# Genericity and Randomness over Feasible Probability Measures[*]

Amy K. Lorentz[†] and Jack H. Lutz[‡]

## Abstract

This paper investigates the notion of resource-bounded genericity developed by Ambos-Spies, Fleischhack, and Huwig. Ambos-Spies, Neis, and Terwijn have recently shown that every language that is $t(n)$-random over the uniform probability measure is $t(n)$-generic. It is shown here that, in fact, every language that is $t(n)$-random over *any* strongly positive, $t(n)$-computable probability measure is $t(n)$-generic. Roughly speaking, this implies that, when genericity is used to prove a resource-bounded measure result, the result is not specific to the underlying probability measure.

[*] This research was supported in part by National Science Foundation Grant CCR-9157382, with matching funds from Rockwell, Microware Systems Corporation, and Amoco Foundation.

[†] Color LaserJet and Consumables Division, Hewlett-Packard Company, Boise, ID 83714, U.S.A. E-mail: amy_lorentz@hp-boise-om8.om.hp.com

[‡] Department of Computer Science, Iowa State University, Ames, IA 50011, U.S.A. E-mail: lutz@cs.iastate.edu

# 1 Introduction

In the 1990's, the development and application of resource-bounded measure – a complexity-theoretic generalization of classical Lebesgue measure developed by Lutz [14] – has shed new light on some of the most central questions in computational complexity. Progress that has resulted from the use of resource-bounded measure – by now the work of many investigators – has been surveyed in [15, 4].

Recently, Ambos-Spies, Neis, and Terwijn [6] have observed that the notion of time-bounded genericity developed by Ambos-Spies, Fleischhack, and Huwig [3] interacts informatively with resource-bounded measure. In fact, this notion of genericity, which (like its recursion-theoretic precursors) was originally formulated as a uniform method for carrying out all diagonalization strategies of a certain strength, provides a new method for proving results on resource-bounded measure. This method, first discovered and applied by Ambos-Spies, Neis, and Terwijn [6] has since been applied by Ambos-Spies [1, 2] and Ambos-Spies and Mayordomo [4]. Time-bounded genericity has also been characterized as a kind of strong immunity property by Balcázar and Mayordomo [8]. Recently, a strengthened version of genericity, called balanced genericity, has been shown by Ambos-Spies, Mayordomo, Wang, and Zheng [5] to give an exact characterization of time-bounded Church stochasticity. The reader is referred to the surveys [2, 4, 10] for discussions of these developments, and of the relationship between this notion of genericity and some other kinds of genericity that have been used in computational complexity. (In this paper, the term "genericity" is reserved for the notion developed by Ambos-Spies, Fleischhack, and Huwig [3].)

The crux of the relationship between genericity and resource-bounded measure is the pair of facts, proven by Ambos-Spies, Neis, and Terwijn [6], that, for fixed $k \in \mathbf{N}$, the $n^k$-generic languages form a measure 1 subset of the complexity class $\mathrm{E} = \mathrm{DTIME}(2^{\mathrm{linear}})$, and the $2^{(\log n)^k}$-generic languages form a measure 1 subset of $\mathrm{E}_2 = \mathrm{DTIME}(2^{\text{polynomial}})$. To put the matter differently, almost every language in E is $n^k$-generic, which is written

$$\mu\left(\mathrm{GEN}(n^k) \middle| \mathrm{E}\right) = 1, \tag{1}$$

and almost every language in $\mathrm{E}_2$ is $2^{(\log n)^k}$-generic, which is written

$$\mu\left(\mathrm{GEN}(2^{(\log n)^k}) \middle| \mathrm{E}_2\right) = 1. \tag{2}$$

This pair of facts is also the crux of the method for using genericity to prove resource-bounded measure results. For example, if one wants to prove that a certain set $X$ of languages has measure 0 in E (written $\mu\left(X \middle| \mathrm{E}\right) = 0$), it suffices by (1) to prove that, for some fixed $k \in \mathbf{N}$, $X \cap \mathrm{E}$ does not contain any $n^k$-generic language.

As it turns out, facts (1) and (2) both follow from a single, tight relationship between time-bounded genericity and the time-bounded randomness concepts investigated by Schnorr [17, 18, 19, 20] some 25 years ago. Specifically, Ambos-Spies, Neis, and Terwijn [6] showed that, for every time bound $t : \mathbf{N} \to \mathbf{N}$, every $t(n)$-random language is $t(n)$-generic, i.e.,

$$\mathrm{RAND}(t(n)) \subseteq \mathrm{GEN}(t(n)). \tag{3}$$

(Note: The actual statement in [6] is that $\mathrm{RAND}(\widetilde{t}(n)) \subseteq \mathrm{GEN}(t(n))$, where $\widetilde{t}(n)$ is enough larger that $t(n)$ to handle some computational simulation tasks. It was then shown in [4] that, with a more careful formulation of these classes, the argument in [6] can be made to achieve (3).) Facts (1) and (2) follow immediately from (3) and the known facts [14, 7] that almost every language in E is $n^k$-random, and almost every language in $\mathrm{E}_2$ is $2^{(\log n)^k}$-random.

Ambos-Spies, Neis, and Terwijn [6] also pointed out that inclusion (3) is proper, i.e.,

$$\mathrm{RAND}(t(n)) \subsetneq \mathrm{GEN}(t(n)) \tag{4}$$

for $t(n) \geq n^2$. In fact, they noted that the genericity method is weaker than direct measure or randomness arguments, in the sense that there are sets of interest in computational complexity that have measure 0 in E, but that cannot be proven to have measure 0 in E by this genericity method.

All the results mentioned thus far involve resource-bounded measure and randomness over the *uniform probability measure* $\mu$ on the set $\mathbf{C}$ of all languages. This corresponds to the random experiment in which a language $A \subseteq \{0,1\}^*$ is chosen by using an *independent* toss of a *fair* coin to decide membership of each string in $A$.

