Sub-computable Bounded Pseudo-Randomness

Douglas Cenzer[1] and Jeffrey B. Remmel[2]

[1] Department of Mathematics, University of Florida, P.O. Box 118105, Gainesville, Florida 32611 *cenzer@math.ufl.edu*,
[2] Department of Mathematics, University of California, San Diego, La Jolla, CA 92093-0112 *jremmel@ucsd.edu*

Abstract. This paper defines a new notion bounded pseudo-randomness for certain classes of subcomputable functions where one does not have access to a universal machine for that class within the class. In particular, we define such a version of randomness the class of primitive recursive function and certain subclass of PSPACE functions. Our new notion of bounded pseudo-randomness is robust in that there are equivalent formulations in terms of (1) Martin-Löf tests, (2) Kolmogorov complexity, and (3) martingales.
Keywords: algorithmic randomness, complexity, computability

1 Introduction

The study of algorithmic randomness has flourished over the past century. The main topic of study in this paper is the randomness of a single real number which, for our purposes, can be thought of as an infinite sequence $X = (X(0), X(1), \dots)$ from $\{0,1\}^\omega$. Many interesting notions of algorithmic randomness for real numbers have been investigated in recent years. The most well-studied notion, Martin-Löf randomness [31] or 1-randomness, is usually defined in terms of measure. A real X is 1-random if it is *typical*, that is, X does not belong to any effective set of measure zero in the sense of Martin-Löf [31]. A second definition of 1-randomness may be given in terms of information content. X is 1-random if it is *incompressible*, that is, the initial segments $(X(0), X(1), \dots, X(n))$ have high Kolmogorov [23] or Levin-Chaitin [10, 25] complexity. A third definition may be given in terms of martingales. X is 1-random if it is unpredictable, that is, there is no effective martingale for which one can can obtain unbounded capital by betting on the values of X [36]. These three versions have been shown by Schnorr [33] to be equivalent. This demonstrates the robustness of the concept of Martin-Löf randomness. Many other notions of algorithmic randomness have been studied and in most cases, formulations are only given for one or perhaps two versions. For a thorough study of the area of algorithmic randomness, the reader is directed to three excellent recently published books: Downey and Hirschfeldt [18], Nies [32] and Li and Vitanyi [27].

In this paper we present a notion of bounded pseudo-randomness for certain classes of subcomputable functions where one does not have access to a universal

⋆ Cenzer was partially supported by the NSF grant DMS-652372.

machine for that class within the class. We will first state our definitions for the class of primitive recursive functions and define a new notion of *bounded primitive recursive pseudo-randomness* (BP randomness). We shall show that there are three equivalent definitions of BP randomness, one in in terms of measure, one in terms of compressibility, and and one in terms of martingales. For measure, a *bounded primitive recursive test* will be a primitive recursive sequence of clopen sets $(U_n)_{n\geq 0}$ such that U_n has measure $\leq 2^{-n}$ and we define X to be BP random if it does not belong to $\cap_{n\geq 0} U_n$ for any such test. For compressibility, we say that X is BP compressed by primitive recursive machine M if there is a primitive recursive function f such that $C_M(X \upharpoonright f(c)) \leq f(c) - c$ for all c where C_M is a primitive recursive analogue Kolomogrov complexity. We will show that X is BP random if and only if X is not compressible by any primitive recursive machine. We will also consider *process machines* and the resulting notion of process complexity as studied recently by Day [13].

For martingales, we say a primitive recursive martingale d succeeds on a sequence X if there is a primitive recursive function f such that $d(X \upharpoonright f(n)) \geq 2^n$ for each n. Thus d makes us rich betting on X and f tells us how fast this happens. We will show that X BP random if and only if there is no primitive recursive martingale which succeeds on X.

These definitions can easily be adapted to define a notion of bounded pseudo-randomness for other classes of sub-computable functions. As an example, we will define a notion of bounded PSPACE pseudo-randomness.

The term *bounded randomess* or *finite randomness* are sometimes used to refer to versions of randomness given by tests in which the c.e. open sets are in fact clopen. Thus our notion of BP randomness is "bounded" in this sense. The term "finite" comes from the fact that any clopen set U is the finite union of intervals $U = [\sigma_1] \cup \cdots \cup [\sigma_k]$. Weak randomness, or Kurtz randomness [24] falls into this category. A real X is Kurtz random if it does not belong to any Π^0_1class Q of measure zero. But any Π^0_1class may be effectively expressed as a decreasing intersection of clopen sets $Q = \cap_n Q_n$ where the clopen sets Q_n are unions of intervals of length n. If $\mu(Q) = 0$, it is easy to find a subsequence $U_i = Q_{n_i}$ with $\mu(U_i) \leq 2^{-i}$ and thus $(U_n)_{n\geq 0}$ is a bounded Martin-Löf test. Another special type of bounded randomness was recently studied by Brodhead, Downey and Ng [6].

As shown by Wang [39], Kurtz random reals need not be stochastic in the sense of Church. For example, it need not be the case that the relative number of occurrences of 0's and 1's in a Kurtz random sequence X tends to 1 in the limit. In such a situation, one often uses the term pseudo-random instead of randomness. Our BP random reals are pseudo-random in this sense. That is, we will construct a recursive real which is BP random but not stochastic. However, we will show that BP random sets satisfy only a weak version of the stochastic property.

A lot of work has been done on various notions of resource-bounded randomness. One of the first approaches to resource-bounded randomness was via the stochastic property of typical reals [12]. It is expected that for a random real,

the relative density of the occurrences of 0 and of 1 should be equal in the limit. We identify a set A of natural numbers with its characteristic function and in those terms we expect that $\lim_n \frac{card(A \cap n)}{n} = \frac{1}{2}$. Levin [25] defined a notion of primitive randomness for a set A to mean that for every primitive recursive set B, $A \cap B$ is stochastic relative to B and constructed a recursive set that is primitive random. Di Paola [14] studied similar notions of randomness in the Kalmar hierarchy of elementary functions. Wilber [40] defined a set A to be P-random if, for every $PTIME$ set B, A and B agree on a set of density $\frac{1}{2}$ and constructed an exponential time computable P-random set.

The literature of computational complexity contains many papers on random number generators and cryptography which examine various notions of pseudorandomness. For example, Blum and Micali [4] gave a weak definition of pseudorandom sequences in which a randomly generated sequence is said to be pseudorandom if it meets all $PTIME$ statistical tests. Ko [22] gives definitions of randomness with respect to polynomial time and space complexity which are in the tradition of algorithmic randomness as established by Levin, Martin-Löf and Chaitin. One of the notions of Ko has equivalent formulations in terms of tests and in terms of compressibility and has bounds on the compressibility that are similar in nature to those presented in this paper. Ko's definitions are based on computation from a universal machine M and in particular state that X is ($PSPACE$) compressed with polynomial bounding function f if, for every k, there exists infinitely many n such that $K_M(X \upharpoonright n) < n - (log\ n)^k$. In conatrast, our definitions are not based on the existence of a universal machine.

Lutz [28] defined an important notion of resource-bounded randomness in terms of martingales. Here a real is say PSPACE random if there is no PSPACE martingale which succeeds on X. One can also say that a set $\mathcal{X}$ of reals has PSPACE measure one if there is no PSPACE martingale which succeeds on every element of $\mathcal{X}$. Then almost every $EXPSPACE$ real is random and this can be used to study properties of EXPSPACE reals by examining whether the set of EXPSPACE reals with the property has measure one. Buhrman and Longpre gave a rather complicated equivalent formulation of $PSPACE$ randomness in terms of compressibility. Lutz's notion of complexity theoretic randomness concept has had great impact on complexity theory [1–3]. Shen et al [11] have recently studied on-line complexity and randomness.

There are several important properties of Martin-Löf randomn reals that are regarded as fundamental such as Ville's theorem which states that any effective subsequence of a random sequence is also random. We will prove an analogue of Ville's theorem for BP randomness. Another fundamental property is random reals is van Lambalgen's theorem, which states that the join $A \oplus B$ of two random sets is random iff A is random relative to B and B is random. We define a notion of relative BP randomness which still has three equivalent formulations, and prove an analogue of van Lambalgen's theorem for this notion. Our formulation is a type of truth-table reducibility similar to that of Miyabe [30].

For the case of bounded $PSPACE$ randomness, we give two different notions, one which has equivalent versions for compression and for measure and the other

of which has equivalent versions for measure and for martingales. These notions are actually a hybrid of polynomial time and space.

We note that we get a notion of bounded computable pseudo-randomness by replacing primitive recursive functions by computable recursive functions in our definitions. In such a case, our definition are equivalent to Kurtz randomness which has nice equivalent formulations in all three settings. This was previously shown by Wang [39] for the martingale definition and by Downey, Griiffiths and Reid [17] for the compression definition. We give relativized versions of these definitions as well.

Jockusch [20] showed that Kurtz random sets are *immune*, that is, they do not have infinite computable subsets. We will consider notions of immunity for oue notion of bounded psuedo-random sets.

We will normally work with the usual alphabet $\Sigma = \{0, 1\}$ and the corresponding set $\{0, 1\}^*$ of finite strings and the Cantor space $\{0, 1\}^\omega$ of infinite sequences, but the results hold for any finite alphabet.

The outline of this paper is as follows. In section two, we study BP randomness and show the equivalence of our three versions. We construct a computable real which is BP random. We prove an analogue of Ville's theorem for primitive recursive subsequences of BP random reals. We will also define a notion of relative randomness and prove an analogue of van Lambalgen's theorem. In section three, we briefly consider bounded computable randomness and observe that this is simply Kurtz randomness. There are equivalent definitions here of all three types. Finally, in section four, we consider two notions of bounded $PSPACE$ pseudorandomness and give two equivalent defintions for each notion.

2 Bounded Primitive Recursive Randomness

In this section, we will define the three notions of primitive recursive randomness, Kolomogorov BP randomness, Martin-Löf BP randomness, and martingale BP randomness and show their equivalence. Hence, we will say that that real X is BP random if it statisfies one of these three definitions. We will then prove analogues of Ville's Theorem and van Lambalgen's Theorem of BP random reals.

Let $Prim$ be the family of primitive recursive functions $M : \Sigma^* \to \Sigma^*$, where Σ is a finite alphabet (traditionally $\{0, 1\}$). Note that we can code finite strings as numbers in order to define these primitive recursive functions and that the coding and decoding functions are all primitive recursive.

Martin-Löf BP randomness

In what follows, the code $c(\sigma)$ of a finite sequence $\sigma = \sigma_1 \dots \sigma_n \in \{0, 1\}^*$ is just the natural number whose binary expansion is $1\sigma_1 \dots \sigma_n$. Given a finite set $S = \{\sigma^{(1)}, \dots, \sigma^{(k)}\}$ of strings in $\{0, 1\}^*$ such that $c(\sigma^{(1)}) < \dots < c(\sigma^{(k)})$, the code $C(S)$ of S is defined be the natural number n whose ternary expansion is $2c(\sigma^{(1)})2 \dots 2c(\sigma^{(1)})$. We let 0 be the code of the empty set. We say a sequence $\{U_n : n \in \mathbb{N}\}$ of clopen sets is a primitive recursive sequence if there is a recursive function f such that for all n, $f(n)$ is a code of finite set $\{\sigma_{1,n}, \dots, \sigma_{k(n),n}\}$ such

that $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k(n),n}]$. Here for any $\sigma \in \{0,1\}^*$, $[\sigma]$ is just the set of all $\tau \in \{0,1\}^*$ that extend or are equal σ. Since we can recover $\{\sigma_{1,n}, \ldots, \sigma_{k(n),n}\}$ from $f(n)$ in polynomial time, it is easy to see that given any primite recursive sequence $\{U_n : n \in \mathbb{N}\}$, we can produce a primitive recursive function g such that $g(n)$ is a code of finite set $\{\tau_{1,n}, \ldots, \tau_{r(n),n}\}$ such that $U_n = [\tau_{1,n}] \cup \cdots \cup [\tau_{r(n),n}]$ and $|\tau_{1,n}| = \cdots = |\tau_{r(n),n}| = \ell(n)$ where r and ℓ are also primitive recursive function.

