Independence Properties of Algorithmically Random Sequences
(Preliminary Draft)

Steven M. Kautz

Department of Mathematics

Randolph-Macon Woman's College

2500 Rivermont Avenue

Lynchburg, VA 24503

April 5, 1995

1   Introduction

Any plausible characterization of what it means for an infinite sequence to be *random* is likely to incorporate the common notion that one random sequence should not contain any information about any other random sequence, or further, that observing *part* of a random sequence should provide no information about any other part of the same sequence. These ideas can be found in the intuitive definition of random sequences proposed by R. von Mises in the 1920's [24]: what makes a sequence A random, he suggested, is that

  (i) *limiting frequencies* exist, i.e.,

$$\lim_{n \to \infty} \frac{\# \text{ of 1's in } A[0..n-1]}{n} = p$$

   for some number p (where $A[0..n-1]$ denotes the first n bits of A), and

  (ii) given any admissible rule for selecting a subsequence A_0 from A, the limiting frequency in A_0 is the same value p.

The exact meaning of the term "admissible" is problematic and controversial, at least in part because Platonistically there certainly exists a selection rule of the form "select bit $A[n]$ iff $A[n] = 1$." Church [5] proposed limiting the "admissible" rules to be recursive functions which given an initial segment $A[0..n-1]$ produce either a zero or one, according to whether the nth bit is to be selected. A sequence satisfying (i) and (ii) above for every recursive place selection of this form may be called *Mises-Church stochastic*. Such a selection rule corresponds to a gambling strategy for a game in which the bits of A are revealed sequentially, such as by successive coin tosses, and a gambler has access only to the past history of the game when deciding whether to place a bet on the next outcome. The sequence A is Mises-Church stochastic if no recursive strategy enables the gambler to alter the expected gain in the long run. It is certainly reasonable to accept this as a necessary condition, however, notice that the definition fails to include other kinds of strategies (which von Mises clearly had in mind) such as "toss a coin, and select bit $A[n]$ if the toss results in heads," which intuitively cannot change the gambler's expected gain either. Evidently the crucial point is

not that the selection process is recursive, but that in some sense it has no information about the sequence A; we might say that A must be independent of the selection rule.

The fact that the definition proposed by Church is indeed too weak to satisfactorily characterize random sequences is a consequence of a result of Ville (see [23] or [21]), i.e., there are Mises-Church stochastic sequences which fail to satisfy certain widely accepted probabilistic laws. Kolmogorov and (independently) Loveland (see [21]) offered the generalization of a selection rule given in Definition 4.1 below. No examples are known of sequences which satisfy (i) and (ii) for every Kolmogorov-Loveland selection rule but which fail to satisfy some "known" probabilistic law [10, p.398], though not every such sequence is algorithmically random in the sense of Definition 3.2 [21], [18].

M. van Lambalgen observed that the relation "A is algorithmically random relative to B" could be interpreted as an *independence* relation, and that relative randomness in this sense satisfies the axiomatization of independence given in [22]. In this paper we investigate the independence properties of algorithmically random sequences related to notions of subsequence selection. We consider two kinds of questions: First, if A is algorithmically random and A_0 is a subsequence chosen according to a (not necessarily recursive) selection rule, what conditions must be imposed on the selection rule to guarantee that A_0 remains algorithmically random? Second, if A_1 denotes the subsequence of *nonselected* bits, for what kinds of selection rules are A_0 and A_1 independent?

The main new result proved here is Theorem 4.5, that A_0 and A_1 are independent when A_0 is chosen via a *bounded* Kolmogorov-Loveland selection rule. While a Mises-Church place selection is a special case of a selection rule of this form, the application we have in mind is that the sequence of queries of a time-bounded Turing machine may, under certain conditions, be construed as a bounded Kolmogorov-Loveland place selection. We indicate, for example, how this fact can be used to prove the well known result [1] that P $\neq$ NP relative to an algorithmically random oracle. More recently Kautz and Miltersen [9] have used Theorem 4.5 to show that relative to a random oracle, NP does not have *measure zero* within the exponential complexity classes DTIME(2^{linear}) or DTIME($2^{\text{polynomial}}$), an (apparently) stronger separation of P from NP. ("Measure zero" refers the resource-bounded measure of Lutz [13].)

2   Preliminaries

Our notation is for the most part standard. Unfamiliar notions from recursion theory can probably be found in Odifreddi[1] [15] or Rogers [16], and everything else we need to know can be found in [7]. Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ denote the natural numbers. A *string* is an element of $\{0,1\}^*$ or $\{0, 1, \bot\}^*$, where the symbol $\bot$ is called an *undefined* bit. The concatenation of strings x and y is denoted xy. For any string x, $|x|$ denotes the length of x, and λ is the unique string of length 0. If $x \in \{0, 1, \bot\}^*$ and $j, k \in \mathbb{N}$ with $0 \le j \le k < |x|$, $x[k]$ is the kth bit (symbol) of x and $x[j..k]$ is the string consisting of the jth through kth bits of x (note that the "first" bit of x is the 0th). For an infinite binary sequence $A \in \{0,1\}^\infty$, the notations $A[k]$ and $A[j..k]$ are defined analogously. For any $x, y \in \{0, 1, \bot\}^*$, $x \sqsubseteq y$ means that if $x[k]$ is defined, then $y[k]$ is also defined and $x[k] = y[k]$; we say that x is an *initial segment*, or *predecessor*, of y or that y is an *extension* of x. Likewise for $A \in \{0,1\}^\infty$, $x \sqsubseteq A$ means $x[k] = A[k]$ whenever bit $x[k]$ is defined. Strings x and y are said to be *incompatible*, or *disjoint*, if there is no string z which is an extension of both x and y; when $x, y \in \{0,1\}^*$, this simply means that $x \not\sqsubseteq y$ and $y \not\sqsubseteq x$.

Fix a standard enumeration of $\{0,1\}^*$, $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, s_4 = 01, \ldots$. A *language* is a subset of $\{0,1\}^*$; a language A will be identified with its characteristic sequence $\chi_A \in \{0,1\}^\infty$, defined by $s_y \in A \iff \chi_A[y] = 1$ for $y \in \mathbb{N}$. We will consistently write A for χ_A. $\overline{A}$ denotes the bitwise complement of A, i.e., the set-theoretic complement of the language A in $\{0,1\}^*$. For $X \subseteq \{0,1\}^\infty$, X^c denotes the complement of X in $\{0,1\}^\infty$. Since the enumeration of strings above

---

[1]Ha! The book is *loaded* with unfamiliar notions from recursion theory!

provides a one-to-one correspondence between strings and natural numbers, we may also regard an infinite sequence A as a subset of $\mathbb{N}$.

Typically strings in $\{0, 1, \perp\}^*$ will be used to represent *partially defined languages* or partially defined subsets of $\mathbb{N}$, and will generally be represented by lower-case greek letters. For $\sigma \in \{0, 1, \perp\}^*$, when no confusion is likely to result we will regard σ, $\sigma \perp^k$, and $\sigma \perp^\infty$ as essentially the same object, since all specify the same language fragment. We avoid using the notation $|\sigma|$ unless $\sigma \in \{0, 1\}^*$, however following [13] we let $||\sigma||$ denote the number of *defined* bits in σ. When $\alpha \in \{0, 1, \perp\}^*$ and $\tau \in \{0, 1\}^*$, the notation $\alpha \downarrow \tau$ ("τ inserted into α") is defined by

$$(\alpha \downarrow \tau)[x] = \begin{cases} \alpha[x] & \text{if } \alpha[x] \text{ is defined,} \\ \tau[j] & \text{if } x \text{ is the } j\text{th undefined} \\ & \text{position in } \alpha \text{ and } j < |\tau|, \\ \perp & \text{otherwise.} \end{cases}$$