In this paper, we investigate the relationship between time-bounded genericity and time-bounded randomness (and measure) over more general probability measures on $\mathbf{C}$. Probability measures other than the uniform probability measure occur naturally in applications, were incorporated by Schnorr [17, 19] into the theory of resource-bounded randomness, and have recently been incorporated by Lutz and Breutzmann [9] into resource-bounded measure.

In our main theorem, we generalize (3) by proving that, for every time bound $t : \mathbf{N} \rightarrow \mathbf{N}$, every language that is $t(n)$-random over *any* strongly positive $t(n)$-time computable probability measure $\nu$ on $\mathbf{C}$ is $t(n)$-generic. That is,

$$\mathrm{RAND}_\nu(t(n)) \subseteq \mathrm{GEN}(t(n)) \tag{5}$$

holds for *every* such probability measure $\nu$. Thus, not only is $t(n)$-genericity weaker than $t(n)$ randomness over the uniform probability measure (as indicated by (4)), but it is *simultaneously* weaker than *all* $t(n)$-randomness notions over strongly positive, $t(n)$-computable probability measures.

Just as (5) is stronger than (3), so are the consequences of (5) for measure in complexity classes stronger than (1) and (2). We show in this paper that, for every positive, p-computable probability measure $\nu$ on $\mathbf{C}$, the languages that are $n^k$-random over $\nu$ form a

$\nu$-measure 1 subset of E. It follows by (5) that, for every strongly positive, p-computable probability measure $\nu$ on $\mathbf{C}$,

$$\nu(\mathrm{GEN}(n^k)\Big|\mathrm{E}) = 1, \tag{6}$$

i.e., $\nu$-almost every language in E is $n^k$-generic. Similarly, we show that, for every strongly positive, $\mathrm{p}_2$-computable probability measure $\nu$ on $\mathbf{C}$,

$$\nu(\mathrm{GEN}(2^{(\log n)^k})\Big|\mathrm{E}_2) = 1, \tag{7}$$

i.e., $\nu$-almost every language in $\mathrm{E}_2$ is $2^{(\log n)^k}$-generic.

What do these results say about the genericity method for proving theorems on measure in complexity classes? Viewed from the standpoint of the uniform probability measure (or any other particular strongly positive, p-computable probability measure), these results say that the genericity method is much weaker than direct martingale arguments. However, viewed from the standpoint of strongly positive, p-computable probability measures in general, (6) and (7) say that the genericity method is *very* powerful. For example, (6) says that, if we can prove that no element of $X \cap \mathrm{E}$ is $n^k$-generic, then it follows that $X$ has $\nu$-measure 0 in E for *every* strongly positive, p-computable probability measure $\nu$ on $\mathbf{C}$.

This paper is largely self-contained. In section 2, we introduce notation and review the notion of genericity developed by Ambos-Spies, Fleischhack, and Huwig [3]. In section 3, we review the notion of time-bounded randomness developed by Schnorr [17, 18, 19, 20], prove our main theorem on time-bounded genericity and time-bounded randomness over feasible probability measures, and derive and discuss the consequences of this theorem for resource-bounded measure. In section 4 we make a brief closing remark.

In order to simplify the exposition of the main ideas, we do not state our results in the strongest possible form in this volume. The technical paper [13] gives a more thorough treatment of these matters.

# 2 Preliminaries

## 2.1 Notation

We write $\{0,1\}^*$ for the set of all (finite, binary) *strings*, and we write $|w|$ for the length of a string $w$. The empty string, $\lambda$, is the unique string of length 0. The *standard enumeration* of $\{0,1\}^*$ is the sequence $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, \ldots$, ordered first by length and then lexicographically. For $w \in \{0,1\}^*$ and $0 \leq n < |w|$, $w[n]$ denotes the $n^{\text{th}}$ bit of $w$. (The leftmost bit of $w$ is $w[0]$.)

The *Boolean value* of a condition $\phi$ is $[\![\phi]\!] = \textbf{if } \phi \textbf{ then } 1 \textbf{ else } 0$.

We work in the *Cantor space* $\mathbf{C}$, consisting of all *languages* $A \subseteq \{0,1\}^*$. We identify each language $A$ with its *characteristic sequence*, which is the (infinite, binary) sequence $A$ whose $n^{\text{th}}$ bit is $[\![s_n \in A]\!]$ for each $n \in \mathbf{N}$. (The leftmost bit of $A$ is the $0^{\text{th}}$ bit.)

Relying on this identification, we also consider $\mathbf{C}$ to be the set of all sequences.

A string $w$ is a *prefix* of a sequence $A$, and we write $w \sqsubseteq A$, if there is a sequence $B$ such that $A = wB$. We write $A[0..n-1]$ for the $n$-bit prefix of $A$. For each string $w \in \{0,1\}^*$, the *cylinder generated by* $w$ is the set

$$\mathbf{C}_w = \left\{ A \in \mathbf{C} \;\middle|\; w \sqsubseteq A \right\}.$$

Note that $\mathbf{C}_\lambda = \mathbf{C}$.

## 2.2 Genericity

We briefly review the notion of time-bounded genericity introduced by Ambos-Spies, Fleishhack, and Huwig [3]. For more motivation and discussion, and for comparisons with other notions of genericity that have been used in computational complexity, the reader is referred to [2, 4, 10].

A *condition* is a set $C \subseteq \{0,1\}^*$, i.e., a language. A language $A \subseteq \{0,1\}^*$ *meets* a condition $C$ if some prefix of (the characteristic sequence of) $A$ is an element of $C$. A condition $C$ is *dense along* a language $A \subseteq \{0,1\}^*$ if $A$ has infinitely many prefixes $w$ for which $\{w0, w1\} \cap C \neq \emptyset$. A condition $C$ is *dense* if it is dense along every language.

**Definition** (Ambos-Spies, Fleischhack, and Huwig [3]). Let $\mathcal{C}$ be a class of conditions. A language $A \subseteq \{0,1\}^*$ is $\mathcal{C}$-*generic*, and we write $A \in \mathrm{GEN}(\mathcal{C})$, if $A$ meets every condition in $\mathcal{C}$ that is dense along A.

We are primarily interested in $\mathcal{C}$-genericity when $\mathcal{C}$ is a time complexity class.