We define a primitive recursive test to be a primitive recursive sequence $(U_n)_{n\geq 0}$ of clopen sets such that, for each n, $\mu(U_n) < 2^{-n}$. Without loss of generality, we may assume that there is a primitive recursive function g such that $g(n)$ is a code of finite set $\{\tau_{1,n}, \ldots, \tau_{r(n),n}\}$ such that $U_n = [\tau_{1,n}] \cup \cdots \cup [\tau_{r(n),n}]$ and $|\tau_{1,n}| = \cdots = |\tau_{r(n),n}| = \ell(n)$ where r and ℓ are also primitive recursive functions. It follows that there is a primitive recursive function m such that $m(n)$ codes the measure $\mu(U_n)$ as a dyadic rational. Since the measures $\mu(U_n)$ may be computed, one could equivalently consider a primitive recursive sequence $\{V_n : n \in \mathbb{N}\}$ such that $lim_n \mu(V_n) = 0$ and there is a primitive recursive function f such that, for each p, $\mu(V_{f(p)}) \leq 2^{-p}$.

We observe here that $\cap_n U_n$ will be a Π^0_1 class of measure 0 so that any primitive recursive test is also a Kurtz test. Moroever, since the sequence of measures $\mu(U_n)$ will be primitive recursive, it follows that this is also a Schnorr test.

We say an infinite sequence $X \in \{0,1\}^\omega$ is *Martin-Löf BP random* if X *passes* every primitive recursive test, that is, for every primitive recursive test $(U_n)_{n\geq 0}$, there is some n such that $X \notin U_n$.

By the remarks above, every weakly random real is BP Martin-Löf random.

Proposition 1. *X is BP random if and only if there is no primitive recursive sequence $\langle U_n \rangle$ of clopen sets with $\mu(U_n) = 2^{-n}$ such that $X \in \bigcap_n U_n$.*

Proof. The if direction is immediate. Now suppose that there is a primitive recursive sequence $(V_n)_{n\geq 0}$ such that $\mu(V_n) \leq 2^{-n}$ and $X \in \bigcap_n V_n$. Let $V_n = \bigcup_{\sigma in G_n} [\sigma]$ where $G_n \subseteq \{0,1\}^{\ell(n)}$ for some primitive recursive function $\ell(n)$ where $\ell(n) \geq n$ for all $n \geq 0$. Then $\mu(V_n) = \frac{card(G_n)}{2^{k(n)}} \leq 2^{-k(n)}$. Now define H_n to be G_n together with $2^{k(n)-n} - card(G_n)$ additional strings of length $k(n)$ and let $U_n = \bigcup_{\tau \in H_n} [\tau]$. Then for each n, $X \in U_n$ and $\mu(U_n) = 2^{-n}$.

We will also need the notion of a *weak* primitive recursive test. A *weak* primitive recursive test is a primitive recursive sequence $(U_n)_{n\geq 0}$ where there are primitive recursive functions k and ℓ such that for each n, $U_n = [\tau_{1,n}] \cup [\tau_{2,n}] \cdots \cup [\tau_{k(n,n}]$ where $|\tau_{i,n}| = \ell(n)$ for all i and $\mu(U_{n+1} \cap [\tau]) \leq \frac{1}{2}\mu([\tau])$.

We can convert each primitive recursive test into a weak primitive recursive test as follows. First, we may assume that $U_{n+1} \subseteq U_n$ for each n, since the sequence given by $W_n = \bigcap_{i\leq n} U_i$ is also a primitive recursive test with $\mu(W_n) \leq \mu(U_n) \leq 2^{-n}$. Next suppose $U_n = [\tau_{1,n}] \cup \cdots \cup [\tau_{k(n),n}]$ where there is a primitive recursive function ℓ such that $|\tau_{i,n}| = \ell(n)$ for $1 \leq i \leq k(n)$. Thus each interval $[\tau_{i,n}]$ has measure exactly $2^{-\ell(n)}$. Now the clopen set $U_{\ell(n)+1}$ has a total measure

$< 2^{-\ell(n)-1}$, so that the relative measure of $U_{\ell(n)+1} \cap [\tau_i]$ must be $\leq \frac{1}{2}$. Then we can define a primitive recursive weak test $(V_n)_{n\geq 0}$ as follows. Let $h(0) = 0$ and let $V_0 = U_0$. Then let $h(1) = \ell(0) + 1$ and $V_1 = U_{h(1)}$. In general for $n > 1$, we let $h(n+1) = \ell(h(n)) + 1$ and let $V_{n+1} = U_{h(n+1)}$. Then the sequence $V_0, V_1, \ldots$ will be a weak primitive recursive test. Since the sequence $\{V_n : n \in \mathbb{N}\}$ is a subsequence of the original sequence $\{U_m : m \in \mathbb{N}\}$, it follows that $\bigcap_n V_n = \bigcap_n U_n$, so that X passes the weak test $\{V_n : n \in \mathbb{N}\}$ if and only if it passed the original test.

It follows that a real X passes every primitive recursive test, then it certainly it passes every weak primitive recursive test. Conversely, if X fails some primitive recursive test, then the argument above shows that it also fails some weak test. Hence we conclude the following.

Proposition 2. *X is Martin-Löf primitive recursively random if and only if it passes every weak primitive recursive test.* □

Kolomogorov BP random.

Let $C_M(\tau)$ be the length $|\sigma|$ of the shortest string σ such that $M(\sigma) = \tau$, that is, the length of the shortest M-description of τ. Notice that we are using plain and not prefix-free complexity. We say that X is primitive recursively compressed by M if there exist primitive recursive functions M and f such that, for every c, $C_M(X \upharpoonright f(c)) \leq f(c) - c$. Our definition X being primitive recursively compressed is a natural analogue for primitive recursive functions of the usual definition of Kolmogorov randomness, which says that, for every c there exists n such that $C_M(X \upharpoonright n) \leq n - c$. Of course, one defines Kolomogorov randomness in terms of prefix-free complexity K_M since there are no infinite Kolmogorov random sequences for plain complexity. We use plain complexity here since every primitive recursive function is total so that there are no prefix-free machines. Later, we will consider a version of prefix-free complexity for primitive recursive functions.

We say that infinite sequence $X \in \{0,1\}^\omega$ is *Kolmogorov BP random* if it cannot be primitive recursively compressed by any primitive recursive machine M.

We also want to consider so-called *process machines* and the resulting notion of process complexity. Let M be a partial computable function on $\{0,1\}^*$. M is said to be a *process machine* if, whenever $\tau \preceq \tau'$ and $\tau, \tau' \in Dom(M)$, then $M(\tau) \preceq M(\tau')$. M is a *strict process machine* if, whenever $\tau \prec \tau'$ and $\tau' \in Dom(M)$, then $\tau \in Dom(M)$ and $M(\tau) \preceq M(\tau')$, that is, M is extension-preserving. Finally, a strict process machine M is a *quick process machine* if M is total and there is an order function h such that, for all $\tau \in \{0,1\}^*$, $|M(\tau)| \geq h(|\tau|)$. We will say that a strict process machine M is a *quick BP process machine* if M is primitive recursive and there is a primitive recursive order function h such that, for all $\tau \in \{0,1\}^*$, $|M(\tau)| \geq h(|\tau|)$.

The definition of a process machine is due to Levin and Zonkin [26] and a similar notion was defined by Schnorr [34]. Day [13] gives characterizatiions of

computable randomness, Schnorr randomness, and weak randomness using quick process machines. We will show that X is Kolmogrov BP random if and only if X cannot be primitive recursively compressed by a quick BP process machine.

Martingale BP random.

A primitive recursive martingale d is a primitive recursive function $d : \{0,1\}^* \to \mathbb{Q} \cap [0, \infty]$ such that for all $\sigma \in \{0,1\}^*$, $d(\sigma) = \sum_{a \in \{0,1\}} d(\sigma^\frown a)/card(\Sigma)$. Of course, any primitive recursive martingale is also computable martingale. We say that the martingale d *succeeds primitive recursively on* X if there is a primitive recursive function f such that, for all n, $d(X \upharpoonright f(n)) \geq 2^n$. (Of course, we could replace 2^n here with any primitive recursive function which is increasing to infinity.) In general, a martingale d is said to succeed on X if $\limsup_n d(X \upharpoonright n) = \infty$, that is, for every n, there exists m such that $d(X \upharpoonright m) \geq 2^n$. Thus our definition is an effectivization of the usual definition where there is primitive recursive function f which witness that d will return 2^n at some point for every n. We say that X is *martingale BP random* if there is no primitive recursive martingale which succeeds primitive recursively on X. If X is *not* BP martingale random, then there is a computable martingale which succeeds primitive recursively on X and thus certainly succeeds on X, so that X is not computably random. Hence every computably random real is also a martingale BP random real.

Our definition of martingale BP random real has the following equivalent formulations.

Proposition 3. *The following are equivalent:*

(1) *X is BP martingale random*
(2) *There do not exists a primitive recursive martingale d and a primitive recursive function f such that, for every n, there exists $m \leq f(n)$ such that $d(X \upharpoonright m) \geq 2^n$.*
(3) *There do not exist a primitive recursive martingale d and primitve recursive function f such that $d(X \upharpoonright m) \geq 2^n$ for all $m \geq f(n)$.*

Proof. Our proof uses the idea of a *savings account* as formulated in [18, 32]. That is, if we have a martingale and function as in (2), then we can modify the martingale so that whenever $d(\tau) \geq 2^{n+1}$ but $d(\sigma) < 2^{n+1}$ for all proper initial seqments of τ, then we put aside 2^n and only bet with the other half of our capital. This means that we can never drop below 2^n in the future. Thus if we use the function $f'(n) = f(n+1)$, we will satisfy condition (3) and hence satisfy (1) as well.

Our main result in this section is to show the three versions of BP random described above are equivalent.

Theorem 1. *The following statements are equivalent for $X \in \Sigma^N$:*

(1) *X is Martin-Löf BP random.*
(2) *X is Kolmogorov BP random.*

(3) *X is quick process BP random.*

Proof. The implication from (2) to (3) is immediate.

(1) implies (2): Suppose X is not Kolmogorov BP random. Then there exist primitive recursive M and f such that, for every c, $C_M(X \upharpoonright f(c)) \leq f(c) - c - 1$.

Let $U_c = \{X : C_M(X \upharpoonright f(c)) \leq f(c) - c - 1\}$. This is certainly a uniformly primitive recursive sequence of clopen sets. That is, given c, compute $M(\sigma)$ for all σ with $|\sigma| \leq f(c) - c - 1$ and let

$$G_c = \{M(\sigma) : \sigma \in \{0,1\}^{\leq f(c)-c-1}\} \cap \{0,1\}^{f(c)}$$

and $U_c = \bigcup_{\tau \in G_c} [\tau]$. Clearly, $(U_c)_{c \geq 0}$ is a primitive recursive sequence of clopen sets.