For $A, B \in \{0, 1\}^\infty$, A/B is the subsequence of A *selected* by B, i.e., if $y_0, y_1, \ldots$ are the positions of the 1-bits of B in increasing order, then $(A/B)[x] = A[y_x]$. Note that A/B is a finite string if B contains only finitely many 1's. For $\sigma, \tau \in \{0, 1\}^*$, σ/τ may be defined analogously. For $A, B \in \{0, 1\}^\infty$, the sequence $A \oplus B$ is defined by

$$A \oplus B[x] = \begin{cases} A[\frac{x}{2}] & \text{if } x \text{ is even,} \\ B[\frac{x+1}{2}] & \text{if } x \text{ is odd.} \end{cases}$$

Let $\langle \cdot, \cdot \rangle : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ be a fixed recursive bijection. Then $A^{[i]}$, the *ith column of A*, is defined by

$$A^{[i]} = \{n : \langle n, i \rangle \in A\}.$$

Given any countable sequence $\{B_i\}$ we can define a set $\bigoplus_i B_i$ whose ith column is B_i:

$$\bigoplus_i B_i = \{\langle n, i \rangle : n \in B_i\}.$$

Let φ_e denote the eth partial recursive (p.r.) function, and φ_e^A the eth p.r. function relative to $A \in \{0, 1\}^\infty$. We write $\varphi_e(x) \downarrow$ if φ_e is defined on x, and $\varphi_e(x) \uparrow$ otherwise; the same holds for the relativized φ_e^A. For $s \in \mathbb{N}$,

$$\varphi_{e,s}(x) = \begin{cases} \varphi_e(x) & \text{if } \varphi_e(x) \text{ converges in } \leq s \text{ steps} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

$\varphi_e^\sigma(x)$ generally abbreviates $\varphi_{e,|\sigma|}^\sigma(x)$; we treat φ_e^σ or $\varphi_{e,s}$ as a partially defined set or language, i.e., it may be regarded as an element of $\{0, 1, \perp\}^*$. As usual, $W_e = \text{dom}(\varphi_e)$ is the eth recursively enumerable (r.e.) set, $W_{e,s} = \text{dom}(\varphi_{e,s})$, $W_e^A = \text{dom}(\varphi_e^A)$, and $W_e^\sigma = \text{dom}(\varphi_e^\sigma)$.

If φ_e^A is total, so that $\varphi_e^A = B$ for some set B (i.e., its characteristic function), we write $B \leq_T A$; if $B \leq_T A$ and $A \leq_T B$, we write $A \equiv_T B$. $A <_T B$ means that $A \leq_T B$ but $B \not\leq_T A$. The equivalence class $\deg(A) = \{B \in \{0, 1\}^\infty : A \equiv_T B\}$ is called the *degree* of A; $\mathcal{D}$ denotes the collection $\{\deg(A) : A \in \{0, 1\}^\infty\}$, the *Turing degrees* or *degrees of unsolvability*. The relation $\leq_T$ induces a well-defined partial order on $\mathcal{D}$ (simply denoted $\leq$) and the operation $\oplus$ induces a well-defined least upper bound operation $\cup$ on $\mathcal{D}$. The *jump* of a set A, denoted A', is the set

$$\{x : \varphi_x^A(x) \downarrow\},$$

and $A^{(n)}$ represents the nth iterate of the jump of A. For functions $f : \mathbb{N} \longrightarrow \mathbb{N}$, by $\deg(f)$ we mean the degree of the graph of f, $\{\langle x, y \rangle : f(x) = y\}$.

A string $\sigma \in \{0, 1, \bot\}^*$ defines the subset $\text{Ext}(\sigma) = \{A \in \{0,1\}^\infty : \sigma \sqsubseteq A\}$ of $\{0,1\}^\infty$, called a *cylinder*. $\text{Ext}(\sigma)$ is referred to as an *interval* if $\sigma \in \{0,1\}^*$; evidently any cylinder is a union of intervals. Likewise if S is a subset of $\{0, 1, \bot\}^*$, $\text{Ext}(S)$ denotes $\bigcup_{\sigma \in S} \text{Ext}(\sigma)$. If $S = W_e$ is an r.e. set of strings, then $\text{Ext}(S)$ is called a Σ_1^0-class; the number e is an *index* of the class. A Π_1^0-class is the complement of a Σ_1^0-class. In general a Π_n^0-class is the complement of a Σ_n^0-class, and a Σ_{n+1}^0-class is of the form $\bigcup_i \mathcal{T}_i$, where $\{\mathcal{T}_i\}$ is a uniform sequence of Π_n^0-classes; likewise a Π_{n+1}^0-class is of the form $\bigcap_i \mathcal{T}_i$, where the $\mathcal{T}_i$ are Σ_n^0-classes. Here, as elsewhere, a *uniform* (or *recursive*) sequence $\{\mathcal{T}_i\}$ is one for which there is a recursive function f such that $f(i)$ is an index for $\mathcal{T}_i$; an index for the function f may be called an index of the sequence. A class is called *arithmetical* if it is Σ_n^0 for some n.

It is also convenient to note that arithmetical classes can be defined in terms of quantifier complexity. Let $\mathcal{L}^*$ be the language of arithmetic with a set constant X and a membership symbol $\in$. Then for a sentence ϕ of $\mathcal{L}^*$ and $A \in \{0,1\}^\infty$, $A \models \phi$ means that ϕ is true in the standard model when X is interpreted as A. A Σ_n^0-class is of the form $\{A : A \models \phi\}$, where ϕ is a Σ_n sentence of $\mathcal{L}^*$; likewise for Π_n^0-classes. Since notions of computation can be expressed in a simple way in $\mathcal{L}^*$ we can, for example, represent a Σ_n^0-class in the form

$$\{A : (\exists x_1)(\forall x_2) \dots (\exists x_n)[\varphi_e^A(x_1, \dots, x_n) \downarrow]\}$$

if n is odd, and in the form

$$\{A : (\exists x_1)(\forall x_2) \dots (\forall x_n)[\varphi_e^A(x_1, \dots, x_n) \uparrow]\}$$

if n is even. See Rogers [16] for details.

The definitions of arithmetical classes can all be relativized; e.g., a Σ_1^C-class is of the form $\text{Ext}(W_e^C)$, etc. Note, for example, that a $\Sigma_1^{0^{(n-1)}}$-class is an *open* Σ_n^0-class, and a $\Pi_1^{0^{(n-1)}}$-class is a *closed* Π_n^0-class, where we take $\{\text{Ext}(\sigma) : \sigma \in \{0,1\}^*\}$ as the base of a topology on $\{0,1\}^\infty$.

By a *measure* we simply mean a probability distribution on $\{0,1\}^\infty$, and for our present purposes it is sufficient to consider the uniform distribution, i.e., each bit is equally likely to be a zero or a one, also called Lebesgue measure. The measure of a subset $\mathcal{E}$ of $\{0,1\}^\infty$, denoted $\mathbf{Pr}(\mathcal{E})$, can be intuitively interpreted as the probability that a sequence produced by tossing a fair coin is in the set $\mathcal{E}$; in particular the measure of an interval $\text{Ext}(\sigma)$, abbreviated $\mathbf{Pr}(\sigma)$, is just $(\frac{1}{2})^{|\sigma|}$ (or $(\frac{1}{2})^{||\sigma||}$ if $\sigma \in \{0, 1, \bot\}^*$). For S a set of strings, we abbreviate $\mathbf{Pr}(\text{Ext}(S))$ by $\mathbf{Pr}(S)$; if S is *disjoint*, i.e., all strings in S are pairwise incompatible, then

$$\mathbf{Pr}(S) = \sum_{\sigma \in S} \mathbf{Pr}(\sigma).$$

Standard results of measure theory (see [6]) show that $\mathcal{E}$ is *measurable* (meaning that $\mathbf{Pr}(\mathcal{E})$ is defined) as long as $\mathcal{E}$ is a *Borel* set, i.e., built up from intervals by some finite iteration of countable union and complementation operations; in particular arithmetical classes are always measurable.

