz's definition of constructive dimension [34]: $\alpha = \inf\{s \in \mathbb{Q} : \exists d \in \Sigma_1$ (d s-supergale and $\mathcal{A} \subseteq S[d]$)$\}$,*

(iii) *$\mathcal{A}$ has Σ_1-dimension α (as defined in Definition 4.2.2), i.e. $\alpha = \inf\{s \in \mathbb{Q} : \exists d \in \Sigma_1$ (d supermartingale and $\mathcal{A} \subseteq S_{2^{(1-s)n}}[d]$)$\}$,*

Proof. (i)$\Longrightarrow$(ii). Suppose $\{\mathcal{U}_n\}_{n\in\omega}$ is an ε-test. Let $\mathcal{U}_{n,t}$ be the computable approximation of $\mathcal{U}_n$ at stage t, and define

$$d_{n,t}(\sigma) := \max\big\{2^{(1-\varepsilon)|\sigma|}\mu^\varepsilon(C|\sigma) : C \subseteq \mathcal{U}_{n,t} \text{ prefix-free }\big\}.$$

Then one can easily check that for each n and t, $d_{n,t}$ is a martingale. Define

$$d_n(\sigma) := \lim_{t\to\infty} d_{n,t}(\sigma),$$

$$d(\sigma) := \sum_{n=0}^{\infty} d_n(\sigma).$$

Then $d(\sigma) < \infty$ for every σ since $d(\lambda) \le \sum_n d_n(\lambda) \le \sum_n 2^{-n}$ and d is a martingale. Note that d is Σ_1. Now if $\sigma \in \mathcal{U}_n$ then $d_n(\sigma) \ge 2^{(1-\varepsilon)|\sigma|}$, so if $A \in \bigcap_n \mathcal{U}_n$ then $A \in S_{2^{(1-\varepsilon)n}}[d]$.

(ii)$\Longrightarrow$(i). Suppose d is a Σ_1-(super)martingale. Fix ε_0. For every $\varepsilon > \varepsilon_0$ we define an ε-test $\{\mathcal{U}_n\}$ such that $\bigcap_n \mathcal{U}_n \supseteq S_{2^{(1-\varepsilon_0)n}}[d]$

Fix $k \geq d(\lambda)$. Define

$$\mathcal{U}_n := \{\sigma : d(\sigma) \geq 2^{(1-\varepsilon)|\sigma|} 2^n k\}.$$

Note that if $A \in S_{2^{(1-\varepsilon_0)n}}[d]$ then for all $\varepsilon > \varepsilon_0$ we have $\limsup_{n\to\infty} \frac{d(A\restriction n)}{2^{(1-\varepsilon)n}} = \infty$, so $A \in \bigcap_n \mathcal{U}_n$. We claim that the $\mathcal{U}_n$ form an ε-test. Namely, let $C \subseteq \mathcal{U}_n$ be prefix-free. Then by Lemma 1.2.2 we have

$$\begin{aligned} 2^n k \cdot \mu^\varepsilon(C) = 2^n k \sum_{\sigma\in C} 2^{-\varepsilon|\sigma|} &\leq \sum_{\sigma\in C} 2^{-\varepsilon|\sigma|} \frac{d(\sigma)}{2^{(1-\varepsilon)|\sigma|}} \\ &\leq \sum_{\sigma\in C} 2^{-|\sigma|} d(\sigma) \leq d(\lambda) \leq k, \end{aligned}$$

so $\mu^\varepsilon(C) \leq 2^{-n}$.

For the equivalence of item (ii) and (iii) see Theorem 4.2.1. □

We now give an explicit construction of a universal ε-test $\{\mathcal{U}_n^\varepsilon\}_{n\in\omega}$ for the sets of Σ_1-dimension less or equal to ε. The definition is a straightforward modification of Martin-Löfs universal Σ_1 null set, Theorem 3.2.1. That a universal ε-test exists follows implicitly also from the analyses of Schnorr [46] and Lutz [34], but below it will be convenient to have the explicit formulation presented here.

Theorem 4.4.3 *For every $\varepsilon \in \mathbb{Q}$ there exists a universal ε-test. That is, there is a computable sequence of Σ_1^0 classes $\mathcal{U}_0^\varepsilon, \mathcal{U}_1^\varepsilon, \ldots$ such that*

- $\mathcal{U}_0^\varepsilon \supseteq \mathcal{U}_1^\varepsilon \supseteq \ldots$
- *for every n and every prefix-free $C \subseteq \mathcal{U}_n^\varepsilon$ it holds that $\mu^\varepsilon(C) < 2^{-n}$*
- *for any class $\mathcal{A}$ of Σ_1-dimension $\leq \varepsilon$ we have $\mathcal{A} \subseteq \bigcap_n \mathcal{U}_n^\varepsilon$.*

Proof. This is very similar to the proof of Theorem 3.2.1. For every n construct a Σ_1^0-class $\mathcal{U}_n^\varepsilon$ as follows. For every $e > n$, $\mathcal{U}_n^\varepsilon$ enumerates all the elements of $W_{\{e\}(e)}$ (where we take this set to be empty if $\{e\}(e)$ is undefined) as long as for every prefix-free $C \subseteq W_{\{e\}(e)}$ it holds that $\mu^\varepsilon(C) < 2^{-e}$. Then if $C \subseteq \mathcal{U}_n^\varepsilon$ is prefix-free we have $\mu^\varepsilon(C) < \sum_{e>n} 2^{-e} = 2^{-n}$, and if $\{e\}$ defines an ε-test then for every n there exists by padding $i \in \omega$ (in fact, infinitely many i) such that $W_{\{e\}(i)} \subseteq \mathcal{U}_n^\varepsilon$ (if $i > n$ is an alternative code for e then $W_{\{e\}(i)} = W_{\{i\}(i)} \subseteq \mathcal{U}_n^\varepsilon$), so $\bigcap_i W_{\{e\}(i)} \subseteq \bigcap_n \mathcal{U}_n^\varepsilon$. □

The following analogue of Theorem 3.2.3 can also be proven, with a similar proof:

Theorem 4.4.4 *For every A of Σ_1-dimension $> \varepsilon$ there exists $k \in \omega$ such that $T^k(A) \in \mathcal{P}_0^\varepsilon$.*

Now we come back to Theorem 3.4.1 that stated that for an c.e. Turing-incomplete set A, ${}^{\leq_T}A$ has Σ_1-measure 0.

