# Randomness, Computation and Mathematics

Rod Downey*

[1] School of Mathematics, Statistics and Operations Research
Victoria University
P. O. Box 600, Wellington, New Zealand.
[2] Isaac Newton Institute for the Mathematical Sciences
20 Clarkson Road, Cambridge CB3 0EH
United Kingdom
rod.downey@vuw.ac.nz

**Abstract.** This article examines some of the recent advances in our understanding of algorithmic randomness. It also discusses connections with various areas of mathematics, computer science and other areas of science. Some questions and speculations will be discussed.

## 1 Introduction

The Copenhagen interpretation of quantum physics suggests to us that randomness is essential to our understanding of the universe. Mathematics has developed many tools to utilize randomness in the development of algorithms and in combinatorial (and other) techniques. For instance, these include Markov Chain Monte Carlo and the metropolis algorithms, methods central to modern science, the probabilistic method is central to combinatorics. Computer science has its own love affair with randomness such as its uses in cryptography, fast algorithms and proof techniques.

Nonetheless, it is not clear what each community means by "randomness". Moreover, even when we agree to try one of the formalizations of the notion of randomness based on computation there is also no clear understanding on how this should be interpreted and the extent to which the applications in the disparate arenas can be reconciled.

In this article I will look at the long term programme of understanding the meaning of randomness via an important part of Turing's legacy, the theory of algorithmic computation: *algorithmic randomness*. The last decade has seen some quite dramatic advances in our understanding of algorithmic randomness. In particular, we have seen significant clarification as to the mathematical relationship between algorithmic computational power of infinite random sources and algorithmic randomness. Much of this material has been reported in the short surveys Downey [27], Nies [53] and long surveys [26, 30] and long monographs

* Research supported by the Marsden Fund of New Zealand. This paper was written whilst the author was a visiting fellow at the Isaac Newton Institute, Cambridge, UK, as part of the Alan Turing "Semantics and Syntax" programme, in 2012.

Downey and Hirschfeldt [29] and Nies [52]. Also the book edited by Hector Zenil [78] has a lot of discussion of randomness of varying levels of technicality, many aimed at the general audience.

To my knowledge, Turing himself though that randomness was a physical phenomenon, and certainly recognized the noncomputable nature of generating random strings. For example, from Turing [71], we have the following quote[3]:

> " An interesting variant on the idea of a digital computer is a "digital computer with a random element." These have instructions involving the throwing of a die or some equivalent electronic process; one such instruction might for instance be, "Throw the die and put the-resulting number into store 1000." Sometimes such a machine is described as having free will (though I would not use this phrase myself)."

John von Neumann (e.g. [75]) also recognized the noncomputable nature of generating randomness, and both seem to believe that physical procedures would be necessary. Von Neumann's quote is famous:

> "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin."

Arguably this idea well predated any notion of computation, but the germ of this can be seen in the following quotation of Joseph Bertrand [14] in 1889.

> "How dare we speak of the laws of chance?
> Is not chance the antithesis of all law?"

There has been a developing body of work seeking to understand not just the theory of randomness but how it arizes in mathematics.

For example, we have also seen an initiative (whose roots go back to work of Demuth [25]) towards using these ideas in the understanding of almost everywhere behaviour and differentiation in analysis (such as Brattka, Miller, Nies [15]). Also halting probabilities are natural and turn up in places apparently removed from such considerations. For instance they turned up naturally in the study of subshifts of finite type (Hochman and Meyerovitch [39], Simpson [66, 68]), fractals (Braverman and Yampolsky [16, 17]) (as we see later), we see randomness giving insight into Ergodic theory such as Avigad [6], Bienvenu et. al. [13] and Franklin et. al. [33].

Randomness has long been intertwined with computer science, (although some regard this as a matter of debate such as Gregorieff and Ferbus [38]) being central to things like polynomial identity testing, proofs like all known proofs of Toda's Theorem and the PCP theorem, as well as cryptographic security. A nice programme of Allender and his co-workers (e.g. [4, 3]) suggests that perhaps complexity classes can be understood by understanding how they relate to

[3] I am indebted to Veronica Becher for discussions of Turing's and Von Neumann's thoughts on randomness.

the collections of strings which are algorithmically random according to various measures.

In this article I will try to give a brief outline of theses topics, and make some tentative suggestions for lines of investigation.

My assumption of the reader of this paper is that they are not well versed in the theory of algorithmic randomness. I will assume that they have a basic training in computability theory to the level of a first course in logic. If you are at all excited by what you read I urge you to look at the surveys or the books suggested above for fuller accounts.

## 2 Basics

I will refer to members of $\{0,1\}^* = 2^{<\omega}$ as *strings*, and infinite binary sequences (members of $2^\omega$, Cantor space) as *reals*. $2^\omega$ is endowed with the tree topology, which has as basic clopen sets

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

where $\sigma \in 2^{<\omega}$. The *uniform* or *Lebesgue measure* on $2^\omega$ is induced by giving each basic open set $[\sigma]$ measure $\mu([\sigma]) := 2^{-|\sigma|}$.

We identify an element $X$ of $2^\omega$ with the set $\{n : X(n) = 1\}$. The space $2^\omega$ is measure-theoretically identical with the real interval $[0,1]$, although the two are not homeomorphic as topological spaces, so we can also think of elements of $2^\omega$ as elements of $[0,1]$. We will let $X \upharpoonright n$ denote the first $n$ bits of $X$.

The earliest work trying to give meaning to the randomness of an individual source was that of von Mises who argued as follows. The real should certainly have to obey the frequency laws like the law of large numbers. Thus

$$\lim_{n\to\infty} \frac{\{m \mid m \leq n \wedge X(m) = 1\}}{n} = \frac{1}{2}.$$

This property is called *normality* and was studied by Borel and others. In fact, any random real clearly should be *absolutely normal*, normal to any basis. It is easy to construct such numbers computably (an interest of Turing discussed in Veronica Becher's article in this volume [8]). In fact any polynomial time random real (in any reasonable sense) is absolutely normal.

von Mises' idea was to consider any possible *selection* of a subsequence and ask that it was normal: Let $f : \omega \to \omega$ be an increasing injection, a selection function. Then a random $X$ should satisfy the following.

$$\lim_{n\to\infty} \frac{\{m \mid m \leq n \wedge X(f(m)) = 1\}}{n} = \frac{1}{2}.$$

von Mises work predated the work in the 30's,culminating in the classic paper of Turing [70], clarifying the notion of computable function. Thus von Mises had no canonical choice for "acceptable selection rules". However, Wald [76, 77] showed that for any *countable* collection of selection functions, there is a sequence that is

random in the sense of von Mises. Church [21] proposed restricting $f$ to (partial) computable increasing functions. This gives rise to notions now called *computable stochasticity*, and *partial computable stochasticity*.

This was how matters stood until the work of Ville. [73] In the following, $S(\alpha, n)$ is the number of 1's in the first $n$ bits of $\alpha$ and similarly $S_f$ for the selected places.

