Measure on P: Strength of the Notion

Martin Strauss*
AT&T Labs
600 Mountain Avenue
Murray Hill, NJ 07974
mstrauss@research.att.com

January 7, 1997

Abstract

We give a notion of measure at P in a paradigm that differs somewhat from the standard theory. Our new notion overcomes some limitations of earlier formulations, specifically, concerning closure of null sets under union. First, we analyze formally some of the difficulties in defining measure at P. We then present the new definitions and determine the basic properties of the notion, including the density and immunity characteristics of a random language. We argue that these results are parallel to previous measure results at exponential time.

1 Introduction

Resource-bounded measure was introduced by Lutz in [Lut90] and [Lut92]. Intuitively, this theory gives a notion of big and small to classes of languages. In recent years this tool has been used with many successes to illuminate the structure of complexity classes, notably E and $\mathrm{E}_2 = \mathrm{EXP}$ [Lut96].

The theory of resource-bounded measure is a parametrized tool. For many complexity classes $\mathcal{C}$, one plugs $\mathcal{C}$ into the general theory, and one gets out a notion of measure in which each singleton set $\{L\}$ is small ($L \in \mathcal{C}$), but $\mathcal{C}$ itself is not small. We informally call such a notion "measure at $\mathcal{C}$."

Unfortunately, Lutz's formulation only works directly for measure at $\mathcal{C} \supseteq \mathrm{E}$. Generalizing Lutz's notion, in [AS] Allender and Strauss introduced a notion of measure at P, PSPACE, and other subexponential classes, called Γ-measure. This notion satisfies many nice theoretical properties, and has some applications to BPP, but provides too few measurable sets for some purposes.

In this paper we provide a new notion of measure at P and other classes between P and E. The new formulation uses, as building blocks, aspects of previous developments. In making this formulation, our primary motivation is to provide as many small sets as possible while satisfying the essential properties of measure, the "measure axioms." As a secondary motivation, to the extent this is possible, we want the new formulation to be compatible with Lutz's formulation at the exponential level. To these ends, we prove that the measure axioms are satisfied, and when we limit the available small sets or deviate from Lutz's formulation we prove (or at least give strong intuition) that this is necessary.

We also mention two other results concerning measure at P, that were shown even as the underlying notion of measure was being formalized. First, in [RSC95a], Regan, Sivakumar and Cai show that the

*Research peformed while the author was at Iowa State University and Rutgers University, supported by NSF grant CCR-9204874 and NSF grant CCR-9157382.

class $AC^0[2]$ of languages accepted by polynomial size, constant depth AND-OR-NOT-PARITY circuits does not have measure zero at P. On the other hand, in [CSS95], Cai, Sivakumar and Strauss show that AC^0, and indeed the larger class of languages accepted by circuits of constant depth and nearly exponential size, *does* have measure zero at P (the latter result implies that $\mathrm{NTIME}(n^{1/11})$ has measure zero at P, settling the analog in P of the Lutz hypothesis that NP does not have measure zero at E). Thus it is possible to settle the measurability of several interesting classes within P. Furthermore, these results express in measure theoretic terms the *separation* of $AC^0[2]$ from AC^0. (The proofs of these two results rely heavily on earlier work showing that the parity is not approximable by AND-OR-NOT circuits, so we cannot attribute a separation to these measure results. Nevertheless, it is hoped that a novel separation using measure techniques will be possible in the future.)

In Section 2 we introduce notation and sketch the formulations of Lutz's exponential measure and the earlier weak subexponential measure. This includes a discussion of "dense martingales," introduced in [AS] as yielding more null sets than the Γ-martingales while not satisfying all the measure axioms. In Section 3 we show that dense martingales become still more powerful if they return the amount they bet, rather than their current capital. In Section 4 we examine the dense martingales more closely, and *prove* that measure cannot be directly defined by them. In Section 5 we provide a new, satisfactory notion of measure at P, that is based on the dense martingales and preserves many of the small sets covered by them.

2 Preliminaries

First we sketch the formulation of resource-bounded measure at E from [Lut92]. Next we review the generalization to measure at P from [AS]. Finally, we give a simple counting argument that will be used in many proofs of this paper.