The idea of the proof of Theorem 3.4.1 is the following. First, any Σ_1-random set is effectively bi-immune. Second, with any effectively immune set one can compute a fixed point free function (FPF for short, f is FPF if for all x, $W_x \neq W_{f(x)}$). The Arslanov completeness criterion (see e.g. [41]) says that a c.e. set is Turing complete if and only if it can compute a FPF function. So if the c.e. set A bounds a Σ_1-random set it follows that A is Turing complete.

We now want to strengthen Theorem 3.4.1 from Σ_1-measure 0 to Σ_1-dimension 0. Note that this is stronger since there are sets A such that $\{A\}$ has Σ_1-dimension 1 but Σ_1-measure 0.[4]

Lemma 4.4.5 *Suppose A has Σ_1-dimension > 0. Then A can compute a fixed point free function.*

Proof. For any e let e_0 and e_1 denote codes (defined in some canonical way from e) such that $W_e = W_{e_0} \oplus W_{e_1}$.

Fix $\varepsilon \in (0,1)$. Let $f(n) = n/\varepsilon$. Define

$$\mathcal{B}_{e,n} = \big\{\ \sigma : |\sigma| = f(n) \wedge\ (\exists s)\big[W_{e_0,s}{\restriction}f(n) = \sigma \wedge W_{e_1,s}{\restriction}f(n) = \overline{\sigma}\ \big]\big\}$$

Here $\overline{\sigma}$ denotes the complement of σ. That is, $\mathcal{B}_{e,n}$ contains all long strings σ (of length $f(n)$) for which the c.e. set W_e provides its $f(n)$ bits. That is, there can be at most one σ in $\mathcal{B}_{e,n}$. $\mathcal{B}_{e,n}$ is an n cover since $|\sigma| = f(n) \geq n$, and

$$\mu^\varepsilon(\mathcal{B}_{e,n}) = \sum_{\sigma \in \mathcal{B}_{e,n}} 2^{-\varepsilon|\sigma|} \leq 2^{-\varepsilon f(n)} = 2^{-n}, \tag{11}$$

so $\mathcal{B}_{e,n}$ is an ε-test. Suppose now that A has Σ_1-dimension $> \varepsilon$. Then by Theorem 4.4.3 there is a k such that $A \notin \mathcal{U}_k^\varepsilon$. For every e we can effectively find $g(e) > k$ such that $\varphi_{g(e)}(j)$ is a code of $\mathcal{B}_{e,j}$ for every j. By (11) the sets $\mathcal{B}_{e,j}$ form an ε-test and by the definition of $\mathcal{U}_n^\varepsilon$ in the proof of Theorem 4.4.3 we have $\mathcal{B}_{e,g(e)} \subseteq W_{\{(g(e)\}(g(e))} \subseteq \mathcal{U}_{g(e)}^\varepsilon \subseteq \mathcal{U}_k^\varepsilon$, so $A \notin \mathcal{B}_{e,g(e)}$.

[4]This can be proved by a direct construction, but it also follows from the fact that the class of reals of dimension 1 is properly Π_3^0 in the arithmetical hierarchy of reals (Theorem 5.2.3), whereas the class of Σ_1-random reals is Σ_2^0 (Theorem 5.1.3). Since the latter is included in the former, they cannot be equal.

Now we use this to construct a fixed point free function $h \leq_T A$: Given e, let $h(e)$ be a code such that $W_{h(e)_0} = A\restriction f(g(e))$ and $W_{h(e)_1} = \overline{A}\restriction f(g(e))$. Then $W_{h(e)} \neq W_e$ for every e, for if $W_{h(e)} = W_e$ then $A\restriction f(g(e)) \in \mathcal{B}_{e,g(e)}$. $\square$

Theorem 4.4.6 *Let A be c.e., $A <_T K$. Then ${}^{\leq_T}A$ has Σ_1-dimension 0.*

Proof. Suppose ${}^{\leq_T}A$ does not have Σ_1-dimension 0. Then by Theorem 4.4.3 there exists $B \leq_T A$ such that $\{B\}$ does not have Σ_1-dimension 0. By Lemma 4.4.5 B can compute a fixed point free function, so by Arslanov's completeness criterion A is Turing complete. $\square$

Since by the low basis theorem there are low Σ_1-random sets, and since there exist high incomplete c.e. sets, we now have both examples of low sets for which ${}^{\leq_T}A$ has Σ_1-dimension 1, and of high sets for which ${}^{\leq_T}A$ has Σ_1-dimension 0. The same examples show that there are low sets for which $\dim_{\Sigma_1}({}^{\leq_m}A)$ is maximal and high sets for which $\dim_{\Sigma_1}({}^{\leq_m}A)$ is minimal.

4.5 Relation with Kolmogorov complexity

In this section we prove a relation between Σ_1-dimension and the prefix-free Kolmogorov complexity. Similar results relating Kolmogorov complexity and *classical* Hausdorff dimension were proven by Cai and Hartmanis, Levin, Ryabko, and Staiger. See Lutz [34] for a discussion of these results.

We use the following lemma for s-gales, the proof of which is completely analogous to the one of Lemma 1.2.1.