**Theorem 1 (Ville's Theorem [73]).** *Let $E$ be any countable collection of selection functions. Then there is a sequence $\alpha = \alpha_0\alpha_1\ldots$ such that the following hold.*

1. $\lim_n \frac{S(\alpha,n)}{n} = \frac{1}{2}$.
2. *For every $f \in E$ that selects infinitely many bits of $\alpha$, we have* $\lim_n \frac{S_f(\alpha,n)}{n} = \frac{1}{2}$.
3. *For all $n$, we have* $\frac{S(\alpha,n)}{n} \leq \frac{1}{2}$.

The killer is item 3 which says that there are never situations with more 1's than 0's in the first $n$ bits of $\alpha$. That is plainly non-random. Ville suggested adding a further statistical law, the law of iterated logarithms, to von Mises' definition. However, we might well ask "How we can be sure that adding this law would be enough?". Why should we expect there not to be a further result like Ville's (which there is, see [29]) exhibiting a sequence that satisfies both the law of large numbers and the law of iterated logarithms, yet clearly fails to have some other basic property that we would naturally associate with randomness?

We could add more and more statistical laws to our collection of desiderata for random sequences, but there is no reason to believe we would ever be done, and we certainly do not want a definition of randomness that changes with time, if we can avoid it. Martin-Löf's fundamental idea in [55] was to define an abstract notion of a performable statistical test for randomness, and require that a random sequence pass *all* such tests. He did so by effectivizing the notion of a set of measure 0. The way to think about Martin-Löf's definition below is that as we effectively shrink the measure of the open sets we regard as "tests", we are specifying reals satisfying them more and more.

In the below a $\Sigma^0_1$ class is a computably enumerable collection $\{[\sigma] \mid \sigma \in W\}$ for some c.e. set $W$ of strings. Alternatively think of this as a c.e. set of intervals in the interval $[0, 1]$.

**Definition 1 (Martin-Löf [55]).**

1. *A* Martin-Löf test *is a sequence $\{U_n\}_{n\in\omega}$ of uniformly $\Sigma^0_1$ classes such that $\mu(U_n) \leq 2^{-n}$ for all $n$.*
2. *A class $C \subset 2^\omega$ is* Martin-Löf null *if there is a Martin-Löf test $\{U_n\}_{n\in\omega}$ such that $C \subseteq \bigcap_n U_n$.*
3. *A set $A \in 2^\omega$ is* Martin-Löf random *if $\{A\}$ is not Martin-Löf null.*

Now there are three main views of algorithmic randomness. The above is called the *measure-theoretical paradigm*.

We briefly discuss the two other main paradigms in algorithmic randomness as they are crucial to our story. The first is the *computational paradigm*: Random sequences are those whose initial segments are all hard to describe, or, equivalently, hard to compress.

We think of Turing machines $U$ with input $\tau$ giving a string $\sigma$. We regard $\tau$ as a description of $\sigma$ and the shortest such is regarded as the intrinsic information in $\sigma$. The plain $U$-Kolmogorov complexity $C_U(\sigma)$ of $\sigma$ is the *length* of the shortest $\tau$ with $U(\tau) = \sigma$. Turing machines can be enumerated $U_0, U_1, \ldots$ and hence we can remove the machine dependence by defining a new (universal) machine

$$U(0^e 1\tau) = U_e(\tau),$$

so that we can define for this machine $M$, $C(\sigma) = C_M(\sigma)$ and for all $e$, $C(\sigma) \leq C_{U_e}(\sigma)+e+1$. We will use the notation $\leq^+$ for constants and will write $C(\sigma) \leq^+ C_{U_e}(\sigma)$.

A simple counting argument due to Kolmogorov [44] shows that as $C(\sigma) \leq^+ |\sigma|$ (using the identity machine), there must be strings of length $n$ with $C(\sigma) \geq n$. We call such strings *C-random*.

We would like to define a real to be random by saying for all $n$, $C(\alpha \upharpoonright n) \geq^+ n$. Unfortunately, there are no such random reals due to a phenomenon called complexity oscillations, which (in a quantative way) say that in very long strings $\sigma$ there must segments with $C(\sigma \upharpoonright n) < n$. This oscillation really due to the fact that on input $\tau$, we don't just get the *bits* of $\tau$ as information but the *length* of $\tau$ as well. Thus we are losing the intentional meaning that the bits of $\tau$ are processed by $U$ to produce $\sigma$. To get around this first Levin [48, 49] and later Chaitin [19] suggested using *prefix-free machines* to capture this intentional meaning.

Prefix free machines work like telephone numbers. If $U(\tau) \downarrow$ (i.e. halts) then for all $\hat{\tau}$ comparable with $\tau$, $U(\hat{\tau}) \uparrow$.

Already we see a theme that there is not one but perhaps *many* notions of computational compressibility of relevance to understanding randomness. In the case of prefix free complexity, in some sense we know we are on the correct track, due to the following theorem which can be interpreted as saying (for discrete spaces) that Occam's razor and Baye's theorem give the same result (in that the shortest description is essentially the probability that the string is output).

**Theorem 2 (Coding Theorem-Levin [48, 49], Chaitin [19]).** *For all $\sigma$, $K(\sigma) =^+ -\log(Q(\sigma))$ where $Q(\sigma)$ is $\mu(\{\tau \mid U(\tau) = \sigma\})$.*

Using this notion, and noticing that the universal machine above would be prefix-free if all the $U_e$ were prefix free, we can define the prefix-free Kolmogorov complexity $K(\sigma)$.

**Definition 2 (Levin [49], Chaitin [19]).** *A set $A$ is* 1-random *if $K(A \upharpoonright n) \geq^+ n$).*

**Theorem 3 (Schnorr).** *A real $A$ is Martin-Löf random iff it is 1-random.*

Hence the two paradigms converge on a common intuition. It is easy to see that since there are only countably many machines, a real is random with probability 1. The classic example of a 1-random real is Chaitin's *halting probability* (for a universal prefix-free machine $U$):

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

the measure of the domain of $U$ (which has meaning as the domain of $U$ is a prefix free set of strings).

It would seem that the definition of $\Omega$ is thoroughly machine independent but in the same spirit as Myhill's theorem, we can define a reducibility we call Solovay reducibility, and show that there is only one $\Omega$ in this sense. To wit, we observe that $\Omega = \lim_s \Omega_s$ where $\Omega_s = \sum_{\{\sigma | U(\sigma)[s]\downarrow\}} 2^{-|\sigma|}$, (i.e. $s$ steps of computation), and hence $\Omega$ is what is called a left c.e.-real. We can define a notion of reducibility on left c.e.-reals $\alpha \leq_S \beta$ iff there is a partial computable function $f$ and a constant $c$, such that for all rationals $q$ (we assume all reals are nonrational for uniformity), if $q < \alpha$ then $f(q)\downarrow$ and $|\alpha - q| \leq c|\beta - f(q)|$. The culmination of a series of papers is the Kučera-Slaman theorem which states that there is really only one left-c.e. random real.