3   Effective Approximations in Measure

Equivalent definitions of algorithmic randomness have been given by Martin-Löf [14], Levin [12], Schnorr [17], Chaitin [2, 3, 4], and Solovay [19], and generalizations and closely related variations have been given by Kurtz [11], Kautz [8], and Lutz [13]. Here we present the definition due to Martin-Löf and the generalization (n-randomness) first investigated in [11]. The idea is to characterize a random sequence by describing the properties of "nonrandomness" which it must *avoid*. For example, we might examine successively longer initial segments σ of a sequence $A \in \{0,1\}^\infty$ and discover that

$$\frac{\# \text{ of ones in } \sigma}{|\sigma|} \geq \frac{3}{4}. \tag{1}$$

We would then suspect that A is not a sequence we would normally think of as random. A "test" for this particular nonrandomness property can be viewed as a recursive enumeration of strings σ for which (1) holds; if A has arbitrarily long initial segments satisfying (1), we reject A as nonrandom. Now among all possible enumerations of strings, how do we decide *a priori* which ones characterize a "nonrandomness" property? Since ultimately we expect the nonrandom sequences to form a class with measure zero, we can require that as we enumerate longer initial segments in the "test", the total measure of their extensions should become arbitrarily small. The mathematical content of this discussion is made precise in following definition.

Definition 3.1 A *Martin-Löf test* is a recursive sequence of Σ_1^0-classes $\{\mathcal{S}_i\}$ with $\mathbf{Pr}(\mathcal{S}_i) \leq 2^{-i}$. A sequence $A \in \{0,1\}^\infty$ is *1-random* if for every Martin-Löf test $\{\mathcal{S}_i\}$, $A \notin \bigcap_i \mathcal{S}_i$.

The requirement that a test consist of recursively enumerable sets of strings is a natural starting point but is admittedly somewhat arbitrary. A generalized form, where Σ_n^0-classes replace Σ_1^0-classes, first appeared in Kurtz [11]. We will also find it useful to define randomness relative to an oracle.

Definition 3.2 Let $A, C \in \{0,1\}^\infty$. A is Σ_n^C-*approximable*, or *approximable in Σ_n^C-measure*, if there is a recursive sequence of Σ_n^C-classes $\{\mathcal{S}_i\}$ with $\mathbf{Pr}(\mathcal{S}_i) \leq 2^{-i}$ and $A \in \bigcap_i \mathcal{S}_i$. The sequence $\{\mathcal{S}_i\}$ is called a Σ_n^C-*approximation*, or if $n = 1$, a *Martin-Löf test* or *constructive null cover* relative to C. A is C-*n-random*, or *n-random relative to C*, if A is not Σ_n^C-approximable. If C is recursive then A is *n-random*. We also say A is *ω-random* if A is n-random for all n.

The definition of *n*-randomness as given above is difficult to work with directly when $n > 1$, and there are two basic tools which simplify our work considerably. The first is Lemma 3.5 below, which asserts that *n*-randomness is the same as 1-randomness relative to $0^{(n-1)}$, or more generally, that $(m + n)$-randomness relative to an oracle C is the same as *n*-randomness relative to $C^{(m)}$. The second is Theorem 3.8, which shows that if A is $(n + 1)$-random, then $A^{(n)} \equiv_T A \oplus 0^{(n)}$. These two facts allow many results on 1-randomness to be straightforwardly generalized.

The proof of Lemma 3.5 depends on the idea that an approximation in measure can be replaced by an approximation using *open* classes of the same arithmetical complexity. Lemma 3.4 extends Kurtz' Lemma 2.2a ([11, p.21]) with a number of technical refinements which will be needed later.

Lemma 3.3 *The predicate "$\mathbf{Pr}(\mathcal{S}) > \epsilon$" is uniformly Σ_n^C, where $\mathcal{S}$ is a Σ_n^C-class and ϵ is rational. Likewise "$\mathbf{Pr}(\mathcal{S}) < \epsilon$" is uniformly Σ_n^C when $\mathcal{S}$ is a Π_n^C-class.*

Proof. See Kurtz [11]. •

Lemma 3.4 (i) *For $\mathcal{S}$ a Σ_n^C-class and $\epsilon > 0$ a rational, we can uniformly and recursively obtain the index of a $\Sigma_1^{C^{(n-1)}}$-class (an open Σ_n^C-class) $\mathcal{U} \supseteq \mathcal{S}$ with $\mathbf{Pr}(\mathcal{U}) - \mathbf{Pr}(\mathcal{S}) \leq \epsilon$.*

(ii) *For $\mathcal{T}$ a Π_n^C-class and $\epsilon > 0$ a rational, we can uniformly and recursively obtain the index of a $\Pi_1^{C^{(n-1)}}$-class (a closed Π_n^C-class) $\mathcal{V} \subseteq \mathcal{T}$ with $\mathbf{Pr}(\mathcal{T}) - \mathbf{Pr}(\mathcal{V}) \leq \epsilon$.*

(iii) *For $\mathcal{S}$ a Σ_n^C-class and $\epsilon > 0$ a rational, we can uniformly in $C^{(n)}$ obtain a closed Π_{n-1}^C-class $\mathcal{V} \subseteq \mathcal{S}$ with $\mathbf{Pr}(\mathcal{S}) - \mathbf{Pr}(\mathcal{V}) \leq \epsilon$. (If $n \geq 2$, $\mathcal{V}$ will be a $\Pi_1^{C^{(n-2)}}$-class.) Moreover, if $\mathbf{Pr}(\mathcal{S})$ is a real recursive in $C^{(n-1)}$, the index for $\mathcal{V}$ can be found recursively in $C^{(n-1)}$.*

(iv) *For $\mathcal{T}$ a Π_n^C-class and $\epsilon > 0$ a rational, we can uniformly in $C^{(n)}$ obtain an open Σ_{n-1}^C-class $\mathcal{U} \supseteq \mathcal{T}$ with $\mathbf{Pr}(\mathcal{U}) - \mathbf{Pr}(\mathcal{T}) \leq \epsilon$. (If $n \geq 2$, $\mathcal{U}$ will be a $\Sigma_1^{C^{(n-2)}}$-class.) Moreover, if $\mathbf{Pr}(\mathcal{T})$ is a real recursive in $C^{(n-1)}$, the index for $\mathcal{U}$ can be found recursively in $C^{(n-1)}$.*

Proof. •

The characterization in terms of approximation by *open* sets now follows easily from Lemma 3.4.

Lemma 3.5 *Let* $A, C \in \{0,1\}^\infty$, $n \geq 1$, *and* $m \geq 0$. *Then* A *is* $\Sigma_n^{C^{(m)}}$-*approximable* $\Longleftrightarrow$ A *is* Σ_{m+n}^C-*approximable.*

Proof. ($\Rightarrow$) Immediate, since any $\Sigma_n^{C^{(m)}}$-class is a Σ_{m+n}^C-class.
($\Leftarrow$) We show that a Σ_{m+1}^C-approximation can be replaced by a $\Sigma_1^{C^{(m)}}$-approximation; the result will then follow by induction on n. Let $C \in \{0,1\}^\infty$ and $m \geq 1$ be arbitrary. Suppose $\{\mathcal{S}_i\}$ is a Σ_{m+1}^C-approximation. By Lemma 3.4(i) we can uniformly find for each i a $\Sigma_1^{C^{(m)}}$-class $\mathcal{U}_i \supseteq \mathcal{S}_i$ with $\mathbf{Pr}(\mathcal{U}_i) - \mathbf{Pr}(\mathcal{S}_i) \leq 2^{-i}$. Thus $\mathbf{Pr}(\mathcal{U}_{i+1}) \leq 2^{-i}$, so $\{\mathcal{U}_{i+1}\}$ is a $\Sigma_1^{C^{(m)}}$-approximation and $\bigcap_i \mathcal{S}_i \subseteq \bigcap_i \mathcal{U}_{i+1}$. •

We conclude this section by stating several results we will need which have been known for 1-randomness, and which can be easily generalized using Lemma 3.5. The first of these is known as the "Universal Martin-Löf Test". For a proof see [14] or [8].