Lemma 4.5.1 (Lutz [34]) *Let d be an s-(super)gale. For any string σ and any prefix-free set $X \subseteq \{\tau : \sigma \sqsubseteq \tau\}$ it holds that*

$$2^{-s|\sigma|}d(\sigma) \geq \sum_{\tau \in X} 2^{-s|\tau|}d(\tau).$$

Theorem 4.5.2 (Levin [60], Lutz [34], Mayordomo [36], Staiger [52]) *For any $A \in 2^\omega$,*

$$\dim_{\Sigma_1}(A) = \liminf_{n\to\infty} \frac{K(A\restriction n)}{n}.$$

Proof. ($\geq$) This direction was first proved by Lutz. Let $\alpha = \dim_{\Sigma_1}(A)$. Clearly if $\alpha = 1$ then the statement is true, so assume that $\alpha < 1$. Fix $\alpha < s < t < 1$, $s, t \in \mathbb{Q}$. By Theorem 4.4.2 there is an s-gale d such that $A \in S[d]$. Fix a rational $r \geq d(\lambda)$. Let

$$B = \{\sigma : d(\sigma) > r\},$$

and denote by B_n be the strings of length n in B. B_n is prefix-free, so by Lemma 4.5.1

$$d(\lambda) \geq \sum_{\sigma \in B_n} d(\sigma) 2^{-sn} \geq d(\lambda)|B_n| 2^{-sn},$$

hence $|B_n| \leq 2^{-sn}$. Since B_n is c.e. we have for every $\sigma \in B_n$,

$$K(\sigma) \leq sn + K(n) + O(1). \tag{12}$$

Since $t > s$ there is n_0 such that for all $n \geq n_0$,

$$K(n) \leq (t-s)n + O(1) \tag{13}$$

(Recall the bound $K(n) \leq 2\log n$ from section 2.2.) Because $A \in S[d]$ we have $A{\restriction}n \in B_n$ for infinitely many n. For these n, (12) and (13) together give

$$K(A{\restriction}n) \leq tn,$$

and hence $\liminf_{n\to\infty} \frac{K(A\restriction n)}{n} \leq t \leq \alpha$.

($\leq$) This direction was proved in Mayordomo [36]. As Staiger pointed out in [52], the result already quickly follows from results in [60] and [34].

Let $t > s > \liminf_{n\to\infty} \frac{K(A\restriction n)}{n}$ be rationals. Define

$$B = \{\sigma : K(\sigma) \leq s|\sigma|\},$$

and let B_n be the strings of length n in B. Then $|B_n| \leq 2^{sn-K(n)+c}$ for some constant c by a version of the Counting Theorem 2.6.3.

Define $d : 2^{<\omega} \to \mathbb{R}^+$ by

$$d(\sigma) = 2^{(t-s)|\sigma|}\Big(\sum_{\sigma\tau \in B} 2^{-s|\tau|} + \sum_{\rho \in B, \rho \subsetneq \sigma} 2^{(s-1)(|\sigma|-|\rho|)}\Big).$$

(Compare this definition of d to the proof of Lemma 3.5.3.) Then d is a Σ_1-t-gale: First, d is Σ_1 function because B is c.e. Second, $d(\lambda)$ is finite: $d(\lambda) = \sum_{\sigma\tau\in B} 2^{-s|\tau|} \leq \sum_n |B_n| 2^{-sn} \leq \sum_n 2^{-K(n)+c} \leq 2^c$. Finally, one can check (by a tedious checking of cases) that d has the t-gale property.

Now if $\sigma \in B$ then $d(\sigma) \geq 2^{(t-s)|\sigma|}$. Because $s > \liminf_{n\to\infty} \frac{K(A\restriction n)}{n}$ there are infinitely many n with $A{\restriction}n \in B$, hence $A \in S[d]$ and $\dim_{\Sigma_1}(A) \leq t$. The result follows since t was arbitrary. □

5 The complexity of randomness and dimension

The material in this section in based on Hitchcock, Lutz, and Terwijn [13].

5.1 Category Methods

Recall that a class $\mathcal{C}$ is *meager* if it is included in a countable union of nowhere dense subsets of 2^ω, and *comeager* if its complement $\overline{\mathcal{C}}$ is meager. The following lemma (implicit in Rogers [44, p 341]) will be useful:

Lemma 5.1.1 *If $\mathcal{C} \in \Sigma^0_2$ and $\overline{\mathcal{C}}$ is dense then $\mathcal{C}$ is meager.*

Proof. Suppose that $\mathcal{C} = \bigcup_n \mathcal{X}_n$, $\mathcal{X}_n$ closed. Since $\overline{\mathcal{C}}$ is dense, $\mathcal{X}_n$ contains no basic open set, hence $\mathcal{X}_n$ is nondense (i.e. its closure contains no basic open set), and $\mathcal{C}$ is a countable union of nondense sets. □

As a warm-up we give a short proof of Shoenfields result that COMP is not a Π^0_3-class.

Theorem 5.1.2 (Shoenfield [44, p344]) COMP *is a Σ^0_3-class, but not a Π^0_3-class.*

Proof. Clearly COMP $\in \Sigma^0_3$. Suppose for a contradiction that $\overline{\text{COMP}}$ is Σ^0_3. Then there is a uniform sequence of Σ^0_1-classes $\mathcal{O}_{n,m}$ such that $\overline{\text{COMP}} = \bigcup_n \bigcap_m \mathcal{O}_{n,m}$. Without loss of generality $\mathcal{O}_{n,m} \supseteq \mathcal{O}_{n,m+1}$ for all n,m. Now COMP is meager because it is countable, so $\overline{\text{COMP}}$ is comeager, so there is an n such that $\bigcap_m \mathcal{O}_{n,m}$ is not nowhere dense, hence dense in some interval $[\sigma]$. Then every $\mathcal{O}_{n,m}$, $m \in \omega$, is dense in $[\sigma]$. Now it is easy to construct a computable set (starting with σ) in $\bigcap_m \mathcal{O}_{n,m}$, contradicting that $\bigcap_m \mathcal{O}_{n,m} \subseteq \overline{\text{COMP}}$. □