**Theorem 4 (Kučera-Slaman Theorem [46]).** *$\alpha$ is 1-random and left-c.e. iff for all left c.e.-reals $\beta$, $\beta \leq_S \alpha$.*

The final randomness paradigm is the one based on prediction. The *unpredictability paradigm* is that we should not be able to predict the next bit of a random sequences even if we know all preceding bits, in the same way that a coin toss is unpredictable even given the results of previous coin tosses.

**Definition 3 (Levy [50]).** *A function $d : 2^{<\omega} \to \mathbb{R}^{\geq 0}$ is a* martingale[4] *if for all $\sigma$,*

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

*$d$ is a* supermartingale *if for all $\sigma$,*

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

*A (super)martingale $d$* succeeds *on a set $A$ if $\limsup_n d(A \upharpoonright n) = \infty$. The collection of all sets on which $d$ succeeds is called the* success set *of $d$, and is denoted by $S[d]$.*

The idea is that a martingale $d(\sigma)$ represents the capital that we have after betting on the bits of $\sigma$ while following a particular betting strategy ($d(\lambda)$

[4] A more complex notion of martingale is used in probability theory. We will discuss this notion, and the connection between it and ours, in [29], where it is discussed how computable martingale processes can be used to characterize 1-random reals.

being our starting capital). The *martingale condition* $d(\sigma) = \frac{d(\sigma 0)+d(\sigma 1)}{2}$ is a fairness condition, ensuring that the expected value of our capital after a bet is equal to our capital before the bet. Ville [73] proved that the success sets of (super)martingales correspond precisely to the sets of measure 0.

Now again we will need a notion of effective betting strategy. We will say that the martingale is computable if $d$ is a computable function (with range $\mathbb{Q}$, without loss of generality), and we will say that $d$ is c.e. iff $d$ is given by an effective approximation $d(\sigma) = \lim_s d_s(\sigma)$ where $d_{s+1}(\sigma) \geq d_s(\sigma)$. This means that we are allowed to bet more as we become more confident of the fact that $\sigma$ is the more likely outcome in the betting, as time goes on.

**Theorem 5 (Schnorr [64, 65]).** *A set is* 1*-random iff no c.e. (super)martingale succeeds on it.*

These all seem basic theorems from long ago, but there remain a lot of things we don't understand even around these basic theorems. For example, here are three questions around these theorems.

First, it seems strange that to define randomness we use c.e. martingales and not computable ones. Based on this possible defect, Schnorr defined two other notions of randomness, *computable randomness* (where the martingales are all computable) and Schnorr randomness (where we use the Martin-Löf definition but insist that $\mu(U_k) = 2^{-k}$ rather than $\leq 2^{-k}$ so we know precisely the $[\sigma]$ in $U_k$ uniformly) meaning in each case that the randomness notion is a computable rather and computably enumerable one. We know that Martin-Löf randomness implies computable randomness which implies Schnorr randomness, and none of these implications are reversible. The first question is:"Can we use some kind of computable randomness to define 1-randomness?". The suggested method to do this is to use a computable *but nonmonotonic* notion of randomness, where we have a betting strategy which bets on bits one at a time, but instead of being increasing can bet in some arbitrary order, and may not bet on all bits. The order is determined by what has happened so far. This gives a notion called *Kolmogorov-Loveland* (or nonmonotonic) randomness and the following question has been open for quite a while.

*Question 1 (Muchnik, Semenov, and Uspensky [59]).* Is every nonmonotonically random sequence 1-random?

A discussion of known results can be found in [29].

The second and third questions actually stem from the proof where we show that there is a translation of Martin-Löf tests into c.e. supermartingales. There, we start with a uniformly c.e. sequence $R_0, R_1, \ldots$ of prefix-free generators for a Martin-Löf test. We build a c.e. supermartingale $d$ that bets evenly on $\sigma 0$ and $\sigma 1$ until it finds that, say, $\sigma 0 \in R_n$, at which point it starts to favor $\sigma 0$, to an extent determined by $n$. If later $d$ finds that $\sigma 1 \in R_m$, then what it does is determined by the relationship between $m$ and $n$. If $m < n$ then $d$ still favors $\sigma 0$, though to a lesser extent than before. If $m = n$ then $d$ again bets evenly on

$\sigma 0$ and $\sigma 1$. If $m > n$ then $d$ switches allegiance and favors $\sigma 1$. This can happen several times, as we find more $R_i$ to which $\sigma 0$ or $\sigma 1$ belong.

The computable enumerability of $d$ is essential in the above. A computable supermartingale (which we have seen we may assume is rational-valued without loss of generality) has to decide which side to favor, if any, immediately. Hitchcock has asked whether an intermediate notion, where we allow our supermartingale to be c.e. but do not allow it to switch allegiances in the way described above, is still powerful enough to capture 1-randomness. The purest version of this question was suggested by Kastermans. A *Kastergale* is a pair consisting of a partial computable function $g : 2^{<\omega} \to \{0, 1\}$ and a c.e. supermartingale $d$ such that $g(\sigma) \downarrow = i$ iff $\exists s \, (d_s(\sigma i) > d_s(\sigma(1 - i)))$ iff $d(\sigma i) > d(\sigma(1 - i))$. A set is *Kastermans random* if no Kastergale succeeds on it. A *Hitchgale* is the same as a Kastergale, except that in addition the proportion $\frac{d_s(\tau j)}{d_s(\tau)}$ (where we regard $\frac{0}{0}$ as being 0) is a $\Sigma^0_1$ function, so that if we ever decide to bet some percentage of our capital on $\tau j$, then we are committed to betting at least that percentage from that point on, even if our total capital on $\tau$ increases later. A set is *Hitchcock random* if no Hitchgale succeeds on it. It is unknown if these notions differ from 1-randomness and the import is that *is any bias allowed in the definition of 1-randomness?*

The message also is that there are many kinds of randomness and they each give insight. Variations of the notion of randomness include Kurtz or weak randomness, Demuth randomness, finite randomness, resource bounded randomness (for analyzing complexity classes), etc. For instance, weak randomness asks that $X$ belongs to all $\Sigma^0_1$ classes of measure 1. We refer mostly to [29, 52] for more. There are similarly many kinds of Kolmogorov complexities such as process and monotone complexities (which solve the "$C$-" problem by asking that the action of machines be continuous rather than prefix free). To wit, if $U(\sigma) \downarrow$ and $U(\nu) \downarrow$, and $\sigma \preceq \nu$, then $U(\sigma) \preceq U(\nu)$. There are various interpretations of this idea, such as $U$ being a multifunction (so that $U$ is really a c.e. collection of pairs of strings) called $Km$, monotone complexity, but for all of them, an analog of Schnorr's Theorem holds so that $\alpha$ is 1-random iff $K(\alpha \upharpoonright n) \geq^+ n$ for all $n$. In most cases, $K(\alpha \upharpoonright n) =^+ n$ since the identity machine is monotone.