**Definition** (Ambos-Spies, Fleischhack, and Huwig [3]) Let $t : \mathbf{N} \to \mathbf{N}$. A language $A \subseteq \{0,1\}^*$ is $t(n)$-*generic* if $A$ is DTIME($t(n)$)-generic.

We close this section with a single expository example, due to Ambos-Spies, Neis, and Terwijn [6]. If $\mathcal{C}$ is a class of languages, recall that a language $A \subseteq \{0,1\}^*$ is $\mathcal{C}$-*bi-immune* if neither $A$ nor $A^c = \{0,1\}^* - A$ contains an infinite element of $\mathcal{C}$. If $t : \mathbf{N} \to \mathbf{N}$, then we say that $A$ is $t(n)$-bi-*immune* if $A$ is DTIME($t(n)$)-bi-immune.

**Example** (Ambos-Spies, Neis, and Terwijn [6]) If $c \geq 2$, then every $n^c$-generic language is $2^{cn}$-bi-immune.

**Proof.** Let $c \geq 2$, and let $A \subseteq \{0,1\}^*$ be $n^c$-generic. To see that $A$ is $2^{cn}$-bi-immune, let $B$ be an infinite element of DTIME($2^{cn}$), and let $b \in \{0,1\}$. Define the condition

$$C = \left\{ wb \,\middle|\, w \in \{0,1\}^* \text{ and } s_{|w|} \in B \right\}.$$

The predicate "$s_{|w|} \in B$" is decidable in $O(2^{c|s_{|w|}|}) = O(|w|^c)$ time, so $C \in \mathrm{DTIME}(n^c)$. Also, for all $D \subseteq \{0,1\}^*$ and $s_n \in B$, $D[0...n-1]b \in C$. Since $A$ is infinite, this implies that $C$ is dense. Since $A$ is $n^c$-generic it follows that $A$ meets $C$. Since this holds for $b = 0$, $B$ cannot be a subset of $A$. Since it holds for $b = 1$, $B$ cannot be a subset of $A^c$. □

# 3 Genericity and $\nu$-Randomness

In this section, we prove our main result, that every language that is $t(n)$-random over a strongly positive, $t(n)$-computable probability measure is $t(n)$-generic. We also briefly discuss the implications of this result for the use of resource-bounded genericity in proving theorems about resource-bounded measure.

## 3.1 Randomness over Feasible Probability Measures

Before proving our main result, we review the notion of time-bounded randomness over a given probability measure as developed by Schnorr [17, 19]. More complete expositions of the ideas reviewed here may be found in [19, 21, 4].

We first recall the well-known notion of a (Borel) probability measure on $\mathbf{C}$.

**Definition.** A *probability measure* on $\mathbf{C}$ is a function

$$\nu : \{0,1\}^* \to [0,1]$$

such that $\nu(\lambda) = 1$, and for all $w \in \{0,1\}^*$,

$$\nu(w) = \nu(w0) + \nu(w1).$$

Intuitively, $\nu(w)$ is the probability that $A \in \mathbf{C}_w$ when we "choose a language $A \in \mathbf{C}$ according to the probability measure $\nu$." We sometimes write $\nu(\mathbf{C}_w)$ for $\nu(w)$.

**Examples.**

1. A *sequence of biases* is a sequence $\vec{\beta} = (\beta_0, \beta_1, \beta_2, \ldots)$, where each $\beta_i \in [0,1]$. Given a sequence of biases $\vec{\beta}$, the *$\vec{\beta}$-coin-toss probability measure* (also called the *$\vec{\beta}$-product probability measure*) is the probability measure $\mu^{\vec{\beta}}$ defined by
$$\mu^{\vec{\beta}}(w) = \prod_{i=0}^{|w|-1} ((1-\beta_i)\cdot(1-w[i]) + \beta_i \cdot w[i])$$
for all $w \in \{0,1\}^*$. If $\beta = \beta_0 = \beta_1 = \beta_2 = \ldots$, then we write $\mu^\beta$ for $\mu^{\vec{\beta}}$. In this case, we have the simpler formula
$$\mu^\beta(w) = (1-\beta)^{\#(0,w)} \cdot \beta^{\#(1,w)},$$
where $\#(b,w)$ denotes the number of $b$'s in $w$. If $\beta = \frac{1}{2}$ here, then we have the *uniform probability measure* $\mu = \mu^{\frac{1}{2}}$, which is defined by
$$\mu(w) = 2^{-|w|}$$
for all $w \in \{0,1\}^*$. (We always reserve the symbol $\mu$ for the meanings assigned in this example.)

2. The function $\nu$ defined by the recursion
$$\begin{aligned}\nu(\lambda) &= 1\\ \nu(0) &= \nu(1) = 0.5\end{aligned}$$
$$\nu(wab) = \begin{cases} 0.7\nu(wa) & \text{if } a \neq b \\ 0.3\nu(wa) & \text{if } a = b\end{cases}$$

(for $w \in \{0,1\}^*$ and $a, b \in \{0,1\}$) is also a probability measure on $\mathbf{C}$.

Intuitively, $\mu^{\vec{\beta}}(w)$ is the probability that $w \sqsubseteq A$ when the language $A \subseteq \{0,1\}^*$ is chosen probabilistically according to the following random experiment. For each string $s_i$ in the standard enumeration $s_0, s_1, s_2, \ldots$ of $\{0,1\}^*$, we (independently of all other strings) toss a special coin, whose probability is $\beta_i$ of coming up heads, in which case $s_i \in A$, and $1 - \beta_i$ of coming up tails, in which case $s_i \notin A$. The probability measure $\nu$ above is a simple example of a probability measure that does not correspond to independent coin tosses in this way.