The class $\mathcal{R}$ of Σ_1-random sets can also easily be classified with category methods:

Theorem 5.1.3 (folk) *The class of Σ_1-random sets $\mathcal{R}$ is a Σ^0_2-class, but not a Π^0_2-class.*

Proof. Analogous to the proof in Rogers [44, p 341] that $\{X : X \text{ finite}\}$ is a Σ^0_2-class but not a Π^0_2-class: Both $\mathcal{R}$ and its complement are dense, so by Lemma 5.1.1, $\mathcal{R}$ is meager. If $\mathcal{R}$ were a Π^0_2-class, its complement would also be meager, contradicting that 2^ω is not meager. □

5.2 Classification of the sets of dimension α

$\mathbf{\Sigma}^0_1$ and $\mathbf{\Pi}^0_1$ denote the levels of the classical Borel hierarchy. Recall that a class $\mathcal{A}$ Wadge reduces to a class $\mathcal{B}$ if there is a continues function $f : 2^\omega \to 2^\omega$ such that $X \in \mathcal{A} \Leftrightarrow f(X) \in \mathcal{B}$.

For every $k > 0$ define the computable order $h_k(n) = 2^{\frac{1}{k}n}$. Let d be a universal Σ_1-supermartingale (see section 3.5). By Lutz [34] $d^{(s)}(w) = 2^{(s-1)|w|}d(w)$ is a universal Σ_1-s-supergale. Hence

$$\bigcup_{s\in\mathbb{Q}^{<1}} S[d^{(s)}] = \bigcup_{s\in\mathbb{Q}^{<1}} S_{2^{(1-s)n}}[d] = \bigcup_{k>0} S_{h_k}[d]. \tag{14}$$

The first equality uses that $S_{h_k}[d] \subseteq S[d/h_{k+1}]$.

Lemma 5.2.1 *Every $S_{h_k}[d]$ is a comeager Π^0_2-class.*

Proof. $\overline{S_{h_k}[d]} \in \Sigma^0_2$ and $S_{h_k}[d]$ is dense. Now apply Lemma 5.1.1. □

Lutz [33, 34] defines the sets of constructive dimension 1 as

$$\mathrm{DIM}^1 = \{X \in 2^\omega : \text{no } \Sigma_1\text{-}s\text{-supergale}, s \in \mathbb{R}^{<1}, \text{ succeeds on } X\}.$$

Note that for $s' > s$ every s-gale is an s'-gale, so if $X \in$ co-DIM^1 there is always some s'-gale that succeeds on X with $s' \in \mathbb{Q}^{<1}$. Hence in classifying DIM^1 we can confine our attention to s-gales with $s \in \mathbb{Q}$. By (14) we have co-DIM$^1 = \{X : \exists s \in \mathbb{Q}^{<1}(X \in S[d^{(s)}])\} = \bigcup_{k>0} S_{h_k}[d]$. So by Lemma 5.2.1, DIM^1 is meager (it is contained in the meager set $\overline{S_{h_k}[d]}$) and co-DIM^1 is comeager. Since every $S_{h_k}[d]$ is a Π^0_2-class we have that co-DIM^1 is a Σ^0_3-class, and hence:

Proposition 5.2.2 DIM^1 *is a meager Π^0_3-class.*

A simple category argument shows that DIM^1 is not a Π^0_2-class: Otherwise co-DIM^1 would be Σ^0_2, and by Lemma 5.1.1 we would have that co-DIM^1 were meager, contradicting Lemma 5.2.1. We now prove that DIM^1 is $\mathbf{\Pi}^0_3$-complete under Wadge reducibility. In particular, DIM^1 is not a Σ^0_3-class.

Theorem 5.2.3 DIM^1 *is not a Σ^0_3-class. Hence it is properly Π^0_3.*

Proof. One could prove this by reducing a known $\mathbf{\Pi}^0_3$-complete class to DIM^1, e.g. the class of sets that have a limiting frequency of 1's that is 0 (this class was proved to be $\mathbf{\Pi}^0_3$-complete by Ki and Linton [20]), but is just as easy to build a direct reduction from an arbitrary $\mathbf{\Pi}^0_3$-class.

Let d be the universal constructive supermartingale. Note that we have

$$S_{2^n}[d] \subsetneq \ldots \subsetneq S_{2^{\frac{1}{k}n}}[d] \subsetneq S_{2^{\frac{1}{k+1}n}}[d] \subsetneq \ldots \subsetneq \mathrm{DIM}^1.$$

Let $\bigcup_k \bigcap_s \mathcal{O}_{k,s}$ be a $\mathbf{\Sigma}^0_3$-class. Without loss of generality $\mathcal{O}_{k,s} \supseteq \mathcal{O}_{k,s+1}$ for all k,s. We define a continuous function $f : 2^\omega \to 2^\omega$ such that

$$\forall k \left(X \in \bigcap_s \mathcal{O}_{k,s} \Longleftrightarrow f(X) \in S_{2^{\frac{1}{k}n}}[d] \right) \tag{15}$$

so that we have

$$\begin{aligned} X \notin \bigcup_k \bigcap_s \mathcal{O}_{k,s} \quad &\Longleftrightarrow \quad \forall k \left(f(X) \notin S_{2^{\frac{1}{k}n}}[d] \right) \\ &\Longleftrightarrow \quad f(X) \in \mathrm{DIM}^1. \end{aligned}$$

The image $Y = f(X)$ is defined in stages, $Y = \bigcup_s Y_s$, such that every initial segment of X defines an initial segment of Y.

At stage 0 we define Y_0 to be the empty sequence.