Theorem 3.6 (Martin-Löf) *For any* $C \in \{0,1\}^\infty$ *and any* $n \geq 1$ *there exists a universal* Σ_n^C-*approximation. That is, there is a recursive sequence of* $\Sigma_1^{C^{(n-1)}}$-*classes* $\{\mathcal{U}_i\}$, *with* $\mathbf{Pr}(\mathcal{U}_i) \leq 2^{-i}$, *such that every* Σ_n^C-*approximable set is in* $\bigcap_i \mathcal{U}_i$.

The next result is a characterization of n-randomness due to Solovay. It shows that the conditions "$\mathbf{Pr}(\mathcal{S}_i) \leq 2^{-i}$" and "$A \in \bigcap_i \mathcal{S}_i$" in definition 3.2 are both stronger than necessary. A proof can be found in [2] or [8].

Theorem 3.7 (Solovay) *Let* $A, C \in \{0,1\}^\infty$ *and* $n \geq 1$. A *is* C-n-*random* $\Longleftrightarrow$ *for every recursive sequence of* Σ_n^C-*classes* $\{\mathcal{S}_i\}$ *with* $\sum_i \mathbf{Pr}(\mathcal{S}_i) < \infty$, A *is in only finitely many* $\mathcal{S}_i$.

We close this section with one of the single most useful facts about n-randomness, since it allows many results about Σ_1^0-approximations to be extended to Σ_n^0-approximations. It strengthens a result originally due to Sacks that the class $\{A : A' \equiv_T A \oplus 0'\}$ has measure one [20]. The proof is in [8].

Theorem 3.8 *For* $n \geq 0$, *if* A *is* $(n+1)$-*random, then* $A^{(n)} \equiv_T A \oplus 0^{(n)}$.

4 Independence and place selections

The definition below describes a very general selection process which encompasses several special cases of interest. The process may be pictured as follows, as suggested in [21]: Suppose the sequence A is represented as a row of cards laid face down; on the face of the ith card is either a zero or a one, corresponding to $A[i]$. We have two functions, F and G, which are used to select some of the cards to create a second sequence, which we continue to call a "subsequence" even though the order of the cards may be changed. Both F and G look at the history of the selection process, that is, the sequence of cards turned over so far. The value of F is a natural number indicating the position of the next card to be turned over. The value of G is either 0 or 1; if the value is 0, the card is merely turned over and observed, while if the value is 1 the card is also *selected*, i.e., added onto the end of the subsequence.

Definition 4.1 A *Kolmogorov-Loveland place selection* [21] is a pair of partial recursive functions $F : \{0,1\}^* \to \mathbb{N}$ and $G : \{0,1\}^* \to \{0,1\}$ (possibly relative to an oracle C). Let $A \in \{0,1\}^\infty$; F and G select a subsequence Q^* from A as follows. First define sequences of strings $\xi_0 \sqsubseteq \xi_1 \sqsubseteq \cdots$ and $\rho_0 \sqsubseteq \rho_1 \sqsubseteq \cdots$ such that $\xi_0 = \rho_0 = \lambda$, $\xi_{j+1} = \xi_j A[F(\xi_j)]$, and $\rho_{j+1} = \rho_j G(\xi_j)$ (with the proviso that ξ_{j+1} is undefined if $F(\xi_j) = F(\xi_i)$ for some $i < j$ or if either F or G fails to converge). If ξ_j and ρ_j are defined for all j let $Q = \lim_j \xi_j$ and $R = \lim_j \rho_j$. Thus Q represents the sequence of all bits of A examined by F, in the order examined. A given bit $Q[j] = A[F(\xi_j)]$ is included in the

subsequence Q^* just if $G(\xi_j) = 1$, i.e. F determines which bits of A to examine, and G determines which ones to include in the sequence Q^*. Formally we define $Q^* = Q/R$. A Kolmogorov-Loveland place selection will be called *bounded* if the function G is determined by a partial recursive function $H : \{0,1\}^* \to \mathbb{N}$ (possibly relative to oracle C) with the following properties:

(i) H is nondecreasing, i.e., if $\xi \sqsubseteq \xi'$ then $H(\xi) \leq H(\xi')$,

(ii) H is unbounded, i.e., if ξ_j and ρ_j are defined for all j then $\lim_j H(\xi_j) = \infty$, and

(iii) G is determined by H according to the rule

$$
\begin{aligned}
F(\xi) < H(\xi) &\Rightarrow G(\xi) = 0 \\
F(\xi) \geq H(\xi) &\Rightarrow G(\xi) = 1.
\end{aligned}
$$

It is also useful to define a sequence B by $B[z] = 1$ if and only if for some j, $F(\xi_j) = z$ and $G(\xi_j) = 1$, so that $N = A/\overline{B}$ consists of the "nonselected" bits of A, in their natural order.

If it is always the case that $F(\xi) = n$, where $n = |\xi|$, then we have a Mises-Church place selection. Note that if in addition $G(\xi)$ depends only on the length of ξ, then the selected subsequence is of the form A/B, for a fixed sequence B.

In general it is not difficult to show that a subsequence selected from an n-random sequence is also n-random.

Theorem 4.2 *Let $A, B, C \in \{0,1\}^\infty$; suppose F and G are partial recursive in B and determine a K-L place selection. If A is algorithmically random relative to $B \oplus C$, then Q^* is algorithmically random relative to C.*

Sketch of proof: Suppose $\{\mathcal{U}_i\}$ is a Σ_1^C-approximation of Q^*; we can construct a $\Sigma_1^{B \oplus C}$-approximation $\{\mathcal{S}_i\}$ of A. Let $\mathcal{U}_i = \text{Ext}(W_e^B)$. For σ enumerated in W_e^B, start with a string $\alpha = \perp^\infty$. simulate F and G: If $G(\xi) = 1$, let $\alpha[F(\xi)] = $ next bit of σ. If $G(\xi) = 0$, then split into two strings, let $\alpha_0[F(\xi)] = 0$ and $\alpha_1[F(\xi)] = 1$. When no more bits of σ are available, enumerate the corresponding string α into S_i. Total measure of all strings α associated with σ is not more than $\mathbf{Pr}(\sigma)$, since each time we split into two strings an additional bit of α is defined. ●

Note that it follows, using Lemma 3.5 and Theorem 3.8 and taking $C = 0^{(n-1)}$, that if A is n-random relative to B, then Q^* is n-random. We can also conclude that if A is n-random relative to B (and B is infinite) then A/B is n-random. Note in particular that, as predicted by von Mises' intuition, the place selection function, or the sequence B, does not have to be recursive. In fact, it is a consequence of the following result that if A is n-random, then *almost every* place selection preserves the randomness properties of A.

Theorem 4.3 *Let $A, C \in \{0,1\}^\infty$. If $\{B : A$ is $\Sigma_1^{B \oplus C}$ approximable$\}$ has positive measure, then A is Σ_1^C-approximable.*

It then follows, that if A is n-random,

$$\{B : A \text{ is } n\text{-random relative to } B\} \tag{2}$$

has measure one: note that by Lemma 3.5 and Theorem 3.8, A is Σ_n^B-approximable iff it is $\Sigma_1^{B^{(n-1)}}$-approximable, and $B^{(n-1)} \equiv_T B \oplus 0^{(n-1)}$. Hence if the set (2) has measure < 1, then $\{B : A$ is $\Sigma_1^{B \oplus 0^{(n-1)}}$-approximable$\}$ has positive measure, which would imply that A is $\Sigma_1^{0^{(n-1)}}$-approximable, i.e., not n-random.

****** NB Mention some of the weird examples showing the relative randomness hypothesis in the above is sufficient, but not necessary - e.g., if A is random, then so is $A/0A$ ($0A$ is A shifted one bit to the right).

Proving that a selected subsequence is actually *independent* of the nonselected bits is quite a bit more subtle. We begin with the relatively straightforward version below. Although it is actually a consequence of Theorem 4.5, the idea of the proof is much more in evidence in this simpler setting.