**Definition.** A probability measure $\nu$ on $\mathbf{C}$ is *positive* if, for all $w \in \{0,1\}^*$, $\nu(w) > 0$.

**Definition.** If $\nu$ is a positive probability measure and $u, v \in \{0,1\}^*$, then the *conditional $\nu$-measure of $u$ given $v$* is

$$\nu(u|v) = \begin{cases} 1 & \text{if } u \sqsubseteq v \\ \frac{\nu(u)}{\nu(v)} & \text{if } v \sqsubseteq u \\ 0 & \text{otherwise.} \end{cases}$$

That is, $\nu(u|v)$ is the conditional probability that $A \in \mathbf{C}_u$, given that $A \in \mathbf{C}_v$, when $A \in \mathbf{C}$ is chosen according to the probability measure $\nu$.

In this paper, we are especially concerned with the following special type of probability measure.

**Definition.** A probability measure $\nu$ on $\mathbf{C}$ is *strongly positive* if $\nu$ is positive and there is a constant $\delta > 0$ such that, for all $w \in \{0,1\}^*$ and $b \in \{0,1\}$, $\nu(wb|w) \geq \delta$. (Equivalently, for all such $w$ and $b$, $\nu(wb|w) \in [\delta, 1 - \delta]$.)

The following relation between probability measures is useful in many contexts.

**Definition.** If $\nu$ and $\rho$ are probability measures on $\mathbf{C}$, then $\nu$ *dominates* $\rho$ if there is a real number $\alpha > 0$ such that, for all $w \in \{0,1\}^*$, $\nu(w) \geq \alpha\rho(w)$.

**Construction 3.1.** Given a sequence $\rho_0, \rho_1, \rho_2, ...$ of probability measures on $\mathbf{C}$, define functions $f, \tilde{\rho} : \{0,1\}^* \to \mathbf{R}$ by

$$\begin{aligned} f(w) &= \sum_{i=0}^{|w|} 4^{-(i+1)}\rho_i(w), \\ \tilde{\rho}(\lambda) &= 1, \\ \tilde{\rho}(w0) &= f(w0) + r_{|w|+1}, \\ \tilde{\rho}(w1) &= \tilde{\rho}(w) - \tilde{\rho}(w0), \end{aligned}$$

where $r_k = \frac{2^{k+1}+1}{4^{k+1}}$ for each $k \in \mathbf{N}$.

**Lemma 3.2.** If $\rho_0, \rho_1, \rho_2, ...$ are probability measures on $\mathbf{C}$, then $\tilde{\rho}$ is a probability measure on $\mathbf{C}$ that dominates each of the probability measures $\rho_i$.

**Proof** (sketch). A routine induction shows that, for all $w \in \{0,1\}^*$,

$$\tilde{\rho}(w) \geq f(w) + r_{|w|}. \tag{8}$$

In particular, this implies that each $\tilde{\rho}(w) \geq 0$. Since Construction 3.1 immediately implies that $\tilde{\rho}(\lambda) = 1$ and each $\tilde{\rho}(w) = \tilde{\rho}(w0) + \tilde{\rho}(w1)$, it follows that $\tilde{\rho}$ is a probability measure on $\mathbf{C}$. To see that $\tilde{\rho}$ dominates each $\rho_i$, fix $i \in \mathbf{N}$. Then (8) implies that, for all $w \in \{0,1\}^*$ with $|w| \geq i$,

$$\tilde{\rho}(w) \geq f(w) \geq 4^{-(i+1)}\rho_i(w).$$

It follows readily from this that $\tilde{\rho}$ dominates $\rho_i$. □

To ensure clarity, we restrict attention to probability measures with rational values that are exactly computable within a specified time bound.

**Definition.** Let $t : \mathbf{N} \to \mathbf{N}$. A probability measure $\nu$ on $\mathbf{C}$ is $t(n)$-*exact* if

$$\nu = \{0,1\}^* \to \mathbf{Q} \cap [0,1]$$

and there is an algorithm that, for all $w \in \{0,1\}^*$, computes $\nu(w)$ in $O(t(|w|))$ steps.

**Examples** (revisited). The uniform probability measure $\mu$ is clearly $t(n)$-exact for $t(n) \geq n$, as is the probability measure $\mu^\beta$, provided that $\beta \in \mathbf{Q} \cap [0,1]$. In contrast, even if the biases in the sequence $\vec{\beta} = (\beta_0, \beta_1, ...)$ are all rational, $\mu^{\vec{\beta}}$ will fail to be $t(n)$-exact if the computation of $\beta_i$ from $i$ is too difficult (or impossible). The probability measure $\nu$ of the preceding example is $t(n)$-exact for $t(n) \geq n$.

**Definition.** A probability measure $\nu$ on $\mathbf{C}$ is p-exact if $\nu$ is $n^k$-exact for some $k \in \mathbf{N}$. A probability measure $\nu$ on $\mathbf{C}$ is $\mathrm{p}_2$-*exact* if $\nu$ is $2^{(\log n)^k}$-exact for some $k \in \mathbf{N}$.

We next review the well-known notion of a martingale over a probability measure $\nu$. Computable martingales were used by Schnorr [17, 18, 19, 20] in his investigations of randomness, and have more recently been used by Lutz [14] in the development of resource-bounded measure.

**Definition.** If $\nu$ is a probability measure on $\mathbf{C}$, then a $\nu$-*martingale* is a function $d : \{0,1\}^* \longrightarrow [0,\infty)$ such that, for all $w \in \{0,1\}^*$,

$$d(w)\nu(w) = d(w0)\nu(w0) + d(w1)\nu(w1). \tag{9}$$

A $\mu$-martingale is even more simply called a *martingale.* (That is, when the probability measure is not specified, it is assumed to be the uniform probability measure $\mu$.)

Intuitively, a $\nu$-martingale $d$ is a "strategy for betting" on the successive bits of (the characteristic sequence of) a language $A \in \mathbf{C}$. The real number $\nu(\lambda)$ is regarded as the amount of money that the strategy starts with. The real number $\nu(w)$ is the amount of money that the strategy has after betting on a prefix $w$ of $\chi_A$. The identity (9) ensures that the betting is "fair" in the sense that, if $A$ is chosen according to the probability measure $\nu$, then the expected amount of money is constant as the betting proceeds. Of course, the "objective" of a strategy is to win a lot of money.