At stage $s > 0$ we consider $X{\restriction}s$, and for each k we define $t_{k,s}$ to be the largest stage $t \leq s$ such that $X{\restriction}s \in \mathcal{O}_{k,t}$. (Let $t_{k,s} = 0$ if such a t does not exist.) Define k to be *expansionary* at stage s if $t_{k,s-1} < t_{k,s}$. Now we let $k(s) = \min\{k : k \text{ is expansionary at } s\}$. There are two substages.

Substage (a). First consider all strings σ extending Y_{s-1} of minimal length with $d(\sigma) \geq 2^{\frac{1}{k(s)}|\sigma|}$, and take the leftmost one of these σ's. Such σ's exist because $S_{2^{\frac{1}{k(s)}n}}[d]$ is dense. If $k(s)$ does not exist let $\sigma = Y_{s-1}$.

Substage (b). Next consider all extensions $\tau \sqsupseteq \sigma$ of minimal length such that $d(\tau{\restriction}i) \leq d(\tau{\restriction}(i-1))$ for every $|\sigma| < i < |\tau|$, and $d(\tau) \leq |\tau|$. Clearly such τ exist, by direct diagonalization against d. Define Y_s to be the leftmost of these τ. This concludes the construction.

So Y_s is defined by first building a piece of evidence σ that d achieves growth rate $2^{\frac{1}{k(s)}n}$ on Y and then slowing down the growth rate of d to the order n. Note that f is continuous. If $X \in \bigcup_k \bigcap_s \mathcal{O}_{k,s}$, then for the minimal k such that $X \in \bigcap_s \mathcal{O}_{k,s}$, infinitely many pieces of evidence σ witness that d achieves growth rate $2^{\frac{1}{k}n}$ on Y, so $Y \notin \mathrm{DIM}^1$. On the other hand, if $X \notin \bigcup_k \bigcap_s \mathcal{O}_{k,s}$ then for every k only finitely often $d(Y_s) \geq 2^{\frac{1}{k}|Y_s|}$

because in substage (a) the extension σ is chosen to be of minimal length, so $Y \notin S_{h_k}[d]$. Hence $Y \in \mathrm{DIM}^1$. □

From Theorem 5.1.3 and Theorem 5.2.3 the following result follows, which can also be proved by a direct construction:

Corollary 5.2.4 (Lutz [34]) *$\mathcal{R}$ is a proper subset of* DIM^1.

One can check that for computable real α with $0 < \alpha < 1$, the above results also hold for DIM^α (the sets of Σ_1-dimension α): DIM^α is a proper Π^0_3-class. This requires only slight changes to the proof of Theorem 5.2.3. Since $\mathrm{DIM}^{\geq\alpha}$ (the sets of Σ_1-dimension $\geq \alpha$) is in Π^0_3, follows that it is also properly Π^0_3, and hence that $\mathrm{DIM}^{<\alpha} = 2^\omega - \mathrm{DIM}^{\geq\alpha}$ is properly Σ^0_3. Other classifications of dimension classes can be found in [13].

5.3 The complexity of classes of random sets

Recall definitions of Schnorr randomness and computable randomness from section 3.1. We denote the class of Schnorr random sets by $\mathcal{S}$.

Theorem 5.3.1 *The class of Schnorr random sets $\mathcal{S}$ is properly Π^0_3.*

Proof. First note that $\mathcal{S} \in \Pi^0_3$: $A \in \mathcal{S}$ if and only if for every pair of codes e and f, either the e-th partial computable function φ_e is not a computable order (i.e. is not total or decreases at some point), or φ_f is not a computable martingale (i.e. is not total or violates the martingale property at some point), or $A \notin S_{\varphi_e}[\varphi_f]$, and that every one of these options is Σ^0_2.

The rest of the proof resembles that of Theorem 5.2.3. Fix a (noncomputable) sequence of computable martingales $\{d_k\}_{k\in\omega}$ and a sequence of computable orders $\{h_k\}_{k\in\omega}$ such that

(i) $A \in \mathcal{S} \Longleftrightarrow \forall k(A \notin S_{h_k}[d_k])$.

(ii) $S_{h_k}[d_k] - S_{\min\{h_j:j<k\}}[\sum_{j<k} d_j]$ is dense for every k.

The d_k can be defined by taking appropriate sums of computable martingales, such that every $S[d]$, d computable, is included in some $S[d_k]$, and for the h_k one can take any family of computable orders such that every computable order h dominates some h_k. (Of course the d_k and h_k cannot be uniformly computable families, but that is of no concern to us.)

Let $\bigcup_k \bigcap_s \mathcal{O}_{k,s}$ be a $\mathbf{\Sigma}^0_3$-class. We define a continuous function $f : 2^\omega \to 2^\omega$ such that

$$\forall k \left(X \in \bigcap_s \mathcal{O}_{k,s} \Longleftrightarrow f(X) \in S_{h_k}[d_k] \right) \tag{16}$$

so that by (i) we have $X \notin \bigcup_k \bigcap_s \mathcal{O}_{k,s} \Longleftrightarrow f(X) \in \mathcal{S}$, and $\mathcal{S}$ is $\mathbf{\Pi}^0_3$-complete.

As in the proof of Theorem 5.2.3 we define the image $Y = f(X)$ in stages. Every time we find a new piece of evidence that $X \in \bigcap_s \mathcal{O}_{k,s}$, at stage s say, we build a piece of evidence that $Y \in S_{h_k}[d_k]$ by choosing an appropriate finite extension at stage s. Such an extension can be found by (ii). The rest of the proof is identical to that of Theorem 5.2.3. □

With only some obvious changes one can prove

Theorem 5.3.2 *The class of computably random sets is properly* Π^0_3.