Theorem 4.4 *Let $A, B, C \in \{0,1\}^\infty$. If $A \oplus B$ is 1-random relative to C, then A is 1-random relative to $B \oplus C$.*

Proof. As the relativization is straightforward we will suppress the oracle C for readability. We show that if A is Σ_1^B-approximable, then $A \oplus B$ is Σ_1^0-approximable. Suppose A is Σ_1^B-approximable, say by $\{\mathcal{T}_i\}$. Let f be a recursive function giving the indices of the classes $\mathcal{T}_i$, i.e., $\mathcal{T}_i = \mathrm{Ext}(W_{f(i)}^B)$. Fix i and let $e = f(i)$. We describe a uniform procedure for enumerating a set of strings S_i such that $\{\mathrm{Ext}(S_j)\}$ is a Σ_1^0-approximation of $A \oplus B$. Let $S_{i,s}$ be the set of strings

$$\{\sigma \oplus \tau : |\sigma| = |\tau| = s \ \& \ (\exists \sigma' \subset \sigma)(\exists \tau' \subset \tau)[\sigma' \in W_e^{\tau'} \ \& \ \mathbf{Pr}(\mathrm{Ext}(W_e^{\tau'})) \leq 2^{-i}]\}$$

and $S_i = \bigcup_s S_{i,s}$. Note that S_i is r.e. Certainly $A \oplus B$ is in $\mathrm{Ext}(S_i)$, since some initial segment σ' of A is in W_e^B and hence in W_e^τ for some $\tau \subset B$ with $s = |\tau| \geq |\sigma'|$. Thus $\sigma \oplus \tau$ is enumerated in $S_{i,s}$, where σ is the initial segment of A of length s.

To show that $\mathbf{Pr}(\mathrm{Ext}(S_i)) \leq 2^{-i}$, since $\mathrm{Ext}(S_{i,s}) \subseteq \mathrm{Ext}(S_{i,s+1})$ it will suffice to show that for each s, $\mathbf{Pr}(\mathrm{Ext}(S_{i,s})) \leq 2^{-i}$. Fix s and fix a string τ of length s. Let τ^* be the longest initial segment of τ such that $\mathbf{Pr}(\mathrm{Ext}(W_e^{\tau^*})) \leq 2^{-i}$. Then for every string of the form $\sigma \oplus \tau$ in $S_{i,s}$ there must be some $\sigma' \subset \sigma$ in $W_e^{\tau^*}$, so the measure contributed to $S_{i,s}$ by strings of the form $\sigma \oplus \tau$ cannot exceed

$$\sum_{\sigma' \in W_e^{\tau^*}} 2^{-|\sigma'|} \cdot 2^{-|\tau|}$$
$$= 2^{-|\tau|} \cdot \mathbf{Pr}(\mathrm{Ext}(W_e^{\tau^*}))$$
$$\leq 2^{-s} \cdot 2^{-i}$$

(where we have tacitly assumed that $W_e^{\tau^*}$ is disjoint). There are 2^s strings τ of length s, so the total measure of $\mathrm{Ext}(S_{i,s})$ is at most 2^{-i}. ●

It follows that if $A \oplus B$ is n-random, then A is n-random relative to B. If A is Σ_n^B-approximable, then A is $\Sigma_1^{B^{(n-1)}}$-approximable (by Lemma 3.5), and hence is $\Sigma_1^{B \oplus 0^{(n-1)}}$-approximable by Theorem 3.8 (note that B is n-random by Theorem 4.2). Thus $A \oplus B$ is $\Sigma_1^{0^{(n-1)}}$-approximable by Theorem 4.4 i.e., not n-random.

A converse has been proved by van Lambalgen [22]: if B is n-random and A is n-random relative to B, then $A \oplus B$ is n-random; then it follows that B is also n-random relative to A.

****** NB this provides an alternate proof of Theorem 4.3.

The result below encompasses Theorem 4.4 as well as a number of other cases of interest, such as Mises-Church place selections and selections of the form A/B for a fixed B. The remainder of this section will be devoted to a proof of the result.

Theorem 4.5 *Let $A, B, C \in \{0,1\}^\infty$. Let F and H be partial recursive functions relative to B which determine a bounded Kolmogorov-Loveland place selection, and let N and Q^* be as in Definition 4.1. If A is algorithmically random relative to $B \oplus C$ and N is infinite, then N is algorithmically random relative to $Q^* \oplus C$.*

8

Notice that using Lemma 3.5 and Theorem 3.8 and taking $C = 0^{(n-1)}$ and B recursive, it follows from Theorem 4.5 that if A is n-random then N is n-random relative to Q^*. Moreover, by the converse to Theorem 4.4 noted above, it follows that Q^* is also n-random relative to N.

Before beginning the proof, we isolate a counting argument that will be needed.

Lemma 4.6 *Let $s \in \mathbb{N}$ and let f be a real-valued function on $\{0,1\}^*$ whose domain includes all strings of length at most s. Suppose there is a constant c such that for every string τ_0 of length s,*

$$\sum_{\tau \sqsubseteq \tau_0} f(\tau) \le c.$$

Then

$$\sum_{j=0}^{s} \sum_{|\tau|=j} 2^{-|\tau|} f(\tau) \le c.$$

That is, the domain of f can be viewed as a full binary tree of height s with a real value assigned to each node; if the sum along each branch is bounded by c, then the sum, for $j \le s$, of the average value of the nodes at level j is also bounded by c.

Proof. First note that if M is any $n \times m$ real matrix and c is a constant such that the sum of each column is bounded by c, then the total of the averages of the rows is bounded by c. This is easy to see, since if

$$\sum_{j=0}^{n-1} M(j,k) \le c$$

for each $k = 0, \ldots, m-1$, then

$$\sum_{j=0}^{n-1} \left(\frac{1}{m} \sum_{k=0}^{m-1} M(j,k) \right) = \frac{1}{m} \sum_{k=0}^{m-1} \sum_{j=0}^{n-1} M(j,k) \le \frac{1}{m} \sum_{k=0}^{m-1} c = c. \tag{3}$$

Let $m = 2^s$ and $n = s+1$ and let $\tau_0, \tau_1, \ldots, \tau_{m-1}$ be a list of all strings of length s. Define an $n \times m$ matrix M by

$$M(j,k) = \begin{cases} f(\tau_k[0..j-1]) & \text{if } j > 0 \\ f(\lambda) & \text{if } j = 0 \end{cases}.$$

That is, the values along the branch τ_k correspond to the kth column of M, so the sums of the columns of M are bounded by c. For each $j = 0, \ldots, n-1$, the values in row j are of the form $f(\tau)$ for strings τ of length j; there are 2^j possible values $f(\tau)$, each of which must occur 2^{s-j} times in row j. Hence

$$\sum_{k=0}^{m-1} M(j,k) = \sum_{|\tau|=j} 2^{s-j} f(\tau)$$

and so

$$\begin{aligned} \sum_{j=0}^{s} \sum_{|\tau|=j} 2^{-|\tau|} f(\tau) &= \sum_{j=0}^{n-1} \sum_{|\tau|=j} 2^{-j} f(\tau) \\ &= \sum_{j=0}^{n-1} \sum_{|\tau|=j} \frac{1}{2^s} 2^{s-j} f(\tau) \\ &= \sum_{j=0}^{n-1} \frac{1}{2^s} \sum_{k=0}^{m-1} M(j,k) \\ &\le c \end{aligned}$$

by (3). ●

Proof of Theorem 4.5 Suppose that $\{U_i\}$ is a constructive null cover relative to Q^* with $N \in \bigcap_i \operatorname{Ext}(U_i)$. We suppress the oracle C. We will exhibit a constructive null cover $\{S_i\}$ (relative to B) of A by describing a procedure for enumerating, uniformly in B, a set S_i such that $A \in \operatorname{Ext}(S_i)$ and $\mathbf{Pr}(S_i) \leq 2^{-i}$. Fix i; we can uniformly obtain an index e for which $U_i = W_e^{Q^*}$. Let e be fixed throughout the remainder of the proof.