**Definition.** A $\nu$-martingale $d$ *succeeds* on a language $A \in \mathbf{C}$ if

$$\limsup_{n \to \infty} d(A[0...n-1]) = \infty.$$

If $d$ is any $\nu$-martingale satisfying $d(\lambda) > 0$, then (9) implies that the function $\rho$ defined by

$$\rho(w) = \frac{d(w)\nu(w)}{d(\lambda)}$$

for all $w \in \{0,1\}^*$ is a probability measure on $\{0,1\}^*$. In fact, for positive $\nu$, it is easy to see (and has long been known [21]) that the set of all $\nu$-martingales is precisely the set of all functions $d$ of the form

$$d = \alpha \frac{\rho}{\nu},$$

where $\alpha \in [0, \infty)$ and $\rho$ is a probability measure on $\mathbf{C}$. It simplifies our presentation to use this idea in the following definition.

**Definition.** Let $\nu$ be a positive probability measure on $\mathbf{C}$, and let $t : \mathbf{N} \to \mathbf{N}$. A $\nu$-martingale $d$ is $t(n)$-*exact* if the function

$$\rho = d\nu \tag{10}$$

is a $t(n)$-exact probability measure on $\mathbf{C}$. A $\nu$-martingale is p-*exact* if it is $n^k$-exact for some $k \in \mathbf{N}$, and is $\mathrm{p}_2$-*exact* if it is $2^{(\log n)^k}$-exact for some $k \in \mathbf{N}$.

**Remarks.**

1. If $\nu$ is positive, we usually write equation 10 in the more suggestive form
$$d = \frac{\rho}{\nu}.$$

2. In any case, (9) ensures that every $t(n)$-exact martingale $d$ satisfies $d(\lambda) = 1$.

3. The above definition does *not* require a $t(n)$-exact martingale to itself be computable in $O(t(n))$ time. For example, if $\nu$ is a positive, uncomputable probability measure on $\mathbf{C}$, then the martingale $d = \frac{\mu}{\nu}$, i.e.,
$$d(w) = \frac{1}{2^{|w|}\nu(w)},$$
is $t(n)$-exact for all $t(n) \geq n$, but $d$ is certainly not computable. Essentially, in defining the time complexity of a $\nu$-martingale $d = \frac{\rho}{\nu}$, we only consider the time complexity of $\rho$, which we think of as the "strategy" of the martingale $d$. The probability measure $\nu$ is the "environment" of $d$, and we do not "charge" $d$ for the complexity of its environment. In any event, this issue does not concern us here, because the probability measures $\nu$ in our results are themselves $t(n)$-exact.

Time-bounded randomness is defined as follows.

**Definition.** Let $\nu$ be a probability measure on $\mathbf{C}$, and let $t : \mathbf{N} \rightarrow \mathbf{N}$. A language $A \in \mathbf{C}$ is *$t(n)$-random over $\nu$*, or *$t(n)$-$\nu$-random*, and we write $A \in \mathrm{RAND}_\nu(t(n))$, if there is no $t(n)$-exact $\nu$-martingale that succeeds on $A$.

**Definition.** Let $\nu$ be a probability measure on $\mathbf{C}$. A language $A \in \mathbf{C}$ is p-*random over $\nu$*, or p-*$\nu$-random*, and we write $A \in \mathrm{RAND}_\nu(\mathrm{p})$, if $A$ is $n^k$-random for all $k \in \mathbf{N}$.

The notion of $t(n)$-$\nu$-randomness is not robust. Its exact meaning – like the meaning of $O(t(n))$-time computation – is sensitive to details of the underlying model of computation. The meaning of time-bounded randomness is also sensitive to details of the definition, such as whether the martingale may be approximated or must be computed exactly, and how the complexity of the probability measure $\nu$ is taken into account. Fortunately, these sensitivities are less than the notion's sensitivity to small changes in the time bound $t(n)$, so the notion of p-$\nu$-randomness *is* robust. That is, for each p-exact probability measure $\nu$, the class $\mathrm{RAND}_\nu(\mathrm{p})$ is the same for all reasonable choices of the underlying computational model and all reasonable variants of the definition of $\mathrm{RAND}_\nu(t(n))$.

When the probability measure is $\mu$, the uniform probability measure, we usually omit it from the above notation and terminology, referring simply to the class $\mathrm{RAND}_\nu(t(n))$, consisting of all $t(n)$-random languages, and the set $\mathrm{RAND}(\mathrm{p})$, consisting of all p-random languages.

## 3.2 $\nu$-Random Languages are Generic

Ambos-Spies, Neis, and Terwijn [6] have shown that every language that is $t(n)$-random over the uniform probability measure is $t(n)$-generic. The following theorem extends this result to arbitrary, strongly positive, $s(n)$-exact probability measures on $\mathbf{C}$.

**Theorem 3.3.** Let $s, t : \mathbf{N} \to \mathbf{N}$. If $\nu$ is a strongly positive, $s(n)$-exact probability measure on $\mathbf{C}$, then every $(s(n)+t(n))$-$\nu$-random language is $t(n)$-generic.

**Proof.** Assume the hypothesis, fix $\delta > 0$ such that $\nu(wb|w) \geq \delta$ for all $w \in \{0,1\}^*$ and $b \in \{0,1\}$, and let $A$ be a language that is $(s(n)+t(n))$-random over $\nu$. To see that $A$ is $t(n)$-generic, let $C$ be a $t(n)$-condition that is dense along $A$. Define a probability measure $\rho$ on $C$ by

$$\rho(wb|w) = \begin{cases} 1 & \text{if } wb \notin C \text{ and } w\overline{b} \in C \\ 0 & \text{if } wb \in C \text{ and } w\overline{b} \notin C \\ \nu(wb|w) & \text{otherwise} \end{cases}$$

for all $w \in \{0,1\}^*$ and $b \in \{0,1\}$, and let $d = \frac{\rho}{\nu}$. Then $\rho$ is an $(s(n)+t(n))$-exact probability measure, so $d$ is an $(s(n)+t(n))$-exact $\nu$-martingale. Since $A$ is $(s(n)+t(n))$-random over $\nu$, it follows that $d$ does not succeed on $A$.