These ideas and associated probability measures have seen applications into geometric measure theory such as Jan Reimann's new proof of (classical) Frostmann's Lemma using methods from effective randomness ([62])[5]. These continuous Kolmogorov complexities tend to be less well understood. Work of Adam Day (see [29]) gives new methods for building machines. One hallmark is Day's remarkable improvement [23] of Gác's Theorem [35] that the Coding Theorem fails for continuous spaces.

For the remainder of this paper we will need some further (stronger) notions of randomness. We can strengthen the idea of randomness by giving the computational devices more compression power via oracles. Then if $\emptyset^{(n)}$ de-

[5] As we soon see, Simpson ([68]) has similar applications of effective measure to derive classical results in Hausdorff dimension.

notes the $n$-th iterate of the halting problem, we say that $X$ is $n+1$-random iff $K^{\emptyset^{(n)}}(X \upharpoonright n) \geq^+ n$ for all $n$.

It is a surprising fact that for all $n$, $n$-randomness can be defined purely in terms of $K$ with no oracle. This follows by the next result.

**Theorem 6 (Bienvenu, Muchnik, Shen, and Vereschagin [12]).** $K^{\emptyset'}(\sigma) = \limsup_m K(\sigma \mid m) \pm O(1)$.

Hence $A$ would be 2-random iff for all $n$, $\limsup_m K(A \upharpoonright n \mid m) \geq^+ n$. In some cases, we know of natural definitions of $n$-randomness. For instance, we have seen that it is impossible for a real to have $C(X \upharpoonright n) \geq^+ n$ for *all* $n$, but Martin-Löf showed in his original paper that there are reals $X$ with $C(X \upharpoonright n) \geq^+ n$ for *infinitely many* $n$. Joe Miller and later Nies, Stephan and Terwijn showed that such randoms are precisely the 2-randoms, and later Miller showed that the 2-randoms are exactly those that achieve maximal prefix-free complexity $(n + K(n))$ infinitely often. Also Becher and Gregorieff [9] have a kind of index set characterizations of higher notions of randomness. I know of no other natural definitions, such as for the 3-randoms.

Another subtext in these investigations is to dispense with Kolmogorov complexity altogether. The idea is to redo algorithmic randomness using total machines.

**Definition 4 (Bienvenu and Merkle [11]).** *A computable function $f$ is a* Solovay function *if $\sum_n 2^{-f(n)} < \infty$ and $\liminf_n f(n) - K(n) < \infty$ (in other words, there is a $c$ such that $f(n) \leq K(n) + c$ for infinitely many $n$).*

Solovay functions were first constructed by Solovay, but any reasonable time bounded version of prefix-free Kolmogorov complexity give rise to one. (An observation of Hölzl, Kräling, and Merkle [40].) Building on earlier work of Gács, and of Miller and Yu, recently Merkle, Miller and Nies have proven that a set $A$ is 1-random iff $C(A \upharpoonright n) \geq n - g(n) - O(1)$ for any Solovay function $g$. In fact by themselves, Solovay functions characterize 1-randomness.

**Theorem 7 (Bienvenu and Downey [10]).** *Let $f$ be a computable function. The following are equivalent.*

1. *$f$ is a Solovay function.*
2. *$\sum_n 2^{-f(n)}$ is a 1-random real.*

Further extensions on this theme, generalizations and relationships with randomness have been found. See [29], and the later material on $K$-triviality.

We have left out the vast amount of work on effective dimensions. In the same way as we effectivize measure, we can effectivize fractional measure. Theorems include characterizations due to Mayordomo [56] that effective Hausdorff dimension of $X$ is equal to $\liminf_{n\to\infty} \frac{K(X\upharpoonright n)}{n}$ and the characterization of effective packing dimension by Athreya, Hitchcock, Lutz, and Mayordomo [5] as $\limsup_{n\to\infty} \frac{K(X\upharpoonright n)}{n}$ ($C$ can replace $K$ in both cases). These concepts have been shown to have fascinating interactions with computability, such as characterizing degree classes, and as we discuss later, have been used to give new proofs of classical theorems. I don't have space to discuss further, but see [29].

## 3 Randomness and classical computability

Interactions of measure, randomness and computability go way back to the early years of the subject such as the paper de Leeuw et. al. [24] where, amongst other things, it is proven that a set $X$ is enumerable from a set of oracles of positive measure iff $X$ is computably enumerable. As a consequence, we get a result later rediscovered by Sacks that if a real $X$ is computable from a collection of sources of positive measure, then $X$ must be computable. Nevertheless, a classical result is the following saying that random sources can have computational power.

**Theorem 8 (Kućera [45], Gács [36]).** *For every set $X$, there is a random $Y$ such that $X \leq_{wtt} Y$, where $\leq_{wtt}$ is Turing reducibility with use bounded by a computable function.*

The above argues that 1-random reals are not random enough to correlate to the thesis that random reals should have no computational power. This intuition was clarified by Stephan who proved the following[6].

**Theorem 9 (Stephan [69]).** *Suppose a random real is powerful enough to compute a $\{0,1\}$-valued function $f$ such that for all $n$, $f(n) \neq \varphi_n(n)$ (i.e. a PA degree). Then $\emptyset' \leq_T X$, so that it is a "false random."*

Thus we can wash away lots of computational power by raising the level of randomness. For example, it can be shown that $X$ is weakly 2-random (i.e. in every $\Sigma^0_2$ class of measure 1) iff $X$ is 1-random and its degree forms a minimal pair with $\emptyset'$. Hence no (weakly) 2-random real can bound a $PA$ degree. A remarkable theorem here is the following, demonstrating a deep relationship between PA degrees and randomness.

**Theorem 10 (Barmpalias, Lewis, and Ng [7]).** *Every PA degree is the join of two 1-random degrees.*

There has been a huge amount of work concerning the interplay between things like PA degrees and weakenings of the notion of fixed point free functions ($f(n) \neq \varphi_n(n)$). For example, you can show that this ability corresponds to traceing, and the speed of growth of the initial segment complexity of a real. As an illustration, $A$ is *$h$-complex* if $C(A \upharpoonright n) \geq h(n)$ for all $n$. $A$ is *autocomplex* if there is an $A$-computable order $h$ such that $A$ is $h$-complex.

**Theorem 11 (Kjos-Hanssen, Merkle, and Stephan [41]).** *A set is autocomplex iff it is of DNC degree.*

Another illustration of the interplay of notions of randomness and Turing degrees is the theorem.

[6] Interpreted by Hirschfeldt as saying that there are two methods of passing a stupidity test. One is the be the genuine article. The other is to be like $\Omega$ is be so smart that you know what a stupid person would say.