We claim that $\mu(U_c) \leq 2^{-c}$. That is, fix c and let $U_c = [\tau_1] \cup [\tau_2] \cup \cdots \cup [\tau_k]$, for distinct $\tau_i \in \{0,1\}^{f(c)}$. Thus there exist $\sigma_1, \ldots, \sigma_k$ such that, for $i = 1, \ldots, k$, $|\sigma_i| \leq f(c) - c - 1$ and such that $M(\sigma_i) = \tau_i$. Since there are only $2^{f(c)-c} - 1$ strings of length $\leq f(c) - c - 1$, it follows that $k \leq 2^{f(c)-c}$. Since for each i, $\mu([\tau_i]) = 2^{-f(c)}$, it follows that

$$\mu(U_c) = k \cdot 2^{-f(c)} \leq 2^{f(c)-c} \cdot 2^{-f(c)} = 2^{-c}.$$

By assumption, $X \in U_c$ for all $c \geq 0$ so that X is not Martin-Löf BP random.

(3) implies (1): Suppose that X is not Martin-Löf BP random. Thus there exist primitive recursive functions g, k, and f so that for all $c \geq 0$, $g(c)$ is a code of a finite set $G_c \subseteq \{0,1\}^{f(c)}$ with cardinality $k(c)$, such that if $U_c = [G_c]$, then $\mu(U_c) \leq 2^{-c}$ and $X \in \bigcap_{c>0} U_c$. Furthermore, we may assume by Proposition 5 that this is a weak test, so that, for each $\sigma \in G_c$, $\mu([\sigma] \cap U_{c=1}) < \frac{1}{2}$. We may assume without loss of generality that for each c, $f(c+1) - (c+1) > f(c) - c$. This is because we may always break each $[\tau]$ into $[\tau^\frown 0] \cup [\tau^\frown 1]$ to increase $f(c)$ by one, if necessary.

We will define a quick process BP machine M such that $C_M(X \upharpoonright f(c) \leq f(c) - c$ for all c in stages as follows.

At stage one, we have $\mu(U_1) \leq \frac{1}{2}$ and , since $\mu(U_1) = k(1) \cdot 2^{-f(1))}$, it follows that $k(1) \leq 2^{f(1)-1}$. Now let $G_1 = \{\tau_1, \ldots, \tau_{k(1)}$, take the lexicographically first k strings $\sigma_{1,c}, \ldots, \sigma_{k(c),c}$ of length $f(1) - 1$ and define $M(\sigma_{i,c}) = \tau_{i,c}$. To make M a total function, the remaining strings of length $f(1) - 1$ are all be mapped to $0^{f(1)}$ and all strings of length $< f(1) - 1$ are mapped to $\emptyset$.

By assumption $X \in U_1$, so that $X \upharpoonright f(1) = \tau_i = M(\sigma_i)$ for some $i$and it follows that $C_M(X \upharpoonright f(1) = f(1) - 1$. Observe that for all strings σ of length $< f(1) - 1$, $M(\sigma)| = 0$ and for all strings σ of length $f(1) - 1$, $M(\sigma)| = f(1)$. Thus we define $h(m) = 0$ for $m < f(1) - 1$ and we define $h(f(1) - 1) = f(1)$.

After stage c, we have defined $M(\sigma)$ for all strings σ of length $\leq f(c) - c$ so that M is extension-preserving and such that, for each $b \leq c$ and each $\tau \in G_b$, there exists σ of length $f(b) - b$ with $M(\sigma) = \tau$. Furthermore, for any σ, if $f(b-1) - b + 1 \leq |\sigma| < f(b) - b$, then $|M(\sigma)| = f(b)$ and also if $|\sigma| = f(c) - c$, then $|M(\sigma)| = f(c)$.

At stage $c+1$, we extend M to all strings σ with $f(c) - c < |\sigma| \leq f(c+1) - c - 1$ as follows. For each ν of length $f(c) - c$ we work on the extensions of ν independently as follows. We first let $M(\sigma) = M(\nu)$ for any extension of ν of length $< f(c+1) - c - 1$.If $M(\nu) \notin G_C$, then $M(\sigma) = M(\nu)^\frown 0^{f(c+1)-1-f(c)}$. Next we let $H_\nu = \{\rho \in \{0,1\}^{f(c+1)-1-f(c)} : M(\nu)^\frown \rho \in G_{c+1}\}$. Then $\mu(H_\nu) \leq \frac{1}{2}$. Thus we may proceed as at stage one to define $M_\nu(\alpha)$ forall strings α of length $\leq f(c+1) - 1 - f(c)$. Finally let $M(\nu^\frown \alpha) = M(\nu)^\frown M_\nu(\alpha)$. It is clear that M continues to be extension-preserving. For any $\tau \in G_{c+1}$, we have $\tau = M(\nu)^\frown \rho$ for some $\rho \in H_\nu$ and it follows that $\rho = M_\nu(\alpha$ for some α of length $f(c) - c$, so that $M(\nu^\frown \alpha) = \tau$. Finally, we have for any σ, if $f(c) - c \leq |\sigma| < f(c+1) - c - 1$, then $|M(\sigma)| = f(c)$ and also if $|\sigma| = f(c+1) - c - 1$, then $|M(\sigma)| = f(c+1)$.

To see that M is a primitive recursive function, observe that since $f(c+1) - c - 1 > f(c) - c > 0$ for all c, we have $f(c) - c > c$. Thus, given a string σ of length m, we need only check $c < m$ to find the least c such that $m \leq f(c) - c$. Then we simply run the process above for c steps to compute $M(\sigma)$.

To verify that M is a quick process machine, define the function h as follows so that $|M(\tau)| \geq h(|\tau|)$ for all τ. First let $h_1(m)$ be the least $c \leq m$ such that $m < f(c+1) - c - 1$ and then let $h(m) = f(h_1(m)$.

By assumption $X \in U_c$ for every c, so that $X \upharpoonright f(c) = \tau$ for some $tau \in G_c$ and hence $M(\sigma) = \tau$ where $|\sigma| = f(c) - c$. It follows that $C_M(X \upharpoonright f(c)) = f(c) - c$.

Hence, X is not quick process BP random.

Theorem 2. *The following statements are equivalent for $X \in \Sigma^N$:*

(1) *X is Martin-Löf BP random.*
(2) *X is martingale BP random.*

Proof. **(1) implies (2)**: Suppose that X is not martingale BP random. Then there is a primitive recursive martingale d which succeeds primitive recursively on X, so that there is a primitive recursive function f such that, for all n, $d(X \upharpoonright f(n)) \geq 2^n$. Let $G_n = \{\tau \in \{0,1\}^{f(n)} : d(\tau) \geq 2^n\}$ and let $U_n = \bigcup_{\tau \in G_n} [\tau]$. Since d and f are primitive recursive, it follows that the sequence $(U_n)_{n \geq 0}$ is a primitive recursive sequence of clopen sets. Certainly $X \in \cap_n U_n$.

Recall that for martingales that $\sum_{|\tau|=m} d(\tau) \leq 2^m$. It follows that there are at most $2^{f(n)-n}$ strings $\tau \in \{0,1\}^{f(n)}$ such that $d(\tau) \geq 2^n$. For each such τ, $\mu([\tau]) = 2^{-f(n)}$. Thus the measure $\mu(U_n) \leq 2^{f(n)-n} \cdot 2^{-f(n)} = 2^{-n}$.

Thus $(U_n)_{n \geq 0}$ is a primitive recursive test so that X is not BP Martin-Löf random.

(2) implies (1): Suppose X is not BP Martin-Löf random. Then $X \in \bigcap_n U_n$, where $(U_n)_{n \geq 0}$ is a weak primitive recursive test. Let $f(n)$ be the length of the strings $\tau_{i,n}$ such that $U_n = [\tau_{1,n}] \cup \cdots \cup [\tau_{k(n),n}]$.

We recursively define our martingale d as follows. For $n = 1$, and given $U_1 = [\tau_{1,1}] \cup \cdots \cup [\tau_{k(1),1}]$, we let $d(\tau_{i,1}) = \frac{2^{f(1)}}{k}$ for $i = 1, \ldots, k$. If $\tau \in \{0,1\}^{f(1)} - \{\tau_{1,1}, \ldots, \tau_{k(1),1}\}$, then we let $d(\tau) = 0$. Since $\mu(U_1) \leq \frac{1}{2}$, it follows that $k \leq$

$2^{f(1)-1}$ and therefore $d(\tau_{i,1}) \geq 2$ for each i. Moroever, $\sum_{\tau\in\{0,1\}^{f(1)}} d(\tau) = k \cdot \frac{2^{f(1)}}{k} = 2^{f(1)}$. Now work backwards using the martingale equation $d(\sigma) = \frac{1}{2}(d(\sigma^\frown 0)+d(\sigma^\frown 1)$ to define $d(\sigma)$ for all σ of length $\leq f(1)$. It follows by induction that for all $j \leq f(1)$, $\sum_{\tau\in\{0,1\}^j} d(\tau) = 2^j$ so that, in particular, $d(\emptyset) = 1$.

Now suppose that we have defined $d(\tau)$ for all τ with $|\tau| \leq f(n)$ such that, for $\tau \in G_n$, $d(\tau) \geq 2^n$. Then we will show how to extend d to strings of length $\leq f(n+1)$. For σ of length $f(n)$, we will define $d(\sigma^\frown\tau)$ for all τ of length $f(n+1) - f(n)$. If $d(\sigma) = 0$, then we simply let $d(\sigma^\frown\tau) = 0$ for all τ. Now fix $\sigma \in G_n$ with $d(\sigma) \geq 2^n$ and consider $G = \{\tau : \sigma^\frown\tau \in G_{n+1}\}$.

Since we have begun with a weak test, it follows that $\mu([G]) \leq \frac{1}{2}$. Thus we may proceed as in the first case where $n = 1$ to define a martingale m such that $m(\sigma) = 1$ and $m(\tau) \geq 2$ for all $\tau \in G$. Now extend the definition of d to the strings below σ by defining $d(\sigma^\frown\tau) = d(\sigma) \cdot m(\tau)$. Since $d(\sigma) \geq 2^n$ and, for $\tau \in G$, $m(\tau) \geq 2$, it follows that for $\sigma^\frown\tau \in G_{n+1}$, $d(\sigma^\frown\tau) \geq 2^{n+1}$. It is easy to see that this extension obeys the martingale equality, since, for any τ,

$$d(\sigma^\frown\tau) = d(\sigma)\cdot m(\tau) = d(\sigma)\cdot\frac{1}{2}(m(\tau^\frown 0)+m(\tau^\frown 1)) = \frac{1}{2}\cdot(d(\sigma\tau^\frown 0)+d(\sigma^\frown\tau^\frown 1)).$$

Since $X \in \cap_n U_n$, it follows that $d(X \upharpoonright f(n)) \geq 2^n$ for each n and hence d succeeds primitive recursively on X.

It is clear that from a given string σ, this defines a primitive recursive procedure to compute $d(\sigma)$. The first step is to compute $f(n)$ for $n \leq |\sigma|$ until we find n so that $|\sigma| \leq f(n)$. Then we look for an extension τ of σ of length $f(n)$. If there is none, then $d(\sigma) = 0$. If there is one, then we follow the procedure outlined above to compute $d(\sigma \upharpoonright f(i))$ for $i \leq n$, and then $d(\tau)$, and finally we backtrack using the martingale inequality to compute $d(\sigma)$ from $d(\tau)$. Thus d is a primitive recursive martingale so that X is not BP martingale random.

Given Theorem 1, we define an $X \in \{0,1\}^\omega$ to be *BP random* if and only if X is Martin-Löf BP random. Since every BP test is also a Kurtz test and a computable test, it follows that in fact all Kurtz random and all computably random reals are BP random.

It is clear that no primitive recursive set can be BP random. It was shown by Jockusch [20] that Kurtz random sets are *immune*, that is, they do not include any c.e. subsets. Here is a version of that result for BP randomness.