Since $C$ is dense along $A$, the set

$$S = \left\{ wb \sqsubseteq A \,\middle|\, w \in \{0,1\}^*, b \in \{0,1\}, \text{ and } wb \in C \text{ or } w\overline{b} \in C \right\}$$

is infinite. We can partition $S$ into the three sets

$$\begin{aligned} S_{01} &= \left\{ wb \in S \,\middle|\, wb \notin C \right\}, \\ S_{10} &= \left\{ wb \in S \,\middle|\, w\overline{b} \notin C \right\}, \\ S_{11} &= \left\{ wb \in S \,\middle|\, wb \in C \text{ and } w\overline{b} \in C \right\} \end{aligned}$$

We have two cases.

Case 1. $S_{10} \neq \emptyset$. Then we immediately have that $A$ meets the condition $C$.

Case 2. $S_{10} = \emptyset$. Then for every prefix $wb$ of $A$, $\rho(wb|w) \geq \nu(wb|w)$, so

$$d(wb) = \frac{\rho(w)\rho(wb|w)}{\nu(w)\nu(wb|w)} \geq d(w)$$

Thus the values of the $\nu$-martingale $d$ are psoitive and nondecreasing along $A$. Also, for every $wb \in S_{01}$,

$$d(wb) = \frac{\rho(w)\rho(wb|w)}{\nu(w)\nu(wb|w)} = \frac{d(w)}{\nu(wb|w)} \geq \frac{d(w)}{1-\delta} > (1+\delta)d(w).$$

Since $d$ does not succeed on $A$, it follows that the set $S_{01}$ must be finite. Since $S$ is infinite and $S_{10} = \emptyset$, this implies that $S_{11} \neq \emptyset$, whence $A$ meets the condition $C$.

Since $A$ meets $C$ in either case, it follows that $A$ is $t(n)$-generic. □

**Corollary 3.4.** let $t : \mathbf{N} \to \mathbf{N}$. If $\nu$ is a strongly positive, $t(n)$-exact probability measure on $\mathbf{C}$, then every $t(n)$-$\nu$-random language is $t(n)$-generic.

**Proof.** This follows immediately from Theorem 3.3 with $s(n) = t(n)$. □

Fix a time bound $t(n) \geq n^2$. For the uniform probability measure, in addition to proving that $\mathrm{RAND}(t(n)) \subseteq \mathrm{GEN}(t(n))$, Ambos-Spies, Neis, and Terwijn [6] proved that this inclusion is proper, by establishing the existence of sparse $t(n)$-generic languages. It is easy to see that any language $A$ that is $t(n)$-random over a strongly positive, $t(n)$-exact probability measure $\nu$ on $\mathbf{C}$ must satisfy the condition

$$\delta \leq \liminf_{n\to\infty} \frac{\#(1, A[0..n])}{n+1} \leq \limsup_{n\to\infty} \frac{\#(1, A[0..n])}{n+1} \leq 1 - \delta \qquad (11)$$

for every witness $\delta > 0$ to the strong positivity of $\nu$, where $\#(1, w)$ is the number of 1's in the string $w$. Since no sparse language can satisfy inequality (11), the existence of a sparse $t(n)$-generic language also shows that there are $t(n)$-generic languages that are not $t(n)$-random over any strongly positive, $t(n)$-exact probability measure. Thus the converses of Theorem 3.3 and Corollary 3.4 do not hold.

For each rational bias $\beta \in \mathbf{Q} \cap (0, 1)$, let $\mathrm{RAND}_\beta(t(n)) = \mathrm{RAND}_{\mu^\beta}(t(n))$, where $\mu^\beta$ is the coin-toss probability measure defined in section 3.1. It is well-known (and easy to see) that every $A \in \mathrm{RAND}_\beta(t(n))$ satisfies the condition

$$\lim_{n\to\infty} \frac{\#(1, A[0..n])}{n+1} = \beta$$

In particular, this implies that, for all $\alpha, \beta \in \mathbf{Q} \cap (0, 1)$,

$$\alpha \neq \beta \Longrightarrow \mathrm{RAND}_\alpha(t(n)) \cap \mathrm{RAND}_\beta(t(n)) = \emptyset. \qquad (12)$$

By Theorem 3.3 and the existence of sparse $t(n)$-generic languages,

$$\bigcup_{\beta \in \mathbf{Q} \cap (0,1)} \mathrm{RAND}_\beta(t(n)) \overset{\subset}{\neq} \mathrm{GEN}(t(n)),$$

and the union on the left is disjoint by (12). In this sense, $t(n)$-genericity is *much* weaker then $t(n)$-randomness over the uniform probability measure.

## 3.3 Genericity and $\nu$-Measure

In order to discuss the implications of Theorem 3.3 for resource-bounded measure proofs, we briefly review the notions of resource-bounded measure and measure in complexity classes, developed by Lutz [14] over the uniform probability measure, and recently extended by Breutzmann and Lutz [9] to more general probability measures. The reader is referred to [15, 4, 9] for more complete discussions of this material.

**Definition.** Let $\nu$ be a p-exact probability measure on $\mathbf{C}$, and let $X \subseteq \mathbf{C}$.

1. $X$ has *p-$\nu$-measure* 0, and we write $\nu_\mathrm{p}(X) = 0$, if there is a p-exact $\nu$-martingale $d$ that succeeds on every element of $X$.

2. $X$ has *p-$\nu$-measure* 1, and we write $\nu_\mathrm{p}(X) = 1$, if $\nu_\mathrm{p}(X^c) = 0$, where $X^c = \mathbf{C} - X$.

3. $X$ has *$\nu$-measure* 0 *in* E, and we write $\nu(X|\mathrm{E}) = 0$, if $\nu_\mathrm{p}(X \cap \mathrm{E}) = 0$.

4. $X$ has *$\nu$-measure* 1 *in* E, and we write $\nu(X|\mathrm{E}) = 1$, if $\nu(X^c|\mathrm{E}) = 0$. In this case, we say that $X$ contains *$\nu$-almost every* element of E.