2.1 Measure at E

Fix an enumeration s_i of Σ^*. For now we follow [Lut92] in arbitrarily using the standard lexicographic order, but in subsequent sections we will discuss the significance of this choice. We identify a language L with its characteristic sequence χ_L, where by definition the i^{th} bit of χ_L is 1 if the i^{th} word s_i is in L. For a sequence ω, we will write $\omega[i]$ for the i^{th} bit of ω, and we will overload this notation in many ways: $\omega[i..j]$ and $\omega[s_i..s_j]$ denote the i^{th} through j^{th} bits, and $\omega[A]$ denotes the bits indexed by a set A of words. If w_1 is a string and w_2 is a string or (infinite) sequence extending w_1, we write $w_1 \sqsubseteq w_2$. The empty string will be denoted $\lambda = s_0$. For a string w, we denote by C_w the *cylinder at* w, i.e., the set of all infinite sequences extending w.

Definition 1 *A* martingale *is a function $d : \Sigma^* \to \mathbb{R}_+$, where the input to d is regarded as a prefix of a characteristic sequence of a language, such that d satisfies the following "average inequality:"*

$$d(w) \geq \frac{d(w0) + d(w1)}{2}. \tag{1}$$

The success set $S^\infty[d]$ *of a martingale d is the set of languages L such that*

$$\limsup_{w \sqsubseteq L} d(w) = \infty. \tag{2}$$

If $L \in S^\infty[d]$ we also say d *covers* L.

Classically the term martingale is reserved for a function d satisfying (1) with equality; the above classically defines a *supermartingale*. We follow [Lut92] in using our terminology.

One can regard a martingale as a betting strategy. For example, the martingale fragment defined by $d(\lambda) = 1, d(0) = 0$ and $d(1) = 2$ corresponds to a bet of all our capital that a random language contains the first word. If L is a specific language that indeed contains the first word, then we "double our money along L." This can be regarded as a "detailed verification" that the set of languages extending the characteristic string $w = 1$ has measure at most $d(\lambda)/d(w) = 1/2$. Similarly, the set of languages on whose charateristic sequences d becomes unbounded has measure zero.

To define measure at the level of $\mathrm{E} = \mathrm{DTIME}(2^{\mathrm{linear}})$, Lutz considers martingales computable in polynomial time. That is, the martingales run in time polynomial in the length $|w|$ of their input w, where $|w| \approx 2^{|s_{|w|}|}$, so the machines run in time exponential in the length of $s_{|w|}$.

Definition 2 *A* p-machine *M is an oracle Turing machine such that, on input x and oracle ω, M only queries $\omega[\lambda..x]$ and M runs in time $|\omega[\lambda..x]|^{O(1)}$).*

A p-function (e.g., a p-martingale) $d(w)$ is a function computed by a p-machine $M^w(s_{|w|})$.

Here, the output of the Turing machine is interpreted as encoding some dyadic rational number. A similar definition is made for martingales that run in time $p_2(|w|) = 2^{\log^{O(1)}|w|}$, and for space bounds *pspace* and p_2*space*.

We will often want to compute "subscripted" functions of Σ^*. The function $d_r(w)$ is in $\Delta(\mathcal{C})$ if there is an oracle Turing machine computing $d_r(w)$ taking $(r, s_{|w|})$ as input and w as oracle. (In Lutz's formulation, the "subscript" r is provided to the Turing machine computing d in unary notation; in this equivalent reformulation, the more customary binary notation is used.) In presenting this reformulation of Lutz's definition, we are following the lead of [RSC95b]. Note that, by providing the input $w = \omega[\lambda..x]$ as an oracle, we are essentially using the model of computation recently made popular in the literature on probabilistically-checkable-proofs [ALM+92, BFLS91].

There are some issues regarding the representation of real numbers, but these have largely been solved [Lut92, AS], and in this paper we simply assume that all reasonable arithmetic is allowed. As a final bit of notation, the variable n will always stand for $|x| = \left|s_{|w|}\right| \approx \log|w|$, so we will sometimes write "d runs in time 2^{cn}" to mean $d(w)$ runs in time $|w|^c$.

The objects we measure are sets of languages. We will use the term "language" and the variable L for sets of words, and reserve "set" and variables A, B, C for sets of languages.