Proposition 4. *If A is BP random, then for any increasing primitive recursive function f, A does not contain the range of f.*

Proof. Suppose for the contrapositive that A contains the range of f. For each n, let $G_n = \{\sigma \in \{0,1\}^{f(n)} : (\forall i < n)(\sigma(f(i)) = 1)\}$. Then let $U_n = \bigcup_{\tau\in G_n}[\tau]$. It is clear that $\mu([U_n]) = 2^{-n}$ so that $(U_n)_{n\geq 0}$ is a primitive recursive test. But A belongs to each U_n, so that A is not BP random.

Theorem 3. *There is a recursive real which is BP random.*

Proof. Let $(g_e, k_e, \ell_e)_{e\geq 0}$ enumerate all triples of primitive recursive functions. We want to construct a recursive real $X = (X(1), X(2), \ldots)$ such that X passes every primitive recursive test. Thus we need on consider those e such for all n, $g_e(n)$ is the code of a finite set of strings $\{\sigma_{1,n}, \ldots, \sigma_{k_e(n),n}\}$ such that (a) $U_n^{(e)} = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k_e(n),n}]$ is a clopen set with measure $\leq 2^{-n}$, (b) $|\sigma_{i,n}| = \ell_e(n)$ for all $i \leq k(n)$, and (c) $U_{n+1} \subseteq U_n$ for all n.

Then we can construct X in stages.

Stage 0. Compute $g_0(1)$, $k_0(1)$, and $\ell_0(1)$. If $g_0(1)$ is the code of a finite set of strings $\{\sigma_{1,1}, \ldots, \sigma_{k_0(1),1}\}$ such that $U_1 = [\sigma_{1,1}] \cup \cdots \cup [\sigma_{k_0(1),1}]$ is a clopen set with measure $\leq 2^{-1}$ and $|\sigma_{i,1}| = \ell_0(1)$ for all $i \leq k_0(1)$, then let $\sigma \in \{0,1\}^{\ell_0(1)}$ be the lexicographically least string of length $\ell_0(1)$ such that $\sigma \notin U_1$ and let $(X(1), \ldots X(\ell_0(1)) = \sigma$ and $r(0) = \ell_0(1)$. Otherwise, let $r(0) = 1$ and $X(1) = 0$.

Stage s+1. Assume that we have defined $r(0) < \ldots < r(s)$ and $(X(1), \ldots, X(r(s))$ such that for all $i \leq s$, either
(I) it is the not the case that $g_i(r(i))$ is the code of a finite set of strings $\{\sigma_{1,i}, \ldots, \sigma_{k_i(i),i}\}$ such that $U_i = [\sigma_{1,i}] \cup \cdots \cup [\sigma_{k_i(i),i}]$ is a clopen set with measure $\leq 2^{-i}$ and $|\sigma_{i,1}| = \ell_i(i)$ for all $i \leq k_i(i)$ or
(II) $g_i(r(i))$ is the code of a finite set of strings or $\{\sigma_{1,i}, \ldots, \sigma_{k_i(i),1}\}$ such that $U_i = [\sigma_{1,i}] \cup \cdots \cup [\sigma_{k_i(i),i}]$ is a clopen set with measure $\leq 2^{-i}$ and $|\sigma_{i,1}| = \ell_i(i)$ for all $i \leq k_i(i)$ and $(X(0), \ldots, X(r(i))) \notin U_i$.

First suppose that $g_{s+1}(2r(s))$ is the code of a finite set of strings $\{\sigma_{1,s+1}, \ldots, \sigma_{k_{s+1}(s+1),s+1}\}$ such that $U_{s+1} = [\sigma_{1,s+1}] \cup \cdots \cup [\sigma_{k_{s+1}(s+1),s+1}]$ is a clopen set with measure $\leq 2^{-2r(s)}$ and $|\sigma_{i,1}| = \ell_{s+1}(s+1)$ for all $i \leq k_{s+1}(s+1)$. It follows that $\ell_{s+1}(s+1) \geq 2r(s)$. Moveover the measure of the set of all stings of τ which extend is $2^{-r(s)}$. Thus there must be an extension σ of $(X(1), \ldots, (X(r(s))$ of length $\ell_{s+1}(r(s))$ such that $\sigma \notin U_{s+1}$. Then let $r(s+1) = \ell_{s+1}(r(s))$ and set $(X(1), \ldots X(r(s+1))) = \sigma$. Otherwise, set $r(s+1) = 2r(s)$ and set $X(1), \ldots X(r(s+1))) = (X(0), \ldots, X(r(s)) \frown 0^{r(s)}$.

It is easy to see that our construction is completely effective so that $X = (X(1), X(2), \ldots)$ will be computable real. Now if e is such for all n, $g_e(n)$ is the code of a finite set of strings $\{\sigma_{1,n}, \ldots, \sigma_{k_e(n),n}\}$ such that (i) $V_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k_e(n),n}]$ is a clopen set with measure $\leq 2^{-n}$, (ii) $|\sigma_{i,n}| = \ell_e(n)$ for all $i \leq k(n)$, and (iii) $V_{n+1} \subseteq V_n$ for all n, then our construction ensures that $(X(1), \ldots, X(r(e)))$ $/in V_{g_e(r(e))}$. Since $V_0 \supseteq V_1 \supseteq \cdots$, it follows that $X \notin \bigcap_{n\geq 0} V_n$. This X passes all primitive recursive tests and, hence, X is BP random.

Next we show that BP random reals satisfy the following analogue of Ville's Theorem.

Theorem 4. *Let $X \in \{0,1\}^n$ be BP random and let g be a primitive recursive increasing function. Then the sequence $X(g(n) : n \in \mathbb{N}\}$ is also BP random.*

Proof. Let $Y(n) = X(g(n))$ and suppose by way of contradiction that Y is not BP random. Let $(U_n)_{n\geq 0}$ be a primitive recursive test such that $Y \in U_n$ for all n. That is, suppose that there are primitive recursive functions a, b, and c such that

1. $U_{n+1} \subseteq U_n$ for all n,
2. $\mu(U_n)$, is $\leq 2^{-n}$ for all n, and
3. for all n, $a(n)$ is the code of a finite set strings $\{\sigma_{1,n}, \ldots, \sigma_{b(n),n}\}$ such that $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{b(n),n}]$ and $|\sigma_{i,n}| = c(n) + 1$ for all $1 \leq i \leq b(n)$.

For any string $\tau = \tau_1 \ldots \tau_{g(c)}$ of length $c(n)$, let $\tau^{(1)}, \ldots, \tau^{(2^{g(c(n))-c(n)})}$ be a list of the $2^{g(c(n))-c(n)}$ strings such that $(\tau^{(i)}_{g(1)}\tau^{(i)}_{g(2)} \ldots \tau^{(i)}_{g(c(n))}) = \tau$. Then define

$$V_n = \{X : (X(g(1), \ldots, X(g(c(n)))\} \in U_n\} = \bigcup_{i=1}^{b(n)} \bigcup_{j=1}^{2^{g(c(n))-c(n)}} [\tau^{(j)}_{i,n}].$$

It is easy to see that $\mu(U_n) = \mu(V_n)$ and the $(V_n)_{n\geq 1}$ is a primitive recursive test. But then $X \in \bigcap_{n\geq 1} V_n$ which would violate the fact that X is BP random. Thus Y must be BP random.

2.1 Prefix-free primitive recursive

Kolmogorov complexity and randomness are usually studied for prefix-free machines. Primitive recursive functions are total, but we can consider partial primitive recursive functions by adding a new symbol, say ∞ for divergence. The usual enumeration of strings is given by $\emptyset, (0), (1), (01), (10), (11), \ldots$ so that the nth string $1^\frown\sigma_n$ is the binary representation of $n + 1$. Then for any primitive recursive function $\phi : \mathbb{N} \to \mathbb{N}$, we can define a partial primitive recursive function $M_\phi :\to$ so that when $\phi(m) = n + 1$, $M_\phi(\sigma_m) = \sigma_n$ and when $\phi(m) = 0$, $M_\phi(\sigma_m) = \infty$. Then as usual M_ϕ is said to be *prefix-free* if whenever $M_\phi(\sigma)$ converges and $\sigma \prec \tau$, then $M_\phi(\tau) = \infty$.

Now define X to be *prefix-free BP random* if there do not exist a prefix-free primitive recursive function M and a primitive recursive function f such that, for all c, $C_M(X \upharpoonright f(c) \leq f(c) - c$.

Proposition 5. *A real X is BP random if and only if it is prefix-free BP random.*

Proof. Certainly if X is BP random then it is prefix-free BP random. Suppose that X is not BP random. Then by Theorem 1, there is a primitive recursive test $\{U_c : c \in \mathbb{N}\}$ such that $X \in \bigcap_c U_c$. We may assume (by replacing U_c with U_{2c} if necessary) that in fact $\mu(U_c) \leq 2^{-2c}$.

Define the primitive recursive function f so that $U_c \subseteq \{0,1\}^{f(c)}$.

Then, for each c, U_c is a clopen set with measure $\leq 2^{-2c}$ of the form $U_c = [\tau_1] \cup [\tau_2] \cup \cdots [\tau_k(c)]$, where each τ_i has length $f(c)$.

We may assume as before that, for each c, $f(c+1) - (c+1) > f(c) - c$.

We will now recursively define a prefix-free primitive recursive function M such that $C_M(X \upharpoonright f(c) \leq f(c) - c$ for all c.

Since $\mu(U_1) = k(1) \cdot 2^{-f(c))} \leq \frac{1}{4}$, it follows that $k(1) \leq 2^{f(1)-2}$. Now take the lexicographically first $k(1)$ strings $\sigma_1, \ldots, \sigma_k$ of length $f(1) - 1$ and define $M(\sigma_i) = \tau_i$. M is undefined for all other strings of length $< f(1)$. Note that $M(\sigma) = \infty$ for at least half of the strings of length $f(1) - 1$

Now suppose that we have defined M, in a prefix-free way, for strings of length $\leq f(c) - c$ so that for each $n \leq c$, and each τ of length $f(n)$, there is some string of length $f(n) - n$ such that $M(\sigma) = \tau$ and furthermore, such that $M(\sigma) = \infty$ for at least 2^{-c} of the strings of length $f(c) - c$.

Now let $U_{c+1} = \tau_1] \cup [\tau_2] \cup \cdots \cup [\tau_k]$, where $k \leq 2^{f(c+1)-2c-2}$. By assumption, there were at least $2^{-c} \cdot 2^{f(c)-c}$ strings σ of length $f(c) - c$ such that M has not been defined on any initial segment of σ. Since each of these has $2^{f(c+1)-f(c)-1}$ extensions of length $f(c+1) - c - 1$, there are $2^{f(c+1)-2c-1}$ strings available of length $f(c+1)-c-1$. Select the lexicographically first k of these and map them to $\tau_1, \ldots, \tau_k$. This will leave at least $2^{f(c+1)-c-1} \cdot 2^{-c}$

Now take the lexicographically first k strings $\sigma_1, \ldots, \sigma_k$ of length $f(c+1) - c - 1$, which do not extend any strings on which M has already been defined, and define $M(\sigma_i) = \tau_i$. Again let M be undefined on all other strings of length $f(c+1) - c - 1$ and on all strings with lengths strictly between $f(c) - c$ and $f(c+1) - c - 1$.

By assumption $X \in U_c$ for every c, so that $X \upharpoonright f(c) = \tau_i$ for some i and hence $M(\sigma_i) = \tau_i = X \upharpoonright f(c)$. Since $|\sigma_i| = f(c) - c$, it follows that $C_M(X \upharpoonright f(c)) = f(c) - c$.

It remains to be checked that M is indeed a primitive recursive function. Observe that since $f(c+1) - c - 1 > f(c) - c > 0$ for all c, we have $g(c) - c > c$. Thus, given a string σ of length m, we need only check $c < m$ to see whether $m = g(c) - c$ for some c and this can be done primitive recursively. If $m = g(c) - c$, then we proceed as above to determine whether $\sigma = \sigma_i$ where $M(\sigma_i) = \tau_i$ or not. If not, or if $m \neq g(c) - c$ for any c, then we just let $M(\sigma) = 0$.