The conditions $\nu_{\mathrm{p}_2}(X) = 0$, $\nu_{\mathrm{p}_2}(X) = 1$, $\nu(X|\mathrm{E}_2) = 0$, and $\nu(X|\mathrm{E}_2) = 1$ are defined analogously for $\mathrm{p}_2$-exact probability measures $\nu$ on $\mathbf{C}$. As usual, when the probability measure $\nu$ is not mentioned, it is assumed to be the uniform probability measure. For example, a set $X$ has *measure* 0 *in* E if $\mu(X|\mathrm{E}) = 0$.

Building on ideas from [14], Breutzmann and Lutz [9] prove theorems justifying the intuition that *a set with $\nu$-measure* 0 *in* E *contains only a negligibly small part of* E (with respect to $\nu$), and similarly for $\mathrm{E}_2$. Of particular importance is the fact that no cylinder $\mathbf{C}_w$ has measure 0 in E or in $\mathrm{E}_2$.

The significance of Theorem 3.3 for resource-bounded measure lies in the following result on the abundance of random languages in E and $\mathrm{E}_2$. (This result generalizes results for the uniform probability measure presented by Lutz [14] and Ambos-Spies, Terwijn, and Zheng [7]; see also [4].)

**Theorem 3.5.** Let $\nu$ be a positive probability measure on $\mathbf{C}$.

1. If $\nu$ is p-exact, then for all $k \in \mathbf{N}$
$$\nu(\mathrm{RAND}_\nu(n^k)|\mathrm{E}) = 1.$$
2. If $\nu$ is $\mathrm{p}_2$-exact, then for all $k \in \mathbf{N}$,
$$\nu(\mathrm{RAND}_\nu(\mathrm{p})|\mathrm{E}_2) = \nu(\mathrm{RAND}_\nu(2^{(\log n)^k})|\mathrm{E}_2) = 1.$$

**Proof** (sketch).

1. Assume the hypothesis, and fix $k \in \mathbf{N}$. Using efficient universal computation, we can construct an enumeration $\rho_0, \rho_1, \rho_2, \ldots$ of all $n^k$-exact probability measures on $\mathbf{C}$ such that the probability measure $\widetilde{\rho}$ of Construction 3.1 is p-exact. Then the $\nu$-martingale $\widetilde{d} = \frac{\widetilde{\rho}}{\nu}$ is also p-exact. Let $A \in \mathrm{RAND}_\nu(n^k)^c$.

Then there is an $n^k$-exact $\nu$-martingale $d$ that succeeds on $A$. Since $d$ is $n^k$-exact, we can write $d = \frac{\rho_i}{\nu}$ for some $i \in \mathbf{N}$. The probability measure $\widetilde{\rho}$ dominates $\rho_i$, so there is a constant $\alpha > 0$ such that, for all $w \in \{0,1\}^*$, $\widetilde{d}(w) \geq \alpha d(w)$. Since $d$ succeeds on $A$, it follows that $\widetilde{d}$ succeeds on $A$. The language $A \in \mathrm{RAND}_\nu(n^k)^c$ is arbitrary here, so this proves 1.

2. This is analogous to 1, noting also that $\mathrm{RAND}_\nu(2^{(\log n)^2}) \subseteq \mathrm{RAND}_\nu(p)$. □

We now have the following consequences of Theorem 3.3.

**Corollary 3.6.** For every strongly positive, p-exact probability measure $\nu$ on $\mathbf{C}$, and for every positive integer $k$,

$$\nu(\mathrm{GEN}(n^k)|\mathrm{E}) = 1.$$

**Proof.** Let $\nu$ and $k$ be as given. Fix a positive integer $l$ such that $\nu$ is an $n^l$-exact probability measure on $\mathbf{C}$, and let $m = \max\{k, l\}$. Then, by Theorem 3.3, with $s(n) = n^l$ and $t(n) = n^k$,

$$\mathrm{RAND}_\nu(n^m) = \mathrm{RAND}_\nu(n^l + n^k) \subseteq \mathrm{GEN}(n^k),$$

so the present corollary follows from Theorem 3.5. □

**Corollary 3.7.** For every strongly positive, $\mathrm{p}_2$-exact probability measure $\nu$ on $\mathbf{C}$, and for every postive integer $k$,

$$\nu(\mathrm{GEN}(\mathrm{p})|\mathrm{E}_2) = \nu(\mathrm{GEN}(2^{(\log n)^k})|\mathrm{E}_2) = 1.$$

**Proof.** The proof is analogous to that of Corollary 3.6, noting also that $\mathrm{GEN}(2^{(\log n)^2}) \subseteq \mathrm{GEN}(\mathrm{p})$. □

In the special case where $\nu$ is the uniform probability measure $\mu$ on $\mathbf{C}$, Corollaries 3.6 and 3.7 say that

$$\mu(\mathrm{GEN}(n^k)|\mathrm{E}) = 1 \tag{13}$$

and

$$\mu(\mathrm{GEN}(\mathrm{p})|\mathrm{E}_2) = \mu(\mathrm{GEN}(2^{(\log n)^k})|\mathrm{E}_2) = 1, \tag{14}$$

respectively. These facts were proven by Ambos-Spies, Neis, and Terwijn [6], who also pointed out that they give a new method for proving results in resource-bounded measure. For example, to prove that a set $X$ of languages has measure 0 in E (i.e., $\mu(X|\mathrm{E}) = 0$), it is sufficient by (13) to prove that $X \cap \mathrm{E}$ contains no $n^k$-generic language. Ambos-Spies, Neis, and Terwijn [6] used this method to prove a new result on resource-bounded measure, namely, the Small Span Theorem for $\leq^{\mathrm{P}}_{k-\mathrm{tt}}$-reductions. (This extended the Small Span Theorems for $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions and $\leq^{\mathrm{P}}_{1-\mathrm{tt}}$-reductions proven by Juedes and Lutz [11] and Lindner [12], respectively.) Ambos-Spies, Neis, and Terwijn [4], Ambos-Spies [1], and Ambos-Spies and Mayordomo [4] have also used this method to reprove a number of previously known results on resource-bounded measure.