Definition 3 *A set A of languages is said to have p-measure zero, if for some $d(w)$ that runs in time $|w|^{O(1)}$ we have $A \subseteq S^\infty[d]$.*

Some of the properties of Lebesgue measure that Lutz sought to preserve are the following measure axioms:

M 1 *Singleton sets are null.*

M 2 *The whole space (i.e., some set) is not null.*

M 3 *Appropriate unions of null sets are null.*

M 4 *A subset of a null set is null.*

The following is a basic property of resource-bounded measure, but has no analog in Lebesgue measure. It says that resource-bounded measure respects the time-heirarchy theorems.

M 5 *For each complexity bound f, the union of all null sets having covers of complexity at most f is null.*

These require some interpretation. Definition 3 can be used to define measure within E, to give meaning to statements like, "almost all languages in E are not SPARSE." With this interpretation we would want that singleton sets of languages in E be null (but singleton sets of languages outside E not necessarily be null). Similarly, we would want E not to have measure zero (so that E would not be a small subset of E), and this is shown by producing from any martingale d a language $L_d \in \mathrm{E} \setminus S^\infty[d]$. In the theory of Lebesgue measure, the union of null sets is not in general null, but a "small" union, i.e., a countable union, of null sets is null. In the resource-bounded setting we can write E as a countable union of null singletons, so we can not expect all countable unions of null sets to be null. Instead, Lutz considered the following generalization:

Definition 4 *A set A is a p-*union *of p-null sets $A_i \subseteq S^\infty[d_i]$ if a single p-machine*

$$M(0^i, w) = M^w(i, s_{|w|})$$

computes $d_i(w)$.

Note that M runs in time polynomial in the length of w and the value of i.

With these interpretations, Lutz has shown [Lut92] that Definition 3 satisfies the above axioms derived from Lebesgue measure.

As hinted above, a singleton set of language L may not have measure zero in E if $L \notin \mathrm{E}$. Such languages L are intuitively random, in a weak sense. More formally and generally:

Definition 5 *A language L is $f(n)$-*random *if no martingale running in time $f(|w|)$ succeeds on L.*
*A language L is p-*random *if no p-martingale succeeds on L.*

Thus, by **M 1**, there are no p-random languages in E. On the other hand, by **M 5**, for each c it is easy to find $(|w|^c)$-random languages in E. This is because, as Lutz showed, there is a p-martingale that covers all non-$(|w|^c)$-random languages. Thus, for each c, "almost every" language in E is $(|w|^c)$-random.

Lutz's formulation works for other classes at least as big as E, notably $\mathrm{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$ and the space analogs ESPACE and E_2SPACE, by considering martingales and resource-bounded unions satisfying the appropriate resource bounds — p_2, *pspace*, and p_2*space*, respectively.

2.2 Previous Measure at P

In this section we describe the generalization to measure at P from [AS].

For sufficiently nice complexity classes $\mathcal{C}$ such as E, one plugs in the complexity class and gets out a notion of measure at that class. In defining a notion of measure at P, one would be tempted at first to do the same thing. Thus, one would take as null sets the sets of languages covered by polytime (in $|x|$) martingales.

The straightforward attempt at measure described above cannot easily be shown to satisfy axiom **M 2**; i.e., apparently too many sets are measurable. Given a martingale d defining measure at E, say, Lutz shows that d does not cover all of E by diagonalizing against d: The leftmost characteristic sequence L such that d never increases along L is clearly not covered, and L is in E since the straightforward decision procedure for $x \in L$ makes $2^{|x|}$ recursive calls to an algorithm in exponential time (in $|x|$.) If one applies Lutz's diagonalization argument against a $\mathrm{DTIME}(|x|^{O(1)})$ martingale, apparently the most one can say about the resulting L (as noted in [May94] in connection with measure at PSPACE) is that

L is *word-decreasing self-reducible*, i.e., that there is a polytime reduction from L to L that on input x queries only strings y that precede x lexicographically. In general we do not see how, with present knowledge, to prove that such a diagonal language is in P.