2.2 Statistical Tests

It is important to see to what extent the BP random sets are statistically random. We begin with a positive result.

Theorem 5. *Let A be a BP random set. For any increasing primitive recursive function f and any $\epsilon > 0$, there is some n such that $|\frac{|card(A \cap f(n))}{f(n)} - \frac{1}{2}| \leq \epsilon$.*

Proof. This follows from the law of large numbers (Chernoff's Lemma [27], p. 61).

Corollary 1. *For any BP random set A, if $\lim_n \frac{|card(A \cap n)}{n}$ exists, then it equals $\frac{1}{2}$.*

On the other hand, BP random sets do not have be stochastic.

Theorem 6. *There exists a computable, BP random set A such that $lim_n \frac{card(A \cap n)}{n}$ does not exist.*

Proof. To construct such a set A, just modify the proof of Theorem 2 by adding long strings of 0's and long strings of 1's (in alternation) after satisfying each requirement. Then we can make the density go below $\frac{1}{3}$ and then above $\frac{2}{3}$ infinitely often.

2.3 Relative randomness

Recall that the set of primitive recursive functions consists the set of function $f : \mathbb{N}^n \to \mathbb{N}^m$ that includes the base functions (i) the constant functions $f(x_1, \ldots, x_n) = m$ for all $n \geq 1$ and $m \geq 0$, (ii) the successor function $s(x) = x + 1$, and the projection functions $f_i(x_1, \ldots, x_n) = x_i$ for all $1 \leq i \leq n$ and is closed composition and primitive recursion. That is, if $g_1, \ldots, g_k$ are m-ary primitive recursive functions and f is a k-ary primitive recursive function, then $h(x_1, \ldots, x_m) = f(g_1(x_1, \ldots, x_m), \ldots g_k(x_1, \ldots, x_m))$ is primitive recursive and if f is a k-ary primitive recursive function and g is a $k + 2$-ary primitive recursive function, then the $k + 1$-ary function H is primitive recursive where H is defined by primitive recursion from f and g by

1. $H(0, x_1, \ldots, x_k) = f(x_1, \ldots, x_k)$ and
2. $H(S(y), x_1, \ldots, x_k) = g(y, H(y, x_1, \ldots, x_k), x_1, \ldots, x_k)$.

Given a recursive real $Y = (Y(0), Y(1), \ldots,)$, the primitive recursive functions relative to Y are obtained by simply adding the function $M(n, Y) = Y(n)$ to the base functions and closing under composition and primitive recursion. Then we can define a real $X = (X(0), X(1), \ldots,)$ to be Martin-Löf BP random relative to Y, Kolmogorov BP random relative to Y, and martingale BP random relative to Y by replacing the primitive recursive functions in the definitions of Martin-Löf BP random, Kolmogorov BP random, and martingal BP random by primitive recursive functions relative to Y, respectively.

It is easy to see that we can simply relativize the proof of Theorem 1 to prove the following.

Theorem 7. *The following are equivalent for $X, Y \in \Sigma^N$:*

(1) X is Kolmogorov BP random relative to Y
(2) X is Martin-Löf BP random relative to Y
(3) X is martingale BP random relative to Y.

Then we have the following analogue of van Lambalgen's Theorem. Recall that if $A, B \subseteq \mathbb{N}$, then $A \oplus B = \{2x : x \in A\} \cup \{2x + 1 : x \in B\}$.

Theorem 8. *For any sets $A, B \subseteq \mathbb{N}$, $A \oplus B$ is BP random if and only if B is BP random relative to A and A is BP random.*

Proof. First we show that $A \oplus B$ is BP random, then B is BP random relative to A. That is, suppose that B is not BP random relative to A so that there is a primitive recursive test $(U_n^A)_{n\geq 0}$ relative to A such that $B \in \bigcap_{n\geq 0} U_n^A$. We can assume that $\mu(U_n^A) = 2^{-n}$. Then let $V_n = \{X \oplus Y : X, Y \in \{0,1\}^\omega \text{ and } Y \in U_n^X\}$. It is easy to see that $(V_n)_{n\geq 0}$ is primitive recursive test such that $\mu(V_n) = \int U_n^X dX = 2^{-n}$. But then $A \oplus B \in \bigcap_{n\geq 0} V_n$ so that $A \oplus B$ is not BP random. Since $A \oplus B$ is BP random and $\{2n : n \in \mathbb{N}\}$ and $\{2n+1 : n \in \mathbb{N}\}$ are the ranges of increasing primitive recursive functions, it also follows that A and B are BP random.

Next we show that A is BP random and B is BP random relative to A, then $A \oplus B$ is BP random. Suppose that $A \oplus B$ is not BP random. Then there exists a primitive recursive test $(U_n^B)_{n\geq 0}$ such that $A \oplus B \in \bigcap_{n\geq 0} U_n$. That is, there are primitive recursive functions g, k, ℓ such that for all $n \geq 0$, $g(n)$ is codes a finite set of strings $\{\sigma_{1,n}, \ldots, \sigma_{k(n),n}\}$ such that $\sigma_{i,n}| = c(n)$ for all i and $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k(n),n}]$. By passing to a subsequences, we may assume that $\mu(U_n) = 2^{-2n}$. Now let

$$V_n = \{X : \mu(\{Y : X \oplus Y \in U_n\}) > 2^{-n}\}$$

Note to determine if $X \in V_n$, let $\alpha = (X(0), \ldots, X(c(n)-1))$ and consider the set of all $\beta = (Y(0), \ldots, Y(c(n)-1)$. Then we can determine in primitive recursively whether $\alpha \oplus \beta \in (X(0), Y(0), \ldots, X(c(n)-1), Y(c(n)-1))$ in U_n since $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k(n),n}]$. is generated by strings of length $c(n)$. It follows that $(V_n)_{n\geq 0}$ is a primitive recursive test. It must be the case that $\mu(V_n) \leq 2^{-n}$ for all n since otherwise $\mu(U_n) > \mu(V_n)2^{-n} > 2^{-n}2^{-n} = 2^{-2n}$. Since A is BP random, it must be the case that $A \in U_n$ for only finitely many n. That is, for all but finitely many n, $\mu(\{Y : A \oplus Y \in U_n\}) \leq 2^{-n}$. Thus put $V_n^A = \{Y : A \oplus Y \in W_n\}$. Then $\mu(V_n^A) \leq 2^{-n}$ for all but finitely many n. Thus there will be an m large enough so that $\mu(V_n^A) \leq 2^{-n}$ for all $n \geq m$. Then we can define a primite recursive test $(W_n)_{n\geq 0}$ relative to A by setting $W_n^A = V_{n+m}^A$ for $n \geq 0$. It will then follow that $B \in \bigcup W_n^A$ so that B is not BP random relative to A.

3 Polynomial-Space Bounded Pseudorandomness

Let $PSPACE^*$ be the family of functions computable in polynomial space where we include the space needed to write the output and let $PTIME$ be the family of functions computable in polynomial time. Then we can define the three notions of PSPACE BP random reals.

Martin-Löf BPS random.

A $PSPACE$ test $(U_n)_{n\geq 0}$ is specified by a pair of functions (G, f) such that $G : \{1\}^* \times \{0,1\}^* \to \{0,1\}$ is a $PSPACE$-function and $f\{1\}^* \to \{1\}^*$ is a strictly length increasing $PTIME$ function such that for each n,

$$G_{n,f} = \{\tau \in \{0,1\}^{\leq |f(1^n)|} : G(1^n, \tau) = 1\} = \{\sigma_{1,n}, \ldots, \sigma_{k(n),n}\}$$

is a set of strings of length $\leq |f(1^n)|$ such that $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k(n),n}]$ is clopen set with measure $\leq 2^{-n}$.

A *weak* $PSPACE$ test $(U_n)_{n\geq 0}$ is specified by a pair (G, f) as above with the additional property that for each n, $\mu(U_{n+1} \cap [\sigma_{i,n}]) \leq \frac{1}{2}\mu([\sigma_{i,n}])$.

We say that X is *Martin-Löf BPS random* if X passes every $PSPACE$ test and is *weakly Martin-Löf BPS random* if X passes every weak $PSPACE$ test.

Kolomogorov BPS random.

An infinite sequence X is *Kolmogorov BPS random* if there do not exist a $PSPACE^*$ function $M : \{0,1\}^* \to \{0,1\}^*$ and a $PTIME$ function $f : \{1\}^* \to \{1\}^*$ such that, for every $n \in \mathbb{N}$, $C_M(X \upharpoonright |f(1^n)|) \leq |f(1^n)| - n$.

Martingale BPS random.

A $PSPACE^*$ martingale $d : \{0,1\} \to \mathbb{Q} \cap [0,\infty]$ succeeds on X if there is a $PTIME$ function $f : \{1\}^* \to \{1\}^*$ such that, for all n, there is some $m \leq |f(1^n)|$ such that $d(X \upharpoonright m) \geq 2^n$. Here we shall think of $\mathbb{Q}\cap[0,\infty]$ as the set of all strings $\sigma 2 \tau$ where $\sigma.\tau$ is the binary expansion of a rational number $r \in \mathbb{Q} \cap [0,\infty]$. We say that X is *martingale BPS random* no $PSACE^*$ martingale succeeds on X.

We now prove two equivalences. First we show that the set of BPS random reals equals the set of Kolomogorov BPS random reals.

Theorem 9. *The following are equivalent for $X \in \{0,1\}^\omega$.*

(1) X is Kolmogorov BPS random.
(2) X is Martin-Löf BPS random.

Proof. **(2) implies (1)**: Suppose that X is not Kolmogorov BPS random. Then there exist a $PSPACE$ function $M : \{0,1\}^* \to \{0,1\}^*$ and a $PTIME$ function $f : \{1\}^* \to \{1\}^*$ such that for every $c \in \mathbb{N}$, $C_M(X \upharpoonright |f(1^c)| \leq |f(1^c)| - c$. Then let $G : \{1\}^* \times \{0,1\}^* \to \{0,1\}$ be computed as follows. Let $G(1^n, \tau) = 0$ if $|\tau| \neq |f(1^n)|$. If $|\tau| = |f(1^n)|$, then in polynomial space, we can search through all the strings σ of length $\leq |f(1^n)| - n$ to see if there is a σ such that $M(\sigma) = \tau$. If there is such a σ, we set $G(1^n, \tau) = 1$ and if there is no such σ, we set $G(1^n, \tau) = 0$. It follows that

$$G_{n,f} = \{\tau : |\tau| = |f(1^n)| \ \&\ (\exists \sigma)(|\sigma| \leq |f(1^n)| - n \ \&\ |M(\sigma)| = \tau\}.$$

Thus if $G_{n,f} = \{\tau_{1,n}, \ldots, \tau_{k(n),n}\}$, then

$$U_n = [\tau_{1,n}] \cup \cdots \cup [\tau_{k(n),n}] = \{X : C_M(X \upharpoonright |f(1^n)|) \leq |f(1^n)| - n\}.$$

We claim that $\mu(U_n) \leq 2^{1-n}$. That is, since there exist $\sigma_{1,n}, \ldots, \sigma_{k(n),n}$ such that for $i = 1, \ldots, k(n)$, $|\sigma_{i,n}| \leq |f(1^n)| - n$ and $M(\sigma_{i,n}) = \tau_{i,n}$ and there are only $2^{|f(1^n)|-n+1} - 1$ strings of length $\leq |f(1^n)| - n$, it follows that $k(n) \leq 2^{|f(1^n)|+1-n}$. For each i, $\mu([\tau_{i,n}]) = 2^{-|f(1^n)|}$. Hence $\mu(U_n) = k(n) \cdot 2^{-|f(1^n)|} \leq 2^{|f(1^n)|+1-n} \cdot 2^{|f(1^n)|} = 2^{1-n}$. It follows that $(U_{n+1})_{n\geq 0}$ is $PSPACE$ test such

that $X \in \bigcap_{n\geq 0} U_{n+1}$. Thus if X is not Kolmogorov BPS random, then X is not Martin-Löf BPS random.