The enumeration of S_i may be loosely described in the following way: we "guess" an initial segment $\tau \sqsubseteq Q^*$ and enumerate strings $\sigma \in W_{e,t}^\tau$ for $t = 0, 1, \ldots, |\tau|$ as long as $\mathbf{Pr}(W_{e,t}^\tau) \leq 2^{-i}$. For each pair (σ, τ) we attempt to "reconstruct" an initial segment $\alpha \sqsubseteq A$. That is, we attempt to construct a string $\alpha \in \{0, 1, \bot\}^*$ such that when the place selection is applied to α (stopping when F attempts to examine an undefined bit), the selected subsequence is exactly τ and the nonselected subsequence is exactly σ. S_i then consists of an enumeration of all the strings α obtained for all possible "guesses" τ.

We give below a formal definition of a partial recursive function

$$S : \{0, 1\}^* \times \{0, 1\}^* \to \{0, 1, \bot\}^*$$

which produces α from an input pair (σ, τ). The construction of S can be informally described as follows: During the course of the construction, we define sequences $\hat{\xi}_0 \sqsubseteq \hat{\xi}_1 \sqsubseteq \cdots$ and $\alpha_0 \sqsubseteq \alpha_1 \sqsubseteq \cdots$ of strings. S will be attempting to simulate the action of F and H on the sequence A, and each string $\hat{\xi}_i$ represents what S believes to be the corresponding actual value of the string ξ_i of Definition 4.1. The strings α_i represent approximations to A. The idea is that S will regard τ as an initial segment of Q^* and σ as an initial segment of N; as S reads through τ it uses the value of $F(\hat{\xi}_i)$ to determine the original position that each of the selected bits originally had in A, and in effect what S does is replace each bit of τ in its proper position in α_i. To simulate the action that F and H would have taken on A, S needs the correct value of the bit examined by F at each step. There are only two possibilities at any stage i in the simulation: if $F(\hat{\xi}_i) \geq H(\hat{\xi}_i)$, the correct value should be the next bit of τ. If $F(\hat{\xi}_i) < H(\hat{\xi}_i)$, the positions in α_i to the left of $H(\hat{\xi}_i)$ which have not yet been defined using bits from τ must correspond to bits of N, so they can be filled in with the initial part of σ and the correct value of A can be determined from $\alpha_i \downarrow \sigma$. Obviously if $\tau \not\sqsubseteq Q^*$ or $\sigma \not\sqsubseteq N$, the simulation will be incorrect and if $S(\sigma, \tau)$ converges to some value α, it is unlikely that $\alpha \sqsubseteq A$. The fact that we only consider pairs (σ, τ) for which $\sigma \in W_{e,t}^\tau$ and $\mathbf{Pr}(W_{e,t}^\tau) \leq 2^{-i}$ will be used to ensure that $\mathbf{Pr}(S_i) \leq 2^{-i}$.

Construction of S: At stage 0, let

$$\alpha_0 = \bot^\infty, \quad \hat{\xi}_0 = \lambda, \quad \text{and } t_0 = 0,$$

where t_i is a marker indicating the next unexamined bit of τ.

At stage $k+1$, let $h = H(\hat{\xi}_k)$ and let u be the number of undefined bits in $\alpha_k[0..h-1]$. If $|\sigma| < u$, then the construction diverges and $S(\sigma, \tau)$ is undefined. If $|\sigma| \geq u$ let $\alpha_k^* = \alpha_k \downarrow \sigma[0..u-1]$. If $|\sigma| = u$ and $|\tau| = t_k$, then the construction terminates at stage $k+1$ with value

$$S(\sigma, \tau) = \alpha_k^*.$$

Otherwise one of the following cases applies:

Case 1: $F(\hat{\xi}_k) < h$. Then let

$$
\begin{aligned}
\hat{\xi}_{k+1} &= \hat{\xi}_k \alpha_k^*[F(\hat{\xi}_k)], \\
t_{k+1} &= t_k, \\
\text{and } \alpha_{k+1} &= \alpha_k.
\end{aligned}
$$

10

Case 2: $F(\hat{\xi}_k) \geq h$. If $t_k \geq |\tau|$ then the construction diverges and $S(\sigma, \tau)$ is undefined. Otherwise let

$$\hat{\xi}_{k+1} = \hat{\xi}_k \tau[t_k],$$
$$t_{k+1} = t_k + 1,$$
$$\text{and for all } z \in \mathbb{N}, \; \alpha_{k+1}[z] = \begin{cases} \tau[t_k] & \text{if } z = F(\hat{\xi}_k) \\ \alpha_k[z] & \text{otherwise.} \end{cases}$$

The crucial properties of the function S are summarized in the claim below. The proof of Claim 4.7 is technical, and we will postpone giving the details until the end of this section.

Claim 4.7 *Let A, Q^*, and N be as in Definition 4.1.*

(i) *If $S(\sigma, \tau)$ converges with value α and $S(\sigma', \tau')$ converges with value α', then $\sigma' \sqsubseteq \sigma$ and $\tau' \sqsubseteq \tau$ imply that $\alpha' \sqsubseteq \alpha$.*

(ii) *If $S(\sigma, \tau)$ converges and σ' is a proper initial segment of σ, there is no proper extension τ' of τ for which $S(\sigma', \tau')$ converges.*

(iii) *If $S(\sigma, \tau)$ converges with value α, then $\mathbf{Pr}(\alpha) = 2^{-|\sigma|-|\tau|}$.*

(iv) *If $\tau \sqsubseteq Q^*$ and $\sigma \sqsubseteq N$ and $S(\sigma, \tau)$ converges with value α, then $\alpha \sqsubseteq A$.*

(v) *For any strings $\tau' \sqsubseteq Q^*$ and $\sigma' \sqsubseteq N$, there exist $\sigma, \tau \in \{0,1\}^*$ such that $\tau' \sqsubseteq \tau \sqsubseteq Q^*$, $\sigma' \sqsubseteq \sigma \sqsubseteq N$, and $S(\sigma, \tau)$ converges.*

We next show how to obtain a constructive null cover $\{S_i\}$ of A, given the properties listed above of the function S. First define a recursive function t by

$$t(\tau) = \max\{r \leq |\tau| : \mathbf{Pr}(W_{e,r}^\tau) \leq 2^{-i}\}.$$

Then for $s \in \mathbb{N}$ and $\tau \in \{0,1\}^*$, let

$$S_{i,\tau} = \{S(\sigma, \tau) : \text{For some } \sigma' \sqsubseteq \sigma, \; \sigma' \in W_{e,t(\tau)}^\tau\}$$
$$S_{i,s} = \bigcup_{|\tau| \leq s} S_{i,\tau}$$
$$S_i = \bigcup_s S_{i,s}$$

We need to verify the following two facts.

Claim 4.8 $A \in \mathrm{Ext}(S_i)$.

Proof of Claim 4.8 Since by assumption $N \in \mathrm{Ext}(U_i)$, there is an initial segment $\sigma' \sqsubseteq N$ with $\sigma' \in W_e^{Q^*}$. It follows that for some $\tau' \sqsubseteq Q^*$, $\sigma' \in W_{e,|\tau'|}^{\tau'}$. By Claim 4.7(iv) and (v), there are strings σ, τ such that $\sigma' \sqsubseteq \sigma \sqsubseteq N$, $\tau' \sqsubseteq \tau \sqsubseteq Q^*$, and $S(\sigma, \tau) = \alpha \sqsubseteq A$. Since $\mathbf{Pr}(W_{e,|\tau|}^\tau) \leq \mathbf{Pr}(U_i) \leq 2^{-i}$, it follows that α is enumerated into $S_{i,\tau}$ and hence into S_i. $\bullet$

Claim 4.9 $\mathbf{Pr}(S_i) \leq 2^{-i}$.