Proof. Note that X is computably random if and only if for every e, φ_e is not a computable martingale or $X \notin S[\varphi_e]$, so the class is Π^0_3. That it is properly Π^0_3 is actually easier than the proof of Theorem 5.3.1 since we only need the sequence $\{d_k\}$ and not the $\{h_k\}$. □

5.4 An extension of the effective Borel hierarchy

The complexity of DIM^α, the Schnorr random sets $\mathcal{S}$, and the computably random sets in the effective hierarchy corresponds exactly with their complexity in the Borel hierarchy, which is why we were able to use (noncomputable) continuous reductions to classify them. For COMP, the class of computable sets, this is not the case, since $\mathrm{COMP} \in \Sigma^0_3 \cap \mathbf{\Sigma}^0_2$, but COMP could be classified using category methods. (The Σ_1-random sets can be classified with both methods.) For some classes, however, we need other methods to classify them. An example of this, namely the class of 1-generic sets, is given below. Other examples can be found in [13]. As it turns out, we need a slight extension of the effective hierarchy to classify a number of natural randomness and dimension classes. We first give this extended definition.

Let $\mathcal{C}$ be a class of predicates. The ordinary definitions of Σ^0_n and Π^0_n use computable predicates. If instead predicates from $\mathcal{C}$ are used, we denote them by $\Sigma^0_n\mathcal{C}]$ and $\Pi^0_n[\mathcal{C}]$.

Definition 5.4.1 • $\mathcal{A} \in \Sigma^0_1[\mathcal{C}]$ if there is $P \in \mathcal{C}$ such that

$$A \in \mathcal{A} \Longleftrightarrow (\exists \sigma \sqsubset A)[\,\sigma \in P\,].$$

- $\mathcal{A} \in \Pi^0_1[\mathcal{C}]$ if $\overline{\mathcal{A}} \in \Sigma^0_1[\neg\mathcal{C}]$, where $P \in \neg\mathcal{C}$ if and only if $\overline{P} \in \mathcal{C}$.
- In general, for $n > 1$, $\mathcal{A} \in \Sigma^0_n[\mathcal{C}]$ if $\mathcal{A}$ is a $\mathcal{C}$-effective union of $\Pi^0_{n-1}[\mathcal{C}]$ classes, i.e. if there is a $\Pi^0_{n-1}[\mathcal{C}]$-class $\mathcal{B} \subseteq 2^\omega \times \omega$ such that $\mathcal{A} = \bigcup_{n\in\omega} \big\{X : (X,n) \in \mathcal{B}\big\}$.
- $\mathcal{A} \in \Pi^0_n[\mathcal{C}]$ if $\overline{\mathcal{A}} \in \Sigma^0_n[\neg\mathcal{C}]$.

Below we will be interested in the case where $\mathcal{C}$ is either Σ^0_1 or Π^0_1. We make the following basic observations:

- For every n we have

$$\Sigma^0_n \subseteq \Sigma^0_n[\Sigma^0_1] \subseteq \Sigma^0_{n+1}, \tag{17}$$

$$\Pi^0_n \subseteq \Pi^0_n[\Pi^0_1] \subseteq \Pi^0_{n+1}. \tag{18}$$

- If n is odd we have $\Sigma^0_n[\Sigma^0_1] = \Sigma^0_n$ and $\Pi^0_n[\Pi^0_1] = \Pi^0_n$.
- If n is even, the inclusions from (17) and (18) are strict, as we will prove in Proposition 5.4.2 below.
- Adding more than one quantifier does not make sense: e.g. $\Pi^0_3[\Sigma^0_3] = \Pi^0_3[\Sigma^0_1]$.

Proposition 5.4.2 *The inclusions from (17) and (18) are strict.*

Here's an example: The class of 1-generic sets. Recall that X is 1-generic if

$$(\forall e)(\exists \sigma \sqsubset X)\big[\,\{e\}^\sigma(e)\downarrow\ \vee\ (\forall \tau \sqsupset \sigma)[\{e\}^\tau(e)\uparrow]\,\big]$$

From this definition it is immediate that 1-generic is in $\Pi^0_2[\Pi^0_1]$, and that it is in $\boldsymbol{\Pi}^0_2$. Below we show that it is not Π^0_2. So this is an example where our one-extra-quantifier hierarchy makes sense.

Note that using computable continuous reductions does not help in classifying 1-generic: Suppose that $X \in 2^\omega$ iff $f(X)$ is 1-generic, for some computable f. Note that if X is computable then also $f(X)$ is. But this is impossible, because there are no computable 1-generics. So we see that an "easy" class like 2^ω does not Wadge reduce via a computable reduction to a "difficult" class like the 1-generic sets.

Also note that we may use category theory to conclude that the class of 1-generic sets is not Σ^0_2, by Lemma 5.1.1.

Now we show, using an ad-hoc argument, since there seems not to be any systematic way of doing it, that 1-generic is not Π^0_2. Suppose it is, X 1-generic iff $(\forall n)(\exists m)\big[R^X(n,m)\big]$, R computable predicate that uses X as an oracle. Since the 1-generic sets are dense, also $\big\{X : (\forall n)(\exists m)\big[R^X(n,m)\big]\big\}$ is dense. But then we can easily construct a computable element of it, using a computable finite extension argument. (Given σ and n, search for extension such that $R^\sigma(n,m)$ for some m. Such extension will be found by density. If extension is found, take it. Proceed to $n+1$.)

In conclusion, we see that the class of 1-generic sets is in $\Pi^0_2[\Pi^0_1] \cap \mathbf{\Pi}^0_2 \setminus (\Sigma^0_2 \cup \Pi^0_2)$.

6 Relativized randomness and lowness properties

In this section we briefly discuss relativized randomness and lowness properties for classes of random sets.