(1) implies (2): Let $X \in \cap_n U_n$, where $(U_n)_{n\geq 0}$ is a $PSPACE$ test. That is, suppose that there is pair of functions (G, f) such that $G : \{1\}^* \times \{0,1\}^* \to \{0,1\}$ is a $PSPACE$-function and $f\{1\}^* \to \{1\}^*$ is a $PTIME$ function such that for each n, $G_{n,f} = \{\tau \in \{0,1\}^{\leq |f(1^n)|} : G(1^n, \tau) = 1\} = \{\sigma_{1,n}, \ldots, \sigma_{\ell(n),n}\}$ is a set of strings of length $\leq |f(1^n)|$ such that $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k(n),n}]$ is clopen set with measure $\leq 2^{-n}$. Now we can replace G by a $PSPACE$ $\overline{G}$ such that $\overline{G}(1^n, \tau) = 0$ if $|\tau| \neq |f(1^n)|$ and if $|\tau| = |f(1^n)|$, then G^* searches the initial seqments σ of τ to see if there is a σ such that $G(1^n, \sigma) = 1$. If there is such a σ, then $\overline{G}(1^n, \tau) = 1$ and otherwise, $\overline{G}(1^n, \tau) = 0$. It follows that $(U_n)_{n\geq 0}$ is a $PSPACE$ test which is specifed by the pair of functions $(\overline{G}, f)$ and

$$\{\tau \in \{0,1\}^{\leq |f(1^n)|} : \overline{G}(1^n, \tau) = 1\} = \{\sigma_{1,n}, \ldots, \sigma_{k(n),n}\}$$

is a set of strings of length $|f(1^n)|$ such that $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k(n),n}]$

We may assume without loss of generality that, for each n, $|f(1^{n+1})| - (n+1) > |f(1^n)| - n$. That is, $|f(1^{n+1})| > |f(1^n)| + 1$. This is because we may always break each $[\tau_i]$ into $[\tau_i{}^\frown 0] \cup [\tau_i{}^\frown 1]$ to increase $|f(1^{n+1})|$ by one, if necessary. That is, if $f(1^n)$ is computed in time on the order of n^r for some fixed r, then we may define $g(1^n)$ by recursion so that $g(1^0) = f(1^0)$ and, for all i, $g(1^{i+1}) = max\{f(1^{i+1}), g(1^i) + 1\}$. Then $g(1^n)$ can be computed in time on the order of n^{r+1}.

Next, we define a $PSPACE$ function M such that $C_M(X \upharpoonright |f(1^n)|) \leq |f(1^n)| - n$ for all $n \in \mathbb{N}$. Since $\mu(U_n) = k \cdot 2^{-|f(1^n|)}$, it follows that $k \leq 2^{|f(1^n)|-n}$. Now take the lexicographically first k strings $\sigma_{1,n}, \ldots, \sigma_{k(n),n}$ of length $|f(1^n)| - n$ and define $M(\sigma_i) = \tau_{i,n}$. To make M a total function, the remaining strings of length $|f(1^n)| - n$ may all be mapped to 0 and all strings not of length $|f(1^n)| - n$ for any $n \in \mathbb{N}$ may also be mapped to 0.

By assumption $X \in U_n$ for every n, so that $X \upharpoonright |f(1^n)| = \tau_{i,n}$ for some i and hence $M(\sigma_{i,n}) = \tau_{i,n} = X \upharpoonright |f(1^n)|$. Since $|\sigma_{i,n}| = |f(1^n)| - n$, it follows that $C_M(X \upharpoonright |f(1^n)|) = |f(1^n)| - n$.

It remains to be checked that M is indeed a $PSPACE$ function. Observe that since $|f(1^{n+1})| - n - 1 > |f(1^n)| - n > 0$ for all n, we have $|f(1^n)| - n > n$. Thus, given a string σ of length m, we need only check $n < m$ to see whether $m = |f(1^n)| - n$ for some n and this can be done in time n^r. If $m = |f(1^n)| - n$, then we enumerate in lexicographic order the strings σ_i of length m, looking for $i \leq k(n)$ such that $\sigma = \sigma_{i,n}$. This only requires space to store the current values of i and of $\sigma_{i,n}$, so can be done in $PSPACE$. If indeed $\sigma = \sigma_{i,n}$ for some $i \leq k(n)$, then $M(\sigma_{i,n}) = \tau_{i,n}$. If not, or if $m \neq |f(1^n)| - n$ for any $n \in \mathbb{N}$, then we just let $M(\sigma) = 0$.

Our next goal is to show that X is martingale BPS random if and only if X is weakly Martin-Löf BPS random. The following lemma about martingales will be needed to help us prove this fact.

Lemma 1. *For any martingale d, any $\sigma \in \{0,1\}^*$ and any pairwise incompatible set H of extensions of σ,*

$$\sum_{\tau \in H} d(\tau) \cdot 2^{-|\tau|} \leq d(\sigma) \cdot 2^{-|\sigma|}.$$

Proof. Let $n = max\{|\tau| : \tau \in H\}$ and note that by the definition of martingales,

$$\sum_{d(\rho):|\rho|=n \ \& \ \sigma \prec \rho} = d(\sigma) \cdot 2^{n-|\sigma|}.$$

For each $\tau \in H$, let $G(\tau) = \{\rho \in \{0,1\}^n : \tau \preceq \rho\}$. Then as above

$$\sum_{\rho \in G(\tau)} d(\rho) = d(\tau) \cdot 2^{n-|\tau|}.$$

Thus we have

$$\sum_{\tau \in H} d(\tau) \cdot 2^{-|\tau|} =$$
$$\sum_{\tau \in H} \sum_{\rho \in G(\tau)} d(\rho) \cdot 2^{-n} \leq \sum \{d(\rho) \cdot 2^{-n} : |\rho| = n \ \& \ \sigma \prec \rho\} = d(\sigma) \cdot 2^{-|\sigma|}.$$

Theorem 10. *The following are equivalent for $X \in \Sigma^N$:*

(1) X is weakly Martin-Löf BPS random;
(2) X is martingale BPS random.

Proof. **(1) implies (2)**: Suppose that there is a $PSPACE^*$ martingale $d : \{0,1\}^* \to (\mathbb{Q} \cap [0,\infty])$ which succeeds on X so that there is a $PTIME$ function $f : \{1\}^* \to \{1\}^*$ such that, for all n, there exists $m \leq |f(1^n)|$ such that $d(X \upharpoonright m) \geq 2^n$. Let r be such that for all $\sigma \in \{0,1\}^*$, $|d(\sigma)| \leq (2 + |\sigma|)^r$. Such an r exists since d is $PSACE^*$ function.

Our proof of this implication will be more difficult than the proof of the corresponding implication for BP randomness since we need to construct a $PSPACE$ weak test that X fails as opposed to a just a $PSACE$ test. Define $G : \{1\}^* \times \{0,1\}^* \to \{0,1\}$ by let $G(1^n, \sigma) = 1$ if $|\sigma| \leq |f(1^n)|$ & $d(\sigma) \geq 2^n$ & $(\forall i < |\sigma|)(d(\sigma \upharpoonright i) < 2^n)$. Note that if $d(\sigma \upharpoonright (|\sigma| - 1)) < 2^{-n}$, then $d(\sigma) < 2^{n+1}$. Since the binary representation of 2^{n+1} is of length $n+1$, d is $PSPACE^*$ function and f is $PTIME$ function, it is easy to see that G is $PSPACE$ function. Thus

$$G_{n,f} = \{\sigma : |\sigma| \leq |f(1^n)| \ \& \ d(\sigma) \geq 2^n \ \& \ (\forall i < |\sigma|)(d(\sigma \upharpoonright i) < 2^n)\}.$$

and $U_n = \bigcup_{\sigma \in G_{n,f}} [\sigma]$. Then $X \in U_n$ for all n by the assumption. By Lemma 1 with $\sigma = \emptyset$, $\sum_{\tau \in G_{n,f}} d(\tau) \cdot 2^{-|\tau|} \leq 1$. Since for all $\tau \in G_{n,f}$, $d(\tau) \geq 2^n$, it follows that

$$\mu([U_n]) = \sum_{\tau \in G_{n,f}} 2^{-|\tau|} \leq 2^{-n}.$$

Now let $V_n = \bigcup_{\tau G_{2n,f}}[\tau]$ for all n. Then $(V_n)_{n\geq 0}$ will be a $PSPACE$ test that X fails. Thus we need only show that the sequence $(V_n)_{n\geq 0}$ is a weak test. We have $\mu(V_n) = \mu(U_{2n}) \leq 2^{-2n}$. For $\sigma \in V_n$, let $H(\sigma) = \{\tau : \sigma \preceq \tau \ \& \ \tau \in V_{n+2}\}$

By Lemma 1,

$$\sum_{\tau\in H(\sigma)} d(\tau)\cdot 2^{-|\tau|} \leq d(\sigma)\cdot 2^{-|\sigma|}.$$

Since $d(\sigma) < 2^{2n+1}$ and for each $\tau \in H(\sigma)$, $d(\tau) \geq 2^{2n+2}$, we obtain

$$\sum_{\tau\in G(\sigma} 2^{2n+2}\cdot 2^{-|\tau|} \leq 2^{2n+1}\cdot 2^{-|\sigma|},$$

so that

$$\mu(\bigcup_{\tau\in H(\sigma)}[\tau]) = \sum_{\tau\in H(\sigma} 2^{-|\tau|} \leq \frac{1}{2}\cdot 2^{-|\sigma|} = \frac{1}{2}\mu([\sigma]).$$

Thus the sequence V_n is a weak $PSPACE$ test as desired. Thus if X is not martingal BPS random, then X is not weakly Martin-Löf BPS random.

(2) implies (1): Suppose that $X \in \bigcap_n U_n$, where $(U_n)_{n\geq 0}$ is a weak bounded $PSPACE$ test. Let $(U_n)_{n\geq 0}$ be specified by a pair of functions (G, f) where $G : \{1\}^* \times \{0,1\}^* \to \{0,1\}$ is a $PSPACE$-function and $f\{1\}^* \to \{1\}^*$ is a $PTIME$ function such that for each n,

$$G_{n,f} = \{\tau \in \{0,1\}^{\leq |f(1^n)|} : G(1^n, \tau) = 1\} = \{\sigma_{1,n}, \ldots, \sigma_{k(n),n}\}$$

is a set of strings of length $\leq |f(1^n)|$ such that for all $n \geq 0$ and $\sigma \in G_{n,f}$, $\mu([\sigma] \cap U_{n+1}) \leq \frac{1}{2}\mu(\sigma)$. Assume that $G_{n,f} = \{\tau_{1,n}, \ldots, \tau_{k(n),n}\}$ so that $U_n = [\tau_{1,n}] \cup \cdots \cup [\tau_{k(n),n}]$. We are not assuming at that all $\tau_{i,n}$ have the same length which will require that our proof be slightly more complicated than the corresponding proof for the primitive recursive case.