Proof of Claim 4.9 Since it is clear that $S_{i,s} \subseteq S_{i,s+1}$ for all s, it suffices to fix s and show that $\mathbf{Pr}(S_{i,s}) \leq 2^{-i}$. For each τ, $|\tau| \leq s$, define a set

$$B(\tau) = \{\sigma : \; S(\sigma, \tau) \text{ converges and some } \sigma' \sqsubseteq \sigma \text{ is in } W_{e,t(\tau)}^\tau\}.$$

11

Note that $S_{i,\tau} = \{S(\sigma, \tau) : \sigma \in B(\tau)\}$ and that

$$S_{i,s} = \{S(\sigma, \tau) : \ |\tau| \le s \text{ and } \sigma \in B(\tau)\}.$$

Define a string $\sigma \in B(\tau)$ to be an *initial* string if there is no proper prefix $\sigma' \sqsubseteq \sigma$ such that $\sigma' \in B(\tau')$ for some $\tau' \sqsubseteq \tau$. Let $B^*(\tau)$ denote the initial strings in $B(\tau)$.

Consider a string τ, $|\tau| \le s$. If $\sigma \in B(\tau)$, there is a unique shortest predecessor $\sigma' \sqsubseteq \sigma$ such that $S(\sigma', \tau')$ converges for some τ' comparable to τ. By Claim 4.7(ii), we may assume that $\tau' \sqsubseteq \tau$. It follows that σ' is an initial string, and if $\sigma' \ne \sigma$ then σ is not an initial string. Then $\bigcup\{B^*(\tau') : \tau' \sqsubseteq \tau\}$ is prefixfree, and so

$$\sum_{\tau' \sqsubseteq \tau} \mathbf{Pr}(B^*(\tau')) = \mathbf{Pr}\left(\bigcup\{B^*(\tau') : \tau' \sqsubseteq \tau\}\right) \le \mathbf{Pr}(W_{e,t(\tau)}^\tau) \le 2^{-i}. \tag{4}$$

It further follows from Claim 4.7(i) that

$$\text{Ext}\{S(\sigma, \tau) : \ |\tau| \le s \text{ and } \sigma \in B(\tau)\} = \text{Ext}\{S(\sigma, \tau) : \ |\tau| \le s \text{ and } \sigma \in B^*(\tau)\}.$$

Then

$$
\begin{aligned}
\mathbf{Pr}(S_{i,s}) &= \mathbf{Pr}\{S(\sigma, \tau) : \ |\tau| \le s \text{ and } \sigma \in B^*(\tau)\} \\
&\le \sum_{\substack{|\tau| \le s \\ \sigma \in B^*(\tau)}} \mathbf{Pr}(S(\sigma, \tau)) \\
&= \sum_{\substack{|\tau| \le s \\ \sigma \in B^*(\tau)}} 2^{-|\sigma| - |\tau|} \quad \text{by Claim 4.7(iii)} \\
&= \sum_{j=0}^{s} \sum_{|\tau| = j} 2^{-|\tau|} \mathbf{Pr}(B^*(\tau)) \\
&\le 2^{-i},
\end{aligned}
$$

where the last inequality follows from (4), using Lemma 4.6 with $f(\tau) = \mathbf{Pr}(B^*(\tau))$. $\bullet$

All that remains is to verify the properties listed in Claim 4.7.

Proof of Claim 4.7. Parts (i) and (ii) are straightforward consequences of the fact that in the construction of S, the inputs are used from left to right. Suppose $S(\sigma, \tau)$ converges to α at stage $k + 1$, and let α_k, $\hat{\xi}_k$, and t_k be the final values of the variables in the construction; suppose also that $S(\sigma', \tau')$ converges to α' at stage $j + 1$ and let α_j, $\hat{\xi}_j$, and t_j be the corresponding final values. Let $h_j = H(\hat{\xi}_j)$ and $h_k = H(\hat{\xi}_k)$. Suppose $\sigma' \sqsubseteq \sigma$ and $\tau' \sqsubseteq \tau$. Since the inputs are used from left to right, the construction of $S(\sigma, \tau)$ is identical to that of $S(\sigma', \tau')$ up to the stage at which the latter converges, i.e., $\alpha_j \sqsubseteq \alpha_k$ and $\hat{\xi}_j \sqsubseteq \hat{\xi}_k$. Since H is nondecreasing, and no bits of α_j to the left of h_j can be defined after stage $j + 1$ in the construction, we know $\alpha_j[0..h_j - 1] = \alpha_k[0..h_j - 1]$. Since the number of undefined bits in $\alpha_j[0..h_j - 1]$ is exactly $|\sigma'|$ (by the definition of the convergence of S), we have

$$\alpha' = (\alpha_j \downarrow \sigma') \sqsubseteq (\alpha_k \downarrow \sigma) = \alpha,$$

which establishes (i).

For (ii), we use the notation of the preceding paragraph, and assume that σ' is a *proper* initial segment of σ and that $\tau \sqsubseteq \tau'$. Again the construction of $S(\sigma, \tau)$ must be identical to that of $S(\sigma', \tau')$ up to the stage at which one of them converges. Suppose that $S(\sigma', \tau')$ converges first, i.e., that $k < j$. Then $\alpha_k \sqsubseteq \alpha_j$, $\hat{\xi}_k \sqsubseteq \hat{\xi}_j$, $h_k \le h_j$, and $\alpha_k[0..h_k - 1] = \alpha_j[0..h_k - 1]$, implying that

$$
\begin{aligned}
|\sigma| &= \ \# \text{ of undefined bits in } \alpha_k[0..h_k - 1] \\
&\ge \ \# \text{ of undefined bits in } \alpha_j[0..h_j - 1] \\
&= \ |\sigma'|,
\end{aligned}
$$

12

contradicting the fact that σ' is a proper initial segment of σ. Therefore $j \leq k$, and so $t_j \leq t_k$ and $|\tau'| \leq |\tau|$, i.e., τ' cannot be a proper extension of τ.

For part (iii), note that when the computation $S(\sigma, \tau)$ converges at a stage $k+1$, exactly $|\tau|$ bits of α_k have been defined, so the value $\alpha = \alpha_k \downarrow \sigma$ has exactly $|\tau| + |\sigma|$ defined bits.

Parts (iv) and (v) involve slightly more work. We first prove inductively that the following conditions (a)–(e) hold. Suppose that $\sigma \sqsubseteq N$ and $\tau \sqsubseteq Q^*$ and $S(\sigma, \tau)$ converges. Then (using the notation of Definition 4.1) at each nonterminating stage k in the computation of $S(\sigma, \tau)$,

(a) $|\xi_k / \rho_k| = t_k$,

(b) $\hat{\xi}_k = \xi_k$,

(c) $\alpha_k \sqsubseteq A$,

(d) for all $z < H(\hat{\xi}_k)$, $\alpha_k[z]$ is defined $\iff B[z] = 1$, and

(e) $\alpha_k^* \sqsubseteq A$.

Base step: When $k = 0$, (a), (b), and (c) are immediate. For (d), note that no bit of A to the left of $H(\lambda)$ is ever selected, so $B[z] = 0$ for $z < H(\lambda)$; also $\alpha_0[z]$ is undefined for all z. For (e), let $h = H(\lambda)$; since α_0 is undefined at all bits,

$$\alpha_0^* = (\alpha_0 \downarrow \sigma[0..h-1]) = \sigma[0..h-1] = N[0..h-1] = A[0..h-1],$$

where the last equality follows from the fact that $B[z] = 0$ for all $z < h$.

Induction step. Suppose (a)–(e) hold for $j \leq k$. For (a), (b), and (c) there are two cases:

Case 1: $F(\hat{\xi}_k) < H(\hat{\xi}_k)$.

(a) By construction $t_k = t_{k+1}$, and since $\hat{\xi}_k = \xi_k$ by the induction hypothesis, $F(\xi_k) < H(\xi_k)$ and so $\rho_k + 1 = \rho_k 0$. Hence

$$|\xi_{k+1}/\rho_{k+1}| = |\xi_k/\rho_k| = t_k = t_{k+1}.$$

(b) By the induction hypothesis, $\alpha_k^* \sqsubseteq A$ and $\hat{\xi}_k = \xi_k$; in view of the latter it is enough to show that the $(k+1)$st bits of $\hat{\xi}_{k+1}$ and ξ_{k+1} are equal:

$$\hat{\xi}_{k+1}[k] = \alpha_k^*[F(\hat{\xi}_k)] = A[F(\xi_k)] = \xi_{k+1}[k].$$

(c) By construction $\alpha_{k+1} = \alpha_k \sqsubseteq A$.