To date, every such genericity proof of a resource-bounded measure result corresponds directly to a martingale proof with the same combinatorial content. The genericity method has not yet led to the discovery of a resource-bounded measure result that had not been (or could not just as easily have been) proven directly by a martingale construction. Nevertheless, time-bounded genericity is a very new method that gives an elegant, alternative mode of thinking about resource-bounded measure, so it may very well lead to such discoveries.

Ambos-Spies, Neis, and Terwijn [6] have also pointed out that there are limitations on this genericity method. For example, if a set $X$ of languages contains no $n^k$-random language, but $X \cap \mathrm{E}$ contains an $n^l$-generic language for every $l \in \mathbf{N}$, then $\mu(X|\mathrm{E}) = 0$, but this fact cannot be proven by the above genericity method. The result by Lutz and Mayordomo [16], stating that every weakly $\leq^{\mathrm{P}}_{n^\alpha-\mathrm{tt}}$-hard languages $H$ for E ($\alpha < 1$) is exponentially dense (i.e., there exists $\epsilon > 0$ such that, for all sufficiently large $n$, it contains at least $2^{n^\epsilon}$ of the strings of length $\leq n$) is an example of a resource-bounded measure result that does not have this sort of genericity proof for precisely this reason.

As pointed out by Ambos-Spies, Neis, and Terwijn [6], this weakness of the genericity method becomes a strength when one adopts the view that the method does not merely give alternative proofs of measure results, but rather gives *proofs of stronger results.* Corollaries 3.6 and 3.7 add considerable force to this argument, becasue they give us specific consequences that are obtained by proving such a result. For example, if a set $X$ of languages contains no $n^k$-generic language, then Corollary 3.6 tells us that $X$ has $\nu$-measure 0 in E for *every* strongly positive, p-exact probability measure $\nu$ on $\mathbf{C}$.

# 4 Conclusion

We have shown that the time-bounded genericity method is very powerful in the sense that it allows one to simultaneously prove resource-bounded measure results over all strongly positive, p-computable probability measures on $\mathbf{C}$. It would be interesting to know whether this strong positivity condition can be relaxed.

**Acknowledgment.** The second author thanks Steve Kautz for pointing out the convenience of the $d = \frac{\rho}{\nu}$ representation of a martingale. Both authors thank Ron Book for many inspiring discussions of randomness in complexity classes.

# References

[1] K. Ambos-Spies. Largeness axioms for NP. Lecture at the Annual Meeting of the Special Interest Group "Logik in der Informatik" of the Gesellschaft für Informatik (GI), Paderborn, Germany, May 1994. Unpublished lecture notes.

[2] K. Ambos-Spies. Resource-bounded genericity. In et al. S. B. Cooper, editor, *Computability, Enumerability, Unsolvability*, volume 224 of *London Mathematical Society Lecture Notes*, pages 1–59. Cambridge University Press, 1996.

[3] K. Ambos-Spies, H. Fleischhack, and H. Huwig. Diagonalizing over deterministic polynomial time. In *Proceedings of Computer Science Logic '87*, pages 1–16. Springer-Verlag, 1988.

[4] K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In A. Sorbi, editor, *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics, pages 1–47. Marcel Dekker, New York, 1996.

[5] K. Ambos-Spies, E. Mayordomo, Y. Wang, and X. Zheng. Resource-bounded balanced genericity, stochasticity, and weak randomness. In *Proceedings of the Thirteenth Symposium on Theoretical Aspects of Computer Science*, pages 63–74. Springer-Verlag, 1996.

[6] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn. Genericity and measure for exponential time. *Theoretical Computer Science*. To appear.

[7] K. Ambos-Spies, S. A. Terwijn, and X. Zheng. Resource bounded randomness and weakly complete problems. *Theoretical Computer Science*, 1996. To appear. See also *Proceedings of the Fifth Annual International Symposium on Algorithms and Computation*, 1994, pp. 369–377. Springer–Verlag.

[8] J. L. Balcázar and E. Mayordomo. A note on genericity and bi-immunity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference*, pages 193–196. IEEE Computer Society Press, 1995.

[9] J. M. Breutzmann and J. H. Lutz. Equivalence of measures of complexity classes. Submitted. (Available at http://www.cs.iastate.edu/tech-reports/catalog.html).

[10] S. A. Fenner. Resource-bounded category: a stronger approach. In *Proceedings of the Tenth Structure in Complexity Theory Conference*, pages 182–192. IEEE Computer Society Press, 1995.

[11] D. W. Juedes and J. H. Lutz. The complexity and distribution of hard problems. *SIAM Journal on Computing*, 24(2):279–295, 1995.

[12] W. Lindner. On the polynomial time bounded measure of one-truth-table degrees and p-selectivity, 1993. Diplomarbeit, Technische Universität Berlin.

[13] A. K. Lorentz and J. H. Lutz. Genericity and randomness over feasible probability measures. In preparation.

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

[15] J. H. Lutz. The quantitative structure of exponential time. In L.A. Hemaspaandra and A.L. Selman (eds.), *Complexity Theory Retrospective II*, Springer-Verlag, 1996, to appear.

[16] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23:762–779, 1994.

[17] C. P. Schnorr. Klassifikation der Zufallsgesetze nach Komplexität und Ordnung. *Z. Wahrscheinlichkeitstheorie verw. Geb.*, 16:1–21, 1970.

[18] C. P. Schnorr. A unified approach to the definition of random sequences. *Mathematical Systems Theory*, 5:246–258, 1971.

[19] C. P. Schnorr. Zufälligkeit und Wahrscheinlichkeit. *Lecture Notes in Mathematics*, 218, 1971.

[20] C. P. Schnorr. Process complexity and effective random tests. *Journal of Computer and System Sciences*, 7:376–388, 1973.

[21] C. P. Schnorr. A survey of the theory of random sequences. In R. E. Butts and J. Hintikka, editors, *Basic Problems in Methodology and Linguistics*, pages 193–210. D. Reidel, 1977.