Note that $\mu(U_1) \leq \frac{1}{2}$. Let $H = \{\tau \in \{0,1\}^{|f(1)|} : (\exists \sigma \in G_{1,f})(\sigma \preceq \tau)\}$. Then $U_1 = \sum_{\tau\in H}[\tau]$ so that $\mu([H]) = \mu([G_1])$. Then as in the proof of Theorem 1, we let $k = card(H)$ and define a martingale d_1 by letting $d_1(\tau) = \frac{2^{f(1)}}{k}$ for all $\tau \in H$, letting $d_1(\tau) = 0$ for all other $\tau \in \{0,1\}^{f(1)}$, and backtracking using the martingale equation to define $d(\sigma)$ for all σ such that $|\sigma| < |f(1)|$. Since $\mu([H]) = \frac{k}{2^{f(1)}} \leq \frac{1}{2}$, it follows that $d_1(\tau) \geq 2$ for all $\tau \in H$. Hence for $\sigma \in G_{1,f}$, every extension of σ of length $f(1)$ is in H so that $d_1(\sigma) \geq 2$ as desired.

The eventual martingale d will have $d(\sigma) = d_1(\sigma)$ for $\sigma \in G_{1,f}$ and $d(\tau) = 0$ for $\tau \in \{0,1\}^{|f(1)|} - H$, but will not necessarily agree with d_1 on the proper extensions of $\sigma \in G_1$.

By induction assume that we have defined $d(\sigma) \geq 2^n$ for all $\sigma \in G_{n,f}$ and set $d(\tau) = 0$ for all $\tau \in \{0,1\}^{\leq |f(1^n)|}$ such that τ does not extend a string in $G_{1,n}$. Then we can extend the definition to G_{n+1} as in the proof of Theorem 1. That is, we fix $\sigma \in G_n$ and let $G = \{\tau \in G_{n+1,f} : \sigma \preceq \tau\}$. Since we started with a weak test, it follows that $\mu([G]) \leq \frac{1}{2}$. So we can define a martingale m such that $m(\tau) \geq 2$ for all $\tau \in G$ and then let $d(\sigma^\frown\tau) = d(\sigma)\cdot m(\tau)$.

It remains to be seen that the recursive calculation of $d(\sigma)$ can be accomplished by a $PSPACE$ procedure. First observe that we can compute $card(G_n)$ from n in $PSPACE$ as follows. First compute $f(n)$ and then test in turn each $\tau \in \{0,1\}^{|f(1^n)|}$ and keep a count (in binary) of the number of members. Since by assumption we have $f(n) \leq n^c$ for some constant c, each τ to be tested has length $\leq n^c$ so that this can be done in $PSPACE$.

Then we may compute $d(\sigma)$ from a given string σ in $PSPACE$ as follows. The first step is to compute $f(1^n n)$ for $n \leq |\sigma|$ until we find n so that $|\sigma| \leq |f(1^n)|$. Then we look for an extension τ of σ of length $|f(1^n)|$. Since by our definition we have $|f(1^n)| \leq |n|^c = n^c$, this can be done in $PSPACE$. If there is no such τ, then $d(\sigma) = 0$. If there is one, then we follow the procedure outlined above to compute $d(\sigma \upharpoonright |f(1^i)|$ for each $i \leq n$, and then $d(\tau)$. Finally we backtrack using the martingale inequality to compute $d(\sigma)$ from $d(\tau)$.

Process BPS random.

A total $PSPACE$ function $M : \{0,1\}^* \to \{0,1\}^*$ is said to be a BPS quick process machine if there is a $PTIME$ function $g : \{1\}^* \to \{1\}^*$ such that, for any n and any σ with $|\sigma| \geq n$, $|M(\sigma)| \geq n$, where for simplicity we let $g(n)$ denote $|g(1^n)|$.

An infinite sequence X is *process BPS random* if there do not exist a $PSPACE^*$ BPS process machine $M : \{0,1\}^* \to \{0,1\}^*$ and a $PTIME$ function $f : \{1\}^* \to \{1\}^*$ such that, for every $n \in \mathbb{N}$, $C_M(X \upharpoonright |f(1^n)|) \leq |f(1^n)| - n$.

Theorem 11. *The following are equivalent for $X \in \Sigma^N$:*

(1) X is weakly Martin-Löf BPS random;
(2) X is process BPS random.

Proof. **(1) implies (2)** We modify the argument of Levin [26] as found in Day [13]. Suppose that X is not weakly Martin-Löf BPS random and let Let M be a quick process machine and f a $PTIME$ function so that for every n, $C_M(X \upharpoonright f(n)) \leq n - c$. Let g be a $PTIME$ order function so that for any n and any σ, if $|\sigma| \geq g(n)$, then $|M(\sigma)| \geq n$ and hence $g(n) \geq n$. Define the $PSPACE$ martingale d as follows. For any string τ, let $E_\tau = \{\sigma \in \{0,1\}^{g(\tau)} : \tau \preceq M(\sigma)\}$. Then define d by

$$d(\tau) = \frac{card(E_\tau)}{2^{g(|\tau|)-|\tau|}}$$

It follows as in Proposition 2.1 of [13] that d is a martingale. To compute $d(\tau)$ in $PSPACE$, first compute $g(|\tau|)$ and then test in turn all strings σ of length $g(|\tau|)$ for membership in E_τ, that is, compute $M(\sigma)$ and see whether it extends τ. Then we can keep a binary counter to obtain $card(E_\tau$. Now $d(\tau)$ may be expressed as the quotient of $card(E_\tau$ with $2^{g(|\tau|)-|\tau|}$, which has binary length $g(|\tau|) - |\tau| + 1$.

Now suppose that $C_M(X \upharpoonright f(n)) \leq n-c$. Let $\tau = X \upharpoonright f(n)$ and let $M(\sigma) = \tau$ where $|\sigma| \leq n - c$. For any σ' such that $|\sigma'| = g(n)$ and $\sigma \preceq \sigma'$, we have $\tau = M(\sigma) \preceq M(\sigma')$ so that $\sigma' \in E_\tau$. Since $g(n) \geq n \geq |\sigma| + c$, It follows that $card(E_\tau) \geq 2^{g(n)-n+c}$ and therefore $d(\tau) \geq 2^c$.

(2) implies (1) : Let $X \in \cap_n U_n$, where $(U_n)_{n\geq 0}$ is a weak $PSPACE$ test. Then, as in the proof of Theorem 9, There is a $PSPACE$ function t $G : \{1\}^* \times \{0,1\}^* \to \{0,1\}$ and a $PTIME$ function $f\{1\}^* \to \{1\}^*$ such that

$$\{\tau \in \{0,1\}^{\leq |f(1^n)|} : \overline{G}(1^n, \tau) = 1\} = G_n = \{\sigma_{1,n}, \ldots, \sigma_{k(n),n}\}$$

is a set of strings of length $|f(1^n)|$ such that $U_n = [G_n]$. Furthermore, for each n,
$|f(1^{n+1})| - (n+1) > |f(1^n)| - n$.

We define in stages M_n a total $PSPACE$ process machine M such that $C_M(X \upharpoonright |f(1^n)|) \leq |f(1^n)| - n$ for all $n \in \mathbb{N}$, as in the proof of Theorem 1. It remains to be checked that $M(\sigma)$ may be computed in $PSPACE$. We will trace out the computation of $M(\sigma)$ for a given σ.

First we compute $f(1^c)$ for $c \leq |\sigma|$ until we find c such that $|\sigma| < f(1^{c+1}) - c - 1$. Now let $m_i = f(1^i)$ for $i \leq c$ and decompose σ into a concatenation $\sigma_1{}^\frown\sigma_2{}^\frown\cdots{}^\frown\sigma_c$ such that $|\sigma_1{}^\frown\cdots{}^\frown\sigma_j| = f(1^j) - j$ for all $j \leq c$. This can all be done using polynomial space and we can store the sequences $m_1, \cdots, m_c$ and $\sigma_1, \cdots, \sigma_c$. Then we will have $M(\sigma) = \rho_1{}^\frown\cdots{}^\frown\rho_c$ where for each $i \leq c$, $\rho_1{}^\frown\cdots{}^\frown\rho_j = M(\sigma_1{}^\frown\cdots{}^\frown\sigma_i$ and has length $f(1^j)$. If $|\sigma| < f(1) - 1$, then $M(\sigma) = \emptyset$. Otherwise, we compute τ_1 as follows. First enumerate all strings of length $f(1^j)$ and find i such that σ_1 is the i'th string. Then enumerate $G_1 = \{\tau_1, \ldots, \tau_{k(1)}$. If $k(1) < i$, then $\rho_1 = 0^{f(1)}$. Otherwise $\rho_i = \tau_i$. Once we have computed ρ_1, we may reset the work tape.

At stage $c+1$, we are given $\sigma_1, \ldots, \sigma_{c+1}$ and $\tau_1, \ldots, \tau_c$. If $|\sigma_1{}^\frown\cdots{}^\frown\sigma_{c+1} < f(1^c) - c$, then $\tau_{c+1} = \emptyset$ and $M(\sigma) = \tau_1{}^\frown\cdots{}^\frown\tau_c$. Otherwise, we compute τ_{c+1} as follows. First enumerate all strings of length $f(1^{c+1}) - c - 1$ and find i such that σ_{c+1} is the i'th string. Then enumerate $\{\tau : \sigma)_1{}^\frown\cdots{}^\frown\sigma_c{}^\frown\tau \in G_{c+1}\} = \{\tau_1, \ldots, \tau_k\}$. If $k < i$, then $\rho_{c+1} = 0^{f(c)}$. Otherwise $\rho_i = \tau_i$. It is clear that these calculations may be done in $PSPACE$, since f is $PTIME$ and $c < |\sigma|$.

To verify that M is a BPS quick process machine, observe that if $|\sigma| \geq f(c) - c$, then $|M(\sigma)| \geq f(c) \geq c$. Hence the $PTIME$ function $g(n) = f(n) - n$ completes the definition.

By assumption $X \in U_c$ for every c, so that $X \upharpoonright f(c) = \tau$ for some $tau \in G_c$ and hence $M(\sigma) = \tau$ where $|\sigma| = f(c) - c$. It follows that $C_M(X \upharpoonright f(c)) = f(c) - c$.

Hence, X is not quick process BP random.

Theorem 12. *There is a $DSPACE(2^{2^n})$ real which is Martin-Löf BPS random.*

Proof. Let $(G^{(e)}, f^{(e)}, a^{(e)}, b^{(e)})_{e\geq 0}$ be an enumeration of all 4-tuples (G, f, a, b) such that $G : \{1\}^* \times \{0,1\}^* \to \{0,1\}$ is $PSPACE$ function such that the space required to compute string G on strings of length n is $\leq (2+n)^a$ for $n \geq 0$ and

$f : \{1\}^* \to \{1\}^*$ is $PTIME$ function such that the time required to compute string f on strings of length n is $\leq (2+n)^b$ for $n \geq 0$. We want to construct a recursive real $X = (X(1), X(2), \ldots)$ such that X passes all $PSPACE$ tests. Thus we need on consider those e such for all n, $G^{(e)}_{n,f^{(e)}}$ is a finite set of strings $\{\sigma_{1,n}, \ldots, \sigma_{k(n),n}\}$ such that (i) $U_n = [\sigma_{1,n}] \cup \cdots \cup [\sigma_{k_e(n),n}]$ is a clopen set with measure $\leq 2^{-n}$, (ii) $|\sigma_{i,n}| = |f^{(e)}(1^n)|$ for all $i \leq k_e(n)$, and (iii) $U_{n+1} \subseteq U_n$ for all n.

Then we can construct X in stages.