**Theorem 12 (Nies, Stephan, and Terwijn [54]).** *If a nonhigh set (i.e.* $A' \not\geq_T \emptyset^{(2)}$*.) is Schnorr random then it is* 1*-random.*

In fact it is possible to show that within the high degrees the separations between computable, Schnorr, and Martin-Löf randomness always occur. In the hyperimmune-free (or computably dominated $\mathbf{a}$, meaning that for every $f \leq \mathbf{a}$ there is a computable $g$ with $f(n) < g(n)$ for all $n$) degrees, weak randomness coincides with all of these as well as weak 2-randomness.

There is a delicate interweaving of randomness notions and properties of Turing degrees. For example, Kurtz and Kautz long ago showed us that every 2-random degree is hyperimmune (i.e. $\exists f \leq \mathbf{a}(\forall g)(g \text{ computable } \rightarrow \exists^\infty n(f(n) > g(n)))$.) Moreover the "almost all" theory of degrees is decidable by another old result of Stillwell. We refer to [29] for a lot more on this, and similar things concerning effective dimensions.

I cannot leave this part of the survey without mentioning the long sequences of results about lowness notions. For any reasonable property $P$ we say that $X$ is *low for* $P$ if $P^X = P$. For example, being low for the Turing jump means that $X' \equiv_T \emptyset'$. A set $A$ is low for 1-randomness iff $A$ does not make any 1-randoms nonrandom. You can also have a notion of lowness for tests, meaning that every $(\text{effective nullset})^A$ can be covered by an effective nullset. In all cases the lowness notion for randomness and for tests have turned out to coincide with a single recent exception of "difference randomness" found by Diamondstone and Fanklin (paper in preparation).

Now it is not altogether clear that noncomputable sets low for 1-randomness should exist. But they do and form a remarkable class called the $K$-trivials. That is, they coincide with the class of reals $A$ such that forall $n$, $K(A \upharpoonright n) \leq^+ K(n)$. (In fact Bienvenu and Downey [10] showed that it is enough to put a Solovay function on the right side.) Many properties of this class have been shown, and particularly Andre Nies proved the deep result that $A$ is $K$-trivial iff $A$ is low for Martin-Löf randomness iff $A$ is useless as a compressor, $K^A =^+ K$. (Nies [51]). A good account of this material can be found in Nies [52, 53], but things are constantly changing, with maybe 17 characterizations of this class. We also refer to [29] for the situation up to mid-2010.

Other randomness notions give quite different lowness notions. For example, there are no noncomputable reals which are low for $C$ and none low for computable randomness. On the other hand, lowness for Schnorr and Kurtz randomness give interesting subclasses of the hyperimmune-free degrees characterized by notions of being computably dominated, and fixed point free functions in the case of Kurtz. Work here is still ongoing and many results proven, but the pattern remains very opaque. Even for a fixed real like $\Omega$ (i.e. when does $\Omega^X$ remain random?) results are quite interesting. In the case of $\Omega$, $X$ is low for $\Omega$ and $X$ is computable from the halting problem, then $X$ is $K$-trivial, whereas if $X$ is random, then it is 2-random. (Results of Joe Miller, see [29].)

These classes again relate to various refinements of the jump and to "traceing" which means giving an effective collection of *possibilities* for (partial) functions computable from the degree at hand. Again this has taken on a life

of its own, and such methods have been used to solve questions from classical computability theory. For instance, Downey and Greenberg's [28] used "strong jump traceability" to solve a longstanding question of Jockusch and Shore on pseudo-jump operators and cone avoidance. Strongly jump traceable reals have their own agenda and form a fascinating class, see e.g. [20].

The final material for this section is the deep results of Reimann and Slaman who were looking at the question (first discussed by Levin): given $X \not\equiv_T \emptyset$, is there a measure relative to which $X$ is random?

Clearly we can concentrate a measure on a real, but assuming that we are not allowed to do this the answer is still that every noncomputable real can be made random. On the other hand, if we ask that there are no atoms in the measure, the situation is very different. We get a class of *never continuously n-random* reals. For each $n$ this class is countable, but the proof of this requires magical things like big fragments of Borel determinacy, *provably*. The reader should look at Reimann and Slaman [63].

## 4 (Some) applications

### 4.1 Left out

I apologize to the workers who are using approximations to $C$ like commercial compression packages to apply Kolmogorov complexity to measure things like common information[7]. As an illustration, I refer to the work of Vitanyi and his co-workers who do phylogenetic analysis (in biology and music evolution, etc) by replacing metrics like maximum parsimony by common information defined via Kolmogorov complexity. (See e.g. [22, 72].)

### 4.2 Ergodic theory

A very important part of classical mathematics is concerned with recurrent actions of some process. For example, A $d$-dimensional *shift* of finite type is a collection of colourings of $\mathbb{Z}^d$ defined by local rules and a shift action (basically saying certain colourings are illegal). Its (Shannon) *entropy* is the asymptotic growth in the number of legal colourings. More formally, consider $G = (\mathbb{N}^d, +)$ or $(\mathbb{Z}^d, +)$, and $A$ a finite set of symbols. We give $A$ the discrete topology and $A^G$ the product topology. The *shift action* of $G$ on $A^G$ is

$$(S^g x)(h) = x(h + g), \text{ for } g, h \in G \wedge x \in A^G.$$

A *subshift* is $X \subseteq A^G$ such that $x \in X$ implies $S^g x \in X$ (i.e. shift invariant). The classical area of *Symbolic Dynamics* studies subshifts usually of "finite type." Such subshifts are well known to be connected to number theory, Ramsey theory etc.

The following is a recent theorem showing that $\Omega$ occurs naturally in this setting.

[7] The earliest calssical application of Kolgorogov compexity I know of is an old one by Schnorr and Fuchs [34] sharpening aspects of Markov Chain Monte Carlo.

**Theorem 13 (Hochman and Meyerovitch, [39]).** *The values of entropies of subshifts of finite type over $\mathbb{Z}^d$ for $d \geq 2$ are exactly the complements of halting probabilities.*

I remark that in the same way that Reimann proved Frostman's Lemma using effective methods, Simpson [68] has proven classical results using our effective methods. Simpson studies topological entropy for subshifts $X$ and the relationship with Hausdorff dimension. If $X \subset A^G$ use the standard metric $\rho(x, y) = 2^{-|F_n|}$ where $n$ is as large as possible with $x \restriction F_n = u \restriction F_n$ and $F_n = \{-n, \ldots, n\}^d$. In discussions with co-workers, Simpson proved that the classical dimension equals the entropy (generalizing a difficult result of Furstenburg 1967) using effective methods, which were much simpler.

**Theorem 14 (Simpson [68]).** *If $X$ is a subshift (closed and shift invariant), then the effective Hausdorff dimension of $X$ is equal to the classical Hausdorff dimension of $X$ is equal to the entropy, moreover there are calculable relationships between the effective and classical quantities. (See Simpson's home page for his recent talks and more precise details.)*

Other types of Ergodic behaviour have been studied.