In computability theory a set A is called *low* if for A', the halting problem relativized to A, it holds that $A' \leq_T \emptyset'$, that is, if the complexity of the halting problem does not increase when relativized to A. In complexity theory, if a class $\mathcal{C}$ has a definition that relativizes, a set A is called *low for* $\mathcal{C}$ if $\mathcal{C} = \mathcal{C}^A$. So the low sets from computability theory are those that are low for the class of sets that are Turing complete for Δ^0_2.

Relativized randomness was studied by several authors, including van Lambalgen [27] and Kautz [17]. The definition of e.g. Σ_1-random relative to A is obtained by reading everywhere in Definition 3.1.1 "A-computable" instead of "computable." That is, a sequence is Martin-Löf random relative to A if there is no uniformly A-computably enumerable sequence of open $\mathcal{U}_n$'s with $\mu(\mathcal{U}_n) \leq 2^{-n}$ that cover the sequence.

M. van Lambalgen and D. Zambella asked whether there exist noncomputable sets A such that every Σ_1-random set is already Σ_1-random relative to A. (The question is first explicitly stated in Zambella [59].) Note that every computable set is low for the Σ_1-random sets. This question was raised in the context of a comparison between randomness properties in classical dynamic systems (specifically, Bernoulli sequences) and recursion theoretic randomness. A result of Kamae [15] showed that the infinite binary sequences that have no information about Bernoulli sequences (normal sequences) are precisely the sequences with zero entropy. The question was whether a similar characterization exists for sets that have no information about Martin-Löf random sequences. This motivated the question whether every set that is low for the Σ_1-random sets has to be computable. The next theorem gives a negative answer:

Theorem 6.0.3 (Kučera and Terwijn [25]) *There exists a noncomputable c.e. set that is low for the* Σ_1*-random sets.*

Kučera and Terwijn left open the question about the exact complexity that such low sets may have. In particular they asked if there are examples outside of Δ^0_2. It was also noted by Downey et al. [9] that the construction of Theorem 6.0.3 bares much resemblance to that of a K-trivial set, i.e. a set A such that $K(A{\restriction}n) \leq K(n) + O(1)$ for every n. K-trivial sets are sets that are as nonrandom as possible in the sense of prefix complexity. Nies [39] clarified the situation by proving that these notions coincide, which by a result of Chaitin implies in particular that every low for Σ_1-random set is in Δ^0_2.

Terwijn and Zambella gave an exact characterization of the sets that are low for the notion of Schnorr-null in terms of the notion of traceability. A sets A is computably traceable if the values of the functions that A computes can be well-approximated by finite sets of a computably bounded size. The computably traceable sets are a strict subset of the sets of hyper-immune free degree, and there exist noncomputable examples of them.

Theorem 6.0.4 (Terwijn and Zambella [55]) *A set A is low for the notion of Schnorr-null if and only if it is computably traceable.*

Theorem 6.0.4 implies that there are uncountably many low for Schnorr-random sets, and that they are all outside of Δ^0_2 (except the computable ones, of course). Note that this radically differs from the situation for the Martin-Löf random sets, where the low sets all had to be *inside* of Δ^0_2.

Finally, for the notion of computable randomness (see Definition 3.1.5) lying in between Martin-Löf and Schnorr randomness, Nies [40]) proved that there are no nontrivial low sets at all:

Theorem 6.0.5 (Nies [40]) *Every set that is low for the computably random sets is computable.*

So we see that for these three notions of randomness the situation of the existence of low sets is completely different.

References

[1] K. Ambos-Spies and A. Kučera, *Randomness in computability theory*, in: P. Cholak et al., Computability Theory: Current Trends and Open Problems, Contemporary Mathematics 257 (2000) 1–14, American Mathematical Society.

[2] K. Ambos-Spies, W. Merkle, J. Reimann, and F. Stephan, *Hausdorff Dimension in Exponential Time*, Computational Complexity 2001, 210-217, IEEE Computer Society, 2001.

[3] C. S. Calude, *Information and Randomness, An Algorithmic Perspective*, Springer, 1994. Second edition 2002.

[4] C. S. Calude, P. H. Hertling, B. Khoussainov, and Y. Wang, *Recursively enumerable reals and Chaitin Ω numbers*, Proc. STACS 1998, Springer (1998) 596–606.

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

[6] G. J. Chaitin, *Algorithmic Information Theory*, Cambridge University Press, 1987.

[7] R. G. Downey, *Some computability-theoretical aspects of reals and randomness*, manuscript, November 2001.

[8] R. G. Downey, D. R. Hirschfeldt, S. Lempp, and R. Solomon, *A Δ^0_2 set with no infinite low subset in either it or its complement*, Journal of Symbolic Logic 66 (2001) 1371–1381.

[9] R. G. Downey, D. R. Hirschfeldt, A. Nies, F. Stephan, *Trivial reals*, In Electronic Notes in Theoretical Computer Science (ENTCS), 2002.

[10] R. Downey and S. A. Terwijn, *Computably enumerable reals and uniformly presentable ideals*, Mathematical Logic Quarterly 48(1) (2002) 29–40.

[11] K. Falconer, *Fractal geometry, mathematical foundations & applications*, Wiley & Sons, 1992.

[12] F. Hausdorff , *Dimension und äußeres Maß*, Mathematische Annalen 79 (1919) 157–179.

[13] J. M. Hitchcock, J. H. Lutz and S. A. Terwijn, *The arithmetical complexity of dimension and randomness*, manuscript, January 2003.

[14] T. Jech, *Set theory*, Academic Press, 1978.

[15] T. Kamae, *Subsequences of normal sequences*, Israel J. Math. 16 (1973) 121–149.

[16] H. P. Katseff, *Complexity dips in random infinite binary sequences*, Information and Control 38 (1978) 258–263.

[17] S. M. Kautz, *Degrees of random sets*, PhD Thesis, Cornell University, 1991.

[18] A. S. Kechris, *Classical descriptive set theory*, Springer-Verlag, 1994.