Case 2: $F(\hat{\xi}_k) \geq H(\hat{\xi}_k)$.

(a) By construction $t_k = t_k + 1$, and since $\hat{\xi}_k = \xi_k$ by the induction hypothesis, $F(\xi_k) \geq H(\xi_k)$, so $\rho_k + 1 = \rho_k 1$; hence

$$|\xi_{k+1}/\rho_{k+1}| = |\xi_k/\rho_k| + 1 = t_k + 1 = t_{k+1}.$$

(b) Again $\hat{\xi}_k = \xi_k$ by the induction hypothesis, and since $\xi_{k+1}/\rho_{k+1} \sqsubseteq \tau \sqsubseteq Q^*$,

$$\hat{\xi}_{k+1}[k] = \tau[t_k] = (\xi_{k+1}/\rho_{k+1})[t_k] = \xi_{k+1}[k]. \tag{5}$$

(c) We have $\alpha_k \sqsubseteq A$ by the induction hypothesis, and by construction $\alpha_{k+1}[z] = \alpha_k[z]$ for all $z \neq F(\hat{\xi}_k)$. By (5) above, $\tau[t_k] = \xi_{k+1}[k]$, which is equal to $A[F(\xi_k)]$. Then

$$\alpha_{k+1}[F(\hat{\xi}_k)] = \tau[t_k] = A[F(\xi_k)] = A[F(\hat{\xi}_k)],$$

so $\alpha_{k+1} \sqsubseteq A$.

13

For (d), suppose that $z < H(\hat{\xi}_{k+1})$. Note that $H(\hat{\xi}_{k+1}) = H(\xi_{k+1})$ by (b) above. Then

$$
\begin{aligned}
\alpha_{k+1}[z] \text{ is defined} \quad &\Longleftrightarrow \quad \text{for some } j \le k,\ z = F(\hat{\xi}_j) \ge H(\hat{\xi}_j) \\
&\Longleftrightarrow \quad \text{for some } j \le k,\ z = F(\xi_j) \ge H(\xi_j) \\
&\Longleftrightarrow \quad B[z] = 1.
\end{aligned}
$$

Part (e) follows from (c) and (d): Let $h = H(\hat{\xi}_{k+1})$, $\beta = B[0..h-1]$, and let u denote the number of undefined bits in $\alpha_{k+1}[0..h-1]$. Then

$$
\begin{aligned}
\alpha_{k+1}^*/\beta \quad &= \quad \alpha_{k+1}/\beta \text{ by (d)} \\
&= \quad A/\beta \text{ by (c)}, \\
\text{so} \quad \alpha_{k+1}^*/\overline{\beta} \quad &= \quad \sigma[0..u-1] \\
&= \quad A/\overline{\beta} \text{ since } \sigma \sqsubseteq N = A/\overline{B}.
\end{aligned}
$$

But $\alpha_{k+1}^*/\beta = A/\beta$ and $\alpha_{k+1}^*/\overline{\beta} = A/\overline{\beta}$ imply that $\alpha_{k+1}^*[0..h-1] = A[0..h-1]$. Since $\alpha_{k+1}^*[z] = \alpha_{k+1}[z]$ for all $z \ge h$, we have $\alpha_{k+1}^* \sqsubseteq A$ by (c). This completes the induction.

Now Claim 4.7(iv) follows from part (e), since when $S(\sigma, \tau)$ converges at a stage $k+1$, the final value is $\alpha = \alpha_k^* \sqsubseteq A$.

The final step is to verify part (v) of Claim 4.7. Consider any integer k for which $F(\xi_k) \ge H(\xi_k)$. Let $h = H(\xi_k)$, and let

$$
\begin{aligned}
\tau \quad &= \quad \xi_k/\rho_k & (6) \\
\text{and} \quad \sigma \quad &= \quad A[0..h-1]/\overline{B}. & (7)
\end{aligned}
$$

Clearly $\tau \sqsubseteq Q^*$ and $\sigma \sqsubseteq N$. It is also the case that $S(\sigma, \tau)$ converges: at stage $k+1$ in the construction, we have $t_k = |\xi_k/\rho_k| = |\tau|$ by part (a), $h = H(\hat{\xi}_k) = H(\xi_k)$ by (b), and by (d),

$$
\begin{aligned}
\text{\# of undefined bits in } \alpha_k[0..h-1] \quad &= \quad \text{\# of zeros in } B[0..h-1] \\
&= \quad |\sigma| \qquad \text{by (7)},
\end{aligned}
$$

so $S(\sigma, \tau)$ converges. Since Q^* and N are assumed to be infinite, it is always possible to find a k such that $F(\xi_k) \ge H(\xi_k)$ and such that the strings τ and σ of (6) and (7) are as long as desired; therefore σ and τ can be found which extend any given $\tau' \sqsubseteq Q^*$ and $\sigma' \sqsubseteq N$.

The proof of Claim 4.7, and hence the proof of Theorem 4.5, is now complete. Thank you for your support. ●

References

[1] C. Bennett and J. Gill. Relative to a random oracle, $P^A \ne NP^A \ne \text{co-}NP^A$. *SIAM Journal on Computing*, 10:96–113, 1981.

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

[3] G.J. Chaitin. Incompleteness theorems for random reals. *Advances in Applied Mathematics*, 8:119–146, 1987.

[4] G.J. Chaitin. A theory of program size formally identical to information theory. *J. Assoc. Comput. Mach.*, 22:329–340, 1975.

[5] A. Church. On the concept of a random sequence. *Bulletin of the AMS*, 46:130–135, 1940.

[6] W. Feller. *An Introduction to Probability Theory and its Applications*. Volume 2, John Wiley and Sons, Inc., 1971.

[7] David Ives. Chicken à la Descartes (favorite chicken recipes of the great philosophers). *The New York Times Magazine,* Sunday, September 25, 1994.

[8] S. M. Kautz. *Degrees of Random Sets.* PhD thesis, Cornell University, 1991.

[9] S.M. Kautz and P.B. Miltersen. Relative to a random oracle, NP is not small. In *Structure in Complexity Theory*, 1994.

[10] A.N. Kolmogorov and V.A. Uspenskii. Algorithms and randomness. *Theory Probab. Appl.,* 32(3):389–412, 1987.

[11] S. Kurtz. *Randomness and Genericity in the Degrees of Unsolvability.* PhD thesis, University of Illinois at Urbana-Champaign, 1981.

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

[13] J.H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44:220–258, 1992.

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

[15] P. Odifreddi. *Classical Recursion Theory.* North-Holland, 1989.

[16] H. Rogers, Jr. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, 1967.

[17] C. P. Schnorr. Process complexity and effective random tests. *Journal of Computer and System Sciences*, 7:376–378, 1973.

[18] A. Kh. Shen´. On relations between different algorithmic definitions of randomness. *Soviet Math. Dokl.*, 38(2):316–319, 1989.

[19] R.M. Solovay. 1975. Reported in [3].

[20] J. Stillwell. Decidability of the "almost all" theory of degrees. *Journal of Symbolic Logic*, 37:501–506, 1972.

[21] V.A. Uspenskii, A.L. Semenov, and A. Kh. Shen´. Can an individual sequence of zeros and ones be random? *Russian Math Surveys*, 45:121–189, 1990.

[22] M. van Lambalgen. The axiomatization of randomness. *Journal of Symbolic Logic*, 55:1143–1167, 1990.

[23] M. van Lambalgen. Von Mises' definition of random sequences reconsidered. *Journal of Symbolic Logic*, 52(3):725–755, 1987.

[24] R. von Mises. *Probability, Statistics and Truth.* George Allen & Unwin Ltd., 1957. Reprinted by Dover Publications, New York, NY in 1981. Originally published in German by J. Springer in 1928.