The general setting is the following. Let $(X, \mu)$ be a probability space, and $T : X \to X$ measure preserving so that for measurable $A \subseteq X$, $\mu(T^{-1}A) = \mu(A)$. Such a map is *invariant* if $T^{-1}A = A$ except on a measure 0 set. Finally the map is *ergodic* if every $T$-invariant subset is either null or co-null. The shift operator above (say, on Cantor space so that $T(a_0a_1 \ldots) = a_1a_2 \ldots$) is an ergodic action with the Bernoulli product measure.

A classic theorem of Poincaré is that if $T$ is ergodic on $(X, \mu)$, then for all $E \subseteq X$ of positive measure and *almost all* $x \in X$, $T^n(x) \in E$ for infinitely many $n$. For a set of measurable subsets $E$ of $X$, we call an $x$ a *Poincaré point* if $T^n(x) \in Q$ for all $Q \in E$ of positive measure. Long ago Kučera [45] showed that $X$ is 1-random iff $X$ is a Poincaré point for the shift operator with respect to the collection of effectively closed subsets of $2^\omega$.

Bienvenu et. al. proved the following extension of this result.

**Theorem 15 (Bienvenu, et. al. [13]).** *Let $T$ be computable ergodic on a computable probability space $(X, \mu)$. Then $x \in X$ is 1-random iff $x$ is a Poincaré point for all effectively closed subsets of $X$.*

We remark that the notion of a computable probability space is natural and along the lines of the Pour-El Richards [61] version of computable metric space. There are again a lot of results here. Franklin et. al. [33] looked at the classic Birkhoff ergodic theorem for $f \in L^1(X)$ (namely $\lim_{n\to\infty} \frac{1}{n} \sum_{i<n} f(T^i(x)) = \int f d\mu$.) and showed that 1-random points satisfy Birkhoff's ergodic theorem. For other interpretations and stronger hypotheses (that the measure of the closed sets is computable), Gács, Hoyrup and Rojas [37], showed that the Birkhoff points are precisely the Schnorr randoms. This is currently an area of intense activity, and many of the classical ergodic theorems remain to be studied. For

example, Furstenburg's one with its applications to arithmetical progressions would seem a natural candidate.

This is also related to metamathematical studies, and here we refer the reader to Avigad [6].

Another interesting application of the ideas from algorithmic randomness is to the area of Julia sets. Recall that this is described by $z \mapsto z^2 + \alpha z$, where $\alpha = e^{2\pi i\theta}$. Braverman and Yampolsky [16, 17] showed that in general even for computable $\theta$, Julia sets can coincide with complements of $\Omega$.

### 4.3 Differentiability is the same as randomness

In his blog, Terry Tao remarks that Ergodic theorems and classical theorems from analysis such as the Lebesgue theorem that functions of bounded variation are differentiable almost everywhere are closely related. In Bishop's book, they have almost the same proof. It is thus not surprising that we see such theorems giving rise to randomness notions. This is an idea going way back to the work of Oswald Demuth, a constructivist from Prague. It is being actively pursued by Brattka, Nies, Miller and others.

Recall that the Denjoy upper and lower derivatives for a function $f$ are defined as follows.

$$\overline{D}f(x) = \limsup_{h\to 0} \frac{f(x) - f(x+h)}{h} \text{ and } \underline{D}f(x) = \liminf_{h\to 0} \frac{f(x) - f(x+h)}{h}.$$

The Denjoy derivate exists iff both of the above quantities exist and are finite. The idea in this is that slopes like those in the definitions can be considered to be martingales.

Using this for one direction, various notions of randomness can be characterized by (i) varying the strength of the notion of computable real valued function (e.g. Markov computable, type 2 computable etc) (ii) varying the theorem.

For an illustration, we have the following.

**Theorem 16 (Brattka, Miller and Nies [15]).** *$z$ is computably random iff every computable (in the type two sense) increasing function $f[0,1] \to \mathbb{R}$ is differentiable at $x$.*

There are similar results relating 1-randomness of $x$ to its differentiability of functions of bounded variation. There is still a lot of activity here, and class like Lipschitz functions and many other classical almost everywhere behaviour in analysis are found to correlate to various notions of randomness. The paper [15] is an excellent introduction to this material.

We might speculate that this could also be related to the general purpose analog computer studied by Shannon, Martin-Pour-El, Ruebel and others last century.

## 5 Relationships between random strings and complexity classes

A very interesting programme is due to Allender and his co-workers (and others such as Day). At first glance it seems rather strange, but the idea is to look at resource bounded reductions to highly noncomputable objects like clean versions of $R_C = \{\sigma : C(\sigma) \geq \frac{|\sigma|}{2}\}$, and similarly $R_Q$ for any other Kolmogorov complexity $Q$. Long ago, Kummer [47] showed that $R_C$ is $tt$-complete. This is by no means an obvious fact and the proof uses $\mathbf{0}''$ nonuniformity to build the reduction. It is not necessarily true for $R_K$ and depends on the choice of universal machine, a fact established by Muchnik (in [58]), using a fascinating game-theoretical argument (see [29] for details).

Kummer's reduction was double exponential length increasing and one might ask what does $P^{R_C}$ look like. Clearly $P^{R_C}$ has noncomputable sets of strings in it, but the idea that this is an artifact of the choice of universal machine. The correct class to look at is

$$\cap_U P^{R_{C_U}}.$$

Sometimes it is suggested that this should be intersected with the computable sets, but Allender conjectures that this makes no difference, $\cap_U P^{R_{C_U}} \cap \mathrm{COMP} = \cap_U P^{R_{C_U}}$.

In [4] it is proven that $P = \cap_U \{A : A \leq^p_{dtt} R_{C_U}\} \cap \mathrm{COMP}$ where the reductions are restricted to polynomial time disjunctive truth table ones. Some of the results so far, for any variants of the Kolmogorov complexity (so we drop the subscript) are $\mathrm{BPP} \subseteq \{A : A \leq^p_{tt} R\} \cap \mathrm{COMP}$, $\mathrm{PSPACE} \subseteq P^R \cap \mathrm{COMP}$, and $\mathrm{NEXP} \subseteq \mathrm{NP}^R \cap \mathrm{COMP}$. Specifically it is open for these containments if we can drop the $\cap\mathrm{COMP}$. The containments might actually be equality, and these are important open questions. Recently, Allender, Friedman and Gasarch [2] have tightened two of these for prefix-free complexity to $\mathrm{BPP} \subseteq \{A : A \leq^p_{tt} R_K\} \cap \mathrm{COMP} \subseteq \mathrm{PSPACE}$ and $\mathrm{NEXP} \subseteq \mathrm{NP}^{R_K} \cap \mathrm{COMP} \subseteq \mathrm{EXPSPACE}$. Interestingly, these proofs come from sharpening Muchnik's game method, along with the fact that the natural home for strategies is PSPACE.

The methods for some of these results use extractors. These are methods of taking weak sources of randomness and producing pseudo-randomness from them, and are particularly successful if you either have independent sources, or some "true" randomness like a physical source assuming quantum assumptions. those have found other uses in algorithmic randomness, such as Zimand's proof [79] that two sources of nonzero effective Hausdorff dimension can together compute a degree which has Hausdorff dimension 1. It is known that one source is not enough as Miller [57] has shown that there is a Turing degree of fractional effective Hausdorff dimension. (See [29]. It is still open if a Turing degree can be minimal and have effective Hausdorff dimension 1.)