[19] B. Khoussainov, *Randomness, computability, and algebraic specifications*, Annals of Pure and Applied Logic 91 (1998) 1–15.

[20] H. Ki and T. Linton, *Normal numbers and subsets of ω with given densities*, Fundamenta Mathematicae 144 (1994) 163–179.

[21] K.-I Ko, *On the notion of infinite pseudorandom sequences*, Theoretical Computer Science 48 (1986) 9–33.

[22] L. G. Kraft, *A device for quantizing, grouping, and coding amplitude modulated pulses*, M.Sc. Thesis, MIT, 1949.

[23] A. Kučera, *Measure, Π^0_1-classes and complete extensions of PA*, in: H.-D. Ebbinghaus, G. H. Müller, and G. E. Sacks (eds), Recursion theory week, Lect. Notes in Math. 1141, 245–259, Springer-Verlag, 1985.

[24] A. Kučera and T. A. Slaman, *Randomness and recursive enumerability*, SIAM J. Comput. 31 (2001) 199–211.

[25] A. Kučera and S. A. Terwijn, *Lowness for the class of random sets*, Journal of Symbolic Logic 64(4) (1999) 1396–1402.

[26] S. A. Kurtz, *Randomness and genericity in the degrees of unsolvability*, PhD Thesis, University of Illinois, 1981.

[27] M. van Lambalgen, *Random sequences*, PhD Thesis, University of Amsterdam, 1987.

[28] J. I. Lathrop and J. H. Lutz, *Recursive computational depth*, Information and Computation 153 (1999) 139–172.

[29] L. A. Levin. *On the notion of a random sequence*, Soviet Math. Dokl. 14 (1973) 1413–1416.

[30] M. Li and P. Vitányi, *An introduction to Kolmogorov complexity and its applications*, Springer-Verlag, 1993.

[31] J. H. Lutz, *Category and measure in complexity classes*, SIAM J. Comput. 19 (1990) 1100–1131.

[32] J. H. Lutz, *Almost everywhere high nonuniform complexity*, J. Comput. System Sci. 44 (1992) 220–258.

[33] J. H. Lutz, *Dimension in complexity classes*, Proc. 15th Conference on Computational Complexity, 158–169, IEEE Computer Society, 2000.

[34] J. H. Lutz, *The dimensions of individual strings and sequences*, Information and Computation, to appear. Preliminary version: *Gales and the constructive dimension of individual sequences*, Proc. 27th International Colloquium on Automata, Languages, and Programming, 902–913, Springer, 2000.

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

[36] E. Mayordomo, *A Kolmogorov complexity characterization of constructive Hausdorff dimension.*, Information Processing Letters 84 (2002) 1–3.

[37] Y. N. Moschovakis, *Descriptive set theory*, North-Holland, 1980.

[38] A. Nies, *Reals which compute little*, typeset manuscript, November 2002.

[39] A. Nies, *Lowness properties of reals and randomness*, typeset manuscript, 2002.

[40] A. Nies, *Each Low(CR) set is computable*, typeset manuscript, January 2003.

[41] P. G. Odifreddi, *Classical recursion theory*, Vol. 1, Studies in logic and the foundations of mathematics Vol. 125, North-Holland, 1989.

[42] P. G. Odifreddi, *Classical recursion theory*, Vol. 2, Studies in logic and the foundations of mathematics Vol. 143, North-Holland, 1999.

[43] J. C. Oxtoby, *Measure and Category*, 2nd edition, Springer 1980.

[44] H. Rogers Jr., *Theory of recursive functions and effective computability*, McGraw-Hill, 1967.

[45] G. E. Sacks, *Degrees of unsolvability*, Annals of Mathematics Studies 55, Princeton University Press, 1963.

[46] C.-P. Schnorr, *Zufälligkeit und Wahrscheinlichkeit*, Lect. Notes in Math. 218, Springer-Verlag, 1971.

[47] C. E. Shannon, *The mathematical theory of communication*, Bell System Tech. J. 27 (1948) 379–423, 623–656.

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

[49] R. J. Solomonoff, *A preliminary report on a general theory of inductive inference*, Tech. Report ZTB-138, Zator Company, Cambridge, Mass., November 1960.

[50] R. Solovay, *A model of set theory in which every set of reals is Lebesgue measurable*, Annals of Mathematics 92 (1970) 1–56.

[51] R. Solovay, *Draft of a paper (or series of papers) on Chattin's work*, unpublished manuscript, IBM Thomas J. Watson Research Center, New York, May 1975, 215 pp.

[52] L. Staiger, *Constructive dimension equals Kolmogorov complexity*, Research Report CDMTCS-210, University of Auckland, January 2003.

[53] S. A. Terwijn, *Computability and measure*, PhD thesis, University of Amsterdam/ILLC, 1998.

[54] S. A. Terwijn, *On the quantitative structure of* Δ^0_2, in: U. Berger, H. Osswald, and P. Schuster (eds.), Reuniting the Antipodes — Constructive and Nonstandard Views of the Continuum, Synthèse Library, Kluwer, 2000, 271–284.

[55] S. A. Terwijn and D. Zambella, *Computational randomness and lowness*, Journal of Symbolic Logic 66(3) (2001) 1199–1205.

[56] J. Ville, *Étude critique de la notion de collectif*, Gauthier-Villars, 1939.

[57] Y. Wang, *Randomness and complexity*, PhD Thesis, University of Heidelberg, 1996.

[58] Y.Wang, *A separation of two randomness concepts*, Information Processing Letters 69(3) (1999) 115–118.

[59] D. Zambella, *On sequences with simple initial segments*, ILLC technical report ML-1990-05, University of Amsterdam, 1990.

[60] A. K. Zvonkin and L. A. Levin, *The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms*, Russian Math. Surveys 25(6) (1970) 83–124.