Stage 0. Let $X(n) = 0$ until you find an n large enough such that in 2^{2^n}-space we can compute $G^{(0)}(1^{2n}, \tau)$ on all strings of length $|f^{(0)}(1^{2n})|$ and $f^{(0)}(1), \ldots f^{(0)}(1^{2n})$. That is, if we can not compute all these computations in 2^{2^n}-space, then we set $X(n) = 0$. There must be such n since $G^{(0)}$ runs in space $(2+n)^{a^{(0)}}$ and f runs in time $(2+n)^{b^{(0)}}$. Assume that n_0 is the least such n. Thus in $2^{2^{n_0}}$-space, we can compute $G^{(0)}_{2n_0,f^{(0)}} = \{\sigma_{1,2n_0}, \ldots, \sigma_{k_0(2n_0),2n_0}\}$ and $f^{(0)}(1), \ldots f^{(0)}(1^{2n_0})$. Let $U^{(0)}_{2n_0} = [\sigma_{1,2n_0}] \cup \cdots \cup [\sigma_{k(2n_0),2n_0}]$. Now if it is not the case that $\mu(U^{(0)}_{2n_0}) \leq 2^{2n_0}$ and $|f^{(0)}(1)| < \cdots < |f^{(0)}(1^{2n_0})|$, then set $X(n_0) = 0$, $r(0) = n_0$ and go onto stage 1. Otherwise, the measure of the set of strings of length $|f^{(0)}(1^{2n_0})|$ which extend 0^{n_0} is $\geq 2^{-n_0}$, so that in space $2^{2^{n_0}}$, we can find the lexigraphic least string σ of length $|f^{(0)}(1^{2n_0})|$ which extends 0^{n_0} and is not $U^{(0)}_{2n_0}$ and set $X \upharpoonright |f^{(0)}(1^{2n_0})|$ and $r(0) = |f^{(0)}(1^{2n_0})|$.

Stage s+1. Assume that we have defined $r(0) < \ldots < r(s)$ $(X(1), \ldots, X(r(s))$ such that for all $i \leq s$, either
(I) it is the not the case that $G^{(i)}_{r(i),f^{(i)}}$ is a finite set of strings $\{\sigma_{1,i}, \ldots, \sigma_{k_i(i),i}\}$ such that $U_i = [\sigma_{1,i}] \cup \cdots \cup [\sigma_{k_i(i),i}]$ is a clopen set with measure $\leq 2^{-i}$ and $|f^{(i)}(1)| < \cdots < |f^{(i)}(1^{r(i)})|$, or
(II) $G^{(i)}_{r(i),f^{(i)}}$ a finite set of strings or $\{\sigma_{1,i}, \ldots, \sigma_{k_i(i),1}\}$ such that $U_i = [\sigma_{1,i}] \cup \cdots \cup [\sigma_{k_i(i),i}]$ is a clopen set with measure $\leq 2^{-i}$ and $|\sigma_{i,1}| = |f^{(i)}(1^{r(i)}|$ for all $i \leq k_i(i)$ and $(X(0), \ldots, X(r(i))) \notin U_i$.

Extend $(X(0), X(1), \ldots X(r(s))$ by setting $X(n) = 0$ until you find an $n > r(s)$ large enough such that in 2^{2^n}-space, we can compute $G^{(s+1)}(1^{2n}, \tau)$ on all strings of length $|f^{(s+1)}(1^{2n})|$ and $f^{(s+1)}(1), \ldots f^{(s+1)}(1^{2n})$. That is, if we can not compute all these computations in 2^{2^n}-space, then we set $X(n) = 0$. There must be such n since $G^{(s+1)}$ runs in space $(2+n)^{a^{(s+1)}}$ and f runs in time $(2+n)^{b^{(s+1)}}$. Assume that n_{s+1} is the least such n. Thus in $2^{2^{n_{s+1}}}$-space, we can compute $G^{(s+1)}_{2n_0,f^{(s+1)}} = \{\sigma_{1,2n_{s+1}}, \ldots, \sigma_{k_{s+1}(2n_{s+1}),2n_{s+1}}\}$ and $f^{(s+1)}(1), \ldots f^{(s+1))}(1^{2n_{s+1}})$. Let
$U^{(s+1)}_{2n_{s+1}} = [\sigma_{1,2n_{s+1}}] \cup \cdots \cup [\sigma_{k_{s+1}(2n_{s+1}),2n_{s+1}}]$. Now if it is not the case that $\mu(U^{(s+1)}_{2n_{s+1}}) \leq 2^{2n_{s+1}}$ and $|f^{(s+1)}(1)| < \cdots < |f^{(s+1)}(1^{2n_{s+1}})|$, then set $X(n_{s+1}) = 0$, $r(0) = n_{s+1}$ and go onto stage $s+1$.

Otherwise, the measure of the set of strings of length $|f^{(s+1)}(1^{2n_{s+1}})|$ which extend $(X \upharpoonright r(s))^\frown 0^{n_{s+1}-r(s)}$ is $\geq 2^{-n_{s+1}}$, so that in space $2^{2^{n_{s+1}}}$, we can find the lexigraphic least string σ of length $|f^{(s+1)}(1^{2n_{s+1}})|$ which extends $0^{n_{s+1}}$ and is not $U_{2n_{s+1}}^{(s+1))}$ and set $X \upharpoonright |f^{(s+1)}(1^{2n_{s+1}})| = \sigma$ and $r(s+1) = |f^{(s+1)}(1^{2n_{s+1}})|$.

It is easy to see that our construction is completely effective so that $X = (X(1), X(2), \ldots)$ will be $DSPACE^{2^{2^n}}$ real which passes all $PSPACE$ tests. Thus X is a BPS random real.

Conjecture 1. There is an $EXPSPACE$ real which is process BPS random.

4 Conclusions and Future Research

In this paper, we define robust notion of primitive recursive and $PSPACE$ randon real in the each definition could be framed in at least two of the three version of random reals via measure, Kolomogorov complexity, or martingales. We view the work of this paper as a possible model for several other classes of sub-computable functions. In future work, we will define similar notions of bounded pseudorandom reals for other classes of sub-computable functions such as elementary, on-line, or $EXPSPACE$.

In future work, we plan to study bounded pseudorandomness for trees and for effectively closed sets. Algorithmic randomness of trees and effectively closed sets was developed in a series of papers by Barmpalias, Cenzer, Remmel et al [**?**].

References

1. E. Allender and M. Strauss. Measure on small complexity classes with applications for BPP, in *Proceedings of the 35th Symposium on Foundations of Computer Science*, IEEE Computer Society (1994), 807-818.
2. E. Allender and M. Strauss, Measure on P : Robustness of the notion, in *Proceedings of the 20th International Symposium on Mathematical Foundations of Computer Science*, Springer-Verlag (1995), 129-138.
3. K. Ambos-Spies and E. Mayordomo, Resource-bounded measure and randomness, in A. Sorbi, ed., *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, New York, N.Y. (1997), 1-47.
4. M. Blum and S. Micali, How to Generate Cryptographically Strong Sequences of Pseudorandom Bits, *Siam J. Computing 13* (1984), 850-864.
5. P. Brodhead, D. Cenzer, F. Toska and S. Wyman, Algorithmic randomness and capacity of closed sets, *Logical Methods in Computer Science* 7 :3,16 (2011, 1-16.
6. P. Brodhead, R. Downey and S. Ng, Bounded randomness, in: M.J. Dinneen et al. (Eds.), *Workshop on Theoretical Computer Science 2012 (Calude Festschrift)*, Springer Lecture Notes in Computer Sciemce 7160 (2012), 59–70.

7. H. Buhrman and L. Longpre, Compressibility and resource bounded measure. *SIAM Journal on Computing*, 31(3):876-886, 2002.
8. C. Calude and M. Zimand. Effective category and measure in abstract complexity theory. *Theoretical Computer Science* 154 (1996), 307-327.
9. D. Cenzer, and J.B. Remmel, Effectively Closed Sets, book manuscript, to appear.
10. G. Chaitin, On the length of programs for computing finite binary sequences, *J. Assoc. Comp. Mach.* 13 (1966), 547-569.
11. A. Chernov, A. Shen, N. Vereschagin and V.Vovk, On-line probability, complexity and randomness, in *Algorithmic Learning Theory 2008*, Springer Lecture Notes in Computer Science 5254 (2008), 138-153.
12. A. Church, On the concept of random sequences, *Bull. Amer. Math. Soc.* 46 (1940), 130-135.
13. A. Day, On process and truth-table characterizations of randomness, *Theoretical Computer Science* 452(2012), 47-55.
14. R. Di Paola, Random sets in subrecursive hierarchies, *J. Assoc. Comp. Mach.* 16 (1969), 621-630.
15. R.G. Downey and E.J. Griffiths, Schnorr randomness, *Electronic Notes in Computer Science* 66 (2002), 25-35.
16. R.G. Downey, E.J. Griffiths, and G. Laforte, On Schnorr and computable randomness, martingales and machines, *Math. Logic Quarterly* 50 (2004), 613-627.
17. R.G. Downey, E. J. Griffiths, and S. Reid, On Kurtz randomness, *Theoretical Computer Science* 321 (2004), 249-270.
18. R. Downey and D. Hirschfeldt, *Algorithmic Randomness and Complexity*, Springer-Verlag, 2011.
19. M. Hitchcock and J. H. Lutz, Why computational complexity requires stricter martingales, *Theory of Computing Systems*, 39 (2006), 277-296.
20. S. Kautz, *Degrees of Random Sets*, Ph.D. Thesis, Cornell University, 1991.
21. S. Kautz, Resource-bounded randomness and compressibility with respect to nonuniform measures, in *Proceedings of the International Workshop on Randomization and Approximation Techniques in Computer Science*, Springer-Verlag (1997), 197-211.
22. K. Ko, On the notion of infinite pseudorandom sequences, *Theoretical Computer Science* 48 (1986), 9-33.
23. A. N. Kolmogorov, Three approaches to the quantitative defintion of information, in *Problems of Information Transmission, Vol. 1* (1965), 1-7.
24. S. Kurtz, *Randomness and Genericity in the Degrees of Unsolvability*, Ph.D. Thesis, University of Illinois at Urbana, 1981.
25. L. Levin, On the notion of a random sequence, *Soviet Math. Doklady* 14 (1973), 1413-1416.
26. L. Levin and A.K. Zvonkin, The complexity of finite objects and the development of the concepts of information and randomness of means of the theory of algorithms, *Russian Math. Surveys* 25 (1970), no. 6.
27. M. Li and P. Vitanyi, *An introduction to Kolmogorov Complexity and Its Applications*, third edition (2008) Springer.
28. J. H. Lutz, Category and measure in complexity classes. *SIAM Journal on Computing*, 19(1990), 1100-1131.
29. J. H. Lutz, Computability versus exact computability of martingales. *Information Processing Letters*, 92(5):235-237, 2004.
30. K. Miyabe, Truth-table Schnorr randomness and truth-table reducible randomness, *Math. Logic Quarterly* 57 (2011), 323-338.

31. P. Martin-Löf, The definition of random sequences, *Information and Control* 9 (1966), 602-619.
32. A. Nies, *Computability and Randomness*, Oxford University Press (2009).
33. C. P. Schnorr, A unified approach to the definition of random sequences, *Mathematical Systems Theory* 5 (1971), 246-258.
34. C. P. Schnorr, Process complexity and effective random test, *Journal of Computer and System Sciences* 7 (1973),376-388.
35. M. van Lambalgen, *Random Sequences*, Ph.D. Dissertation, University of Amsterdam (1987).
36. J. Ville, *Étude Critique de la Notion de Collectif*. Gauthier-Villars, Paris, 1939.
37. R. von Mises, Grundlagen der Wahrscheinlichkeitsrechnung, *Math. Zeitschrift* 5 (1919), 52-99.
38. Y. Wang, Randomness and Complexity, Ph.D. dissertation, University of Heidelberg, 1996.
39. Y. Wang, Resource bounded randomness and computational complexity. *Theoretical Computer Science*, 237 (2000), 33-55.
40. Randomness and the density of hard problems, Proc. 24th IEEE Symposium on Foundations of Computer Science (1983), 335-342.