## 6 Physics

In this last section I will mention a few things of relevance. First, it is possible to look at various natural phenomena which are regarded as random, such as, say, Brownian motion. Fouche [31, 32], Kjos-Hanssen and Nerode [42] and B. Kjos-Hanssen and T. Szabados [46] have a nice body of work here, showing that, for instance, 1-randomness can be used to understand Brownian motion.

Another major area of randomness is quantum physics under the Copenhagen interpretation. Some physicists claim that this produces *true randomness*. In the same way that we don't know if the universe can produce any incomputability, it seems that we don't know if it can even produce 1-randomness, say. In spite of this, it seems that we can buy true randomness by Internet, via companies using semi-transparent mirrors. One such company is *Quantis*: quantum mechanical random number generator produced and sold by id Quantique of the University of Geneva. They seem to pass reasonable practical statistical tests.

It seems that this is a hypothesis that might be analyzed. Assuming that the universe is a (computable) manifold and assuming the Copenhagen interpretation, we could ask if we could produce initial segments of random reals. Calude, Svozil and others are looking at this idea e.g. [1, 18]

## 7 Conclusion

This is my interpretation of a few themes and high points for the exciting area of algorithmic randomness. Space considerations preclude me including more. I do hope I have at least wetted your interest in this fascinating subject.

## References


1. A. A. Abbott, C. S. Calude, K. Svozil. *Incomputability of quantum physics,* in preparation.
2. E. Allender, L. Friedman and W. Gasarch, *Limits on the computational power of random strings,* ICALP, 2011.
3. E. Allender, H. Buhrman, M. Koucký, D. van Melkebeek, and D. Ronneburger, *Power from Random Strings,* SIAM J. Comp. Vol. 35 (2006), 1467-1493.
4. E. Allender, H. Buhrman, and M. Koucký, *What Can be Efficiently Reduced to the Kolmogorov-Random Strings?,* Annals of Pure and Applied Logic, 138 (2006) 2-19.
5. K. Athreya, J. Hitchcock, J. Lutz, and E. Mayordomo. *Effective strong dimension in algorithmic information and computational complexity*, SIAM Jour. Comput., 37 (2007), 671–705.
6. J. Avigad, *The metamathematics of ergodic theory* Annals of Pure and Applied Logic, 157 (2009), 64-76.
7. G. Barmpalias, A. Lewis, and K. M. Ng. *The importance of $\Pi^0_1$ classes in effective randomness*, JSL, 75(1) (2010), 387–400.
8. V. Becher, *Turing's normal numbers: towards randomness* this proceedings.
9. V.Becher, S.Grigorieff, *From index sets to randomness in $\emptyset^n$, Random reals and possibly infinite computations*, Journal of Symbolic Logic, 74:1 (2009), 124–156.

10. L. Bienvenu and R. Downey. *Kolmogorov complexity and Solovay functions*, in STACS 2009, 147–158.
11. L. Bienvenu and W. Merkle. *Reconciling data compression and Kolmogorov complexity*, in ICALP 2007, Lecture Notes in Computer Science 4596. Springer, 2007.
12. L. Bienvenu, An. A. Muchnik, A. Shen, and N. Vereshchagin. *Limit complexities revisited*, in STACS 2008.
13. L. Bienvenu, A. Day, M. Hoyrup, I. Mezhirov, and A. Shen, *Ergodic-type characterizations of algorithmic randomness*, To appear in Information and Computation.
14. J. Bertrand, *Calcul des Probabilités*, 1889.
15. V. Brattka, J. Miller, and A. Nies, *Randomness and differentiability*, to appear.
16. M. Braverman and M. Yampolsky, *Non-Computable Julia Sets* Journ. Amer. Math. Soc. 19(3), 2006
17. M. Braverman and M. Yampolsky, *Computability of Julia Sets*, Springer-Verlag, 2008.
18. C. Calude, K. Svozil. *Quantum randomness and value indefiniteness,* Advanced Science Letters 1 (2008), 165168.
19. G. Chaitin, *A theory of program size formally identical to information theory*, Journal of the ACM, 22 (1975), 329–340.
20. P. Cholak, R. Downey, and N. Greenberg. *Strong-jump traceablilty. I. The computably enumerable case*, Advances in Mathematics, 217 (2008) 2045–2074.
21. A. Church, *On the concept of a random sequence*, Bulletin of the American Mathematical Society, 46 (1940), 130–135.
22. R. Cilibrasi, P.M.B. Vitanyi, R. de Wolf, *Algorithmic clustering of music based on string compression,* Computer Music J., 28:4(2004), 49-67.
23. A. Day. *Increasing the gap between descriptional complexity and algorithmic probability,* Transactions of the American Mathematical Society, 363 (2011), 5577-5604.
24. K. de Leeuw, E. F. Moore, C. E. Shannon, and N. Shapiro. *Computability by probabilistic machines*, In C. E. Shannon and J. McCarthy, editors, *Automata studies*, number 34 in Annals of Mathematics Studies, pages 183–212. Princeton University Press, Princeton, N. J., 1956.
25. O. Demuth, *The differentiability of constructive functions of weakly bounded variation on pseude-numbers,* Comment. Math. Univ. Carolina. Vol. 16 (1975), 583-599.
26. Downey, R., *Five Lectures on Algorithmic Randomness,* in *Computational Prospects of Infinity, Part I: Tutorials* (Ed. C. Chong, Q. Feng, T. A. Slaman, W. H. Woodin and Y. Yang) Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore Vol 14, World Scientific, Singapore, 2008, 3-82.
27. R. Downey, *Algorithmic randomness and computability, Proceedings of the 2006 International Congress of Mathematicians,* Vol 2, *European Mathematical Society*, (2006), 1-26.
28. R. Downey and N. Greenberg, *Pseudo-jump operators and SJTHard sets,* submitted.
29. R. Downey and D. Hirschfeldt, *Algorithmic Randomness and Complexity*, Springer-Verlag, 2010.
30. Downey, R., D. Hirschfeldt, A. Nies, and S. Terwijn, *Calibrating randomness,* Bulletin Symbolic Logic. Vol. 12 (2006), 411-491.
31. W. Fouche, *The descriptive complexity of Brownian motion,* Advances in Mathematics 155 (2000), 317–343.

32. W. Fouche, *Dynamics of a generic Brownian motion: Recursive aspects*, Theoretical Computer Science 394 (2008), 175-186.
33. J. Franklin, N. Greenberg, J. Miller and Keng Meng Ng, *Martin-Loef random points satisfy Birkhoff's ergodic theorem for effectively closed sets,* to appear, Proc. Amer. Math. Soc.
34. H. Fuchs and C. Schnorr, *Monte Carlo methods and patternless sequences,* in *Operations Research Verfahren*, Vol XXV, Symp. Heidelberg, 1977, 443-450.
35. P. Gács. *On the relation between descriptional complexity and algorithmic probability*, Theoretical Computer Science, 22 (1983), 71–93.
36. P. Gács. *Every set is reducible to a random one*, Information and Control, 70:186–192, 1986.
37. P. Gács, M. Hoyrup and C. Rojas, *Randomness on computable probability spaces, a dynamical point of view,* to appear, Theory of Computing Systems.
38. S. Gregorieff and M. Ferbus, *Is Randomness native to Computer Science? Ten years after* in [78], (2011) 243-263.
39. M. Hochman and T. Meyerovitch, *A characterization of the entropies of multidimensional shifts of finite type,* Annals of Mathematics Vol. 171 (2010), No. 3, 2011-2038
40. R. Hölzl, T. Kräling, and W. Merkle. *Time bounded Kolmogorov complexity and Solovay functions*, in MFCS 2009, volume 5734 of *Lecture Notes in Computer Science*, pages 392–402. Springer, 2009.
41. B. Kjos-Hanssen, W. Merkle, and F. Stephan. *Kolmogorov complexity and the recursion theorem*, in STACS 2006, LNCS 3884, 149–161. Springer.
42. B. Kjos-Hanssen and A. Nerode, *Effective dimension of points visited by Brownian motion* Theoretical Computer Science 410 (2009), no. 4-5, 347-354.
43. B. Kjos-Hanssen and T. Szabados, *Kolmogorov complexity and strong approximation of Brownian motion,* Proc. Amer. Math. Soc. 139 (2011) no. 9, 3307-3316.
44. A. N. Kolmogorov, *Three approaches to the quantitative definition of information*, Problems of Information Transmission, 1 (1965), 1–7.
45. A. Kučera. *Measure, $\Pi^0_1$ classes, and complete extensions of PA*, In *Recursion Theory Week*, volume 1141 of *Lecture Notes in Mathematics*, pages 245–259, Oberwolfach, 1984, 1985. Springer, Berlin.
46. A. Kučera T. Slaman, *Randomness and recursive enumerability*, SIAM J. on Comp., 31 (2001), 199–211.
47. M. Kummer. *On the complexity of random strings*, in STACS '96, LNCS 1046, 25–36. Springer, 1996.
48. L. Levin. *Some theorems on the algorithmic approach to probability theory and information theory*, Dissertation in Mathematics Moscow University, 1971.
49. L. Levin. *Laws of information conservation* (*non-growth*) *and aspects of the foundation of probability theory*, Problems of Information Transmission, 10 (1974) 206–210, 1974.
50. P. Lévy, *Théorie de l'Addition des Variables Aléatoires*. Gauthier-Villars, 1937.
51. Nies, A., *Lowness properties and randomness*, Advances in Mathematics 197, 1 (2005), 274-305..
52. A. Nies, *Computability and Randomness,* Oxford University Press, 2009.
53. A. Nies, *Interactions of computability and randomness,* in *Proceedings of the International Congress of Mathematicians,* (S. Ragunathan, ed.) 30-57 (2010).
54. A. Nies, F. Stephan, and S. A. Terwijn. *Randomness, relativization, and Turing degrees*, JSL, 70(2) (2005), 515–535.

55. P. Martin-Löf, *The definition of random sequences*, Information and Control, 9 (1966) 602–619.
56. E. Mayordomo. *A Kolmogorov complexity characterization of constructive Hausdorff dimension* Infor. Proc.Lett., 84 (2002), 1–3.
57. J. Miller. *Extracting information is hard: a Turing degree of non-integral effective Hausdorff dimension*, to appear Advances in Mathematics.
58. An. A. Muchnik and S. P. Positselsky. *Kolmogorov entropy in the context of computability theory*, Theor. Comp. Sci., 271:15–35, 2002.
59. An. A. Muchnik, A. Semenov, and V. Uspensky, *Mathematical metaphysics of randomness*, Theor. Comp. Sci., 207(2) (1998), 263–317.
60. A. Nies and J. Miller, *Randomness and computability: Open questions*, Bull. Symb. Logic. 12 no 3 (2006) 390-410.
61. M. Poul-El and I. Richards, *Computability in Analysis and Physics*, Springer-Verlag, 1989.
62. J. Reimann, *Effectively closed classes of measures and randomness,* Annals of Pure and Applied Logic, 156(1) (2008), 170–182.
63. J. Reimann and T. Slaman, *Randomness for continuous measures*, to appear. (draft available from Reimann's web site.)
64. C. P. Schnorr, *A unified approach to the definition of a random sequence*, Mathematical Systems Theory, 5 (1971), 246–258.
65. C. P. Schnorr, *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*, volume 218 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin–New York, 1971.
66. S. Simpson, *Medvedev Degrees of 2-Dimensional Subshifts of Finite Type*, to appear, Ergodic Theory and Dynamical Systems.
67. S. Simpson, *Mass Problems Associated with Effectively Closed Sets* (2010) to appear Tohoku Mathematical Journal.
68. S. Simpson, *Symbolic Dynamics: Entropy = Dimension = Complexity* (2011) to appear.
69. F. Stephan. *Martin-Löf random sets and PA-complete sets*, In *Logic Colloquium '02*, volume 27 of *Lecture Notes in Logic*, 342–348. Association for Symbolic Logic, 2006.
70. A. Turing, *On computable numbers with an application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society, 42 (1936), 230–265, 1936. Correction in Proceedings of the London Mathematical Society, 43 (1937), 544–546.
71. A. Turing, *Computing machinery and intelligence*, Mind, 59 (1950), 433-460.
72. P. Vitanyi, *Information distance in multiples,* IEEE Trans. Inform. Theory, 57:4(2011), 2451-2456.
73. J. Ville, *Étude Critique de la Notion de Collectif*, Gauthier-Villars, 1939.
74. R. von Mises, *Grundlagen der Wahrscheinlichkeitsrechnung*, Math. Z. 5 (1919), 52–99.
75. J. von Neumann, *Various techniques used in connection with random digits,* in in *Monte Carlo Method,* (A.S. Householder, G.E. Forsythe, and H.H. Germond, editors), National Bureau of Standards Applied Mathematics Series, vol. 12 1951: 36-38.
76. A. Wald, *Sur le notion de collectif dans la calcul des probabilitiés*, Comptes Rendes des Seances de l'Académie des Sciences, 202 (1936), 1080–1083.
77. A. Wald, *Die Weiderspruchsfreiheit des Kollektivbegriffes der Wahrscheinlichkeitsrechnung*, Ergebnisse eines mathematischen Kolloquiums, 8 (1937), 38–72.

78. H. Zenil, *Randomness Through Computation: Some Answers, More Questions,* (Hector Zenil editor), World Scientific, Singapore, 2011.
79. M. Zimand. *Two sources are better than one for increasing the Kolmogorov complexity of infinite sequences*, LNCS 5010 (2008), 326–338. Springer.