To define measure at P, [AS] considered not all polytime martingales, but only those requiring at most polynomially many recursive calls to perform this diagonalization. To enforce this restriction on the martingales, we required that on input w representing memberships of words x, $d(w)$ does not query w about any words x outside some P-printable set G_d (a set G_d is P-printable [HY84, AR88] if $G_d \cap \Sigma^n$ can be printed in time polynomial in n). Given any such d, the language with leftmost characteristic sequence along which d never increases can be computed in polynomial time, since there are at most polynomially-many recursive calls (corresponding to words in G_d). A finite union of P-printable sets is P-printable, and it follows that the finite unions (and indeed infinite enumerated unions) of null sets are null by this characterization. This formulation of measure is called $\Gamma(\mathrm{P})$-measure.

The P-printable formulation gives a notion of measure that satisfies many closure properties, but, since this formulation essentially replaces Σ^* with only a sparse subset, there are some intuitively small sets that no martingale of this type can cover. (For example, no $\Gamma(\mathrm{P})$ martingale can cover SPARSE itself, the set of all the languages of density at most $n^{O(1)}$.) In [AS], Allender and Strauss also considered a generalization intended to make the martingales more powerful. Instead of a *single* P-printable set G_d, we allowed $d(w)$ to query bits from a set $\tilde{G}_{d,x}$ that depends on x provided that diagonalizing against d generates only polynomially-many recursive calls. More precisely, we defined *dense martingales* as follows:

Definition 6 *Let $\tilde{G}_{d,x}$ be a sequence of sets (called* dependency sets*) printable from x in $|x|^{O(1)}$ time, such that if $y \in \tilde{G}_{d,x}$ then $\tilde{G}_{d,y} \subseteq \tilde{G}_{d,x}$. A function (e.g., a martingale) $d : \Sigma^* \to \mathbb{R}$ is a* dense *computable function (martingale) if $d(\omega[\lambda..x])$ only queries ω on words in $\tilde{G}_{d,x}$.*

Thus, for a dense computable martingale d, $d(\omega[\lambda..s_i])$ can differ from $d(\omega[\lambda..s_{i-1}])$ for all i, in contrast with Γ-martingales which move only for $s_i \in G_d$.

The transitive closure property insures that, given any dense martingale d, one can diagonalize against d in polynomial time, since only polynomially-many recursive calls are generated. That is, as noted in [AS], **M 2** holds for "measure" defined via dense martingales. In [AS95] it is erroneously claimed that dense martingales satisfy **M 3** for a natural notion of union; in Section 4 we *prove* that without further modification they do not satisfy even closure under finite unions. We will return to dense martingales in Section 5, where we develop a new notion of measure based on the dense martingales, that satisfies all the axioms.

In [AS] it is shown that, while Γ-martingales do not even cover the set SPARSE, dense martingales cover the set of languages with lower density less than 1/2 (a language L has lower density ρ if for infinitely many N, there are at most ρN words in L among the first N words of Σ^*). We recall that proof in detail, since it will be a building block for other proofs in this paper:

Theorem 7 *The set X of languages with lower density less than $\epsilon < 1/2$ is covered by a dense martingale.*

Proof.

Partition Σ^n into blocks of n^2 words, and label all the blocks of Σ^* by $R_0, R_1, \ldots$. Thus R_j consists of words of length n, for some $n > \log j$.

Let X_j denote the languages with density less than ϵ on the j^{th} block. By the Chernoff inequality, for some c that depends on ϵ,

$$\mu(X_j) \le e^{-cn^2} \le 2^{-3n} \le \frac{1}{j^3}.$$

We next construct a martingale d_j that climbs from 1 to j^3 on X_j, works in time polynomial in n, and with dependency set R_j of size n^2. Given input w, let a be the number of 1's in $w[R_j]$. We can set $d_j(w)$ to the exact value

$$\sum_{i<\epsilon n^2 - a} \binom{n^2 - |w[R_j]|}{i}$$

of $\frac{\Pr(X_j|C_w)}{\Pr(X_j)}$, since this takes time polynomial in $n = \log|w|$ and has the desired dependency set.

Classically, the argument would proceed by summing the martingales d_j/j^2. Intuitively, instead we will do the following:

- Make sure (inductively) that we have $1/(j-1)$ capital available before starting to bet on R_j.
- Bet on R_j using strategy d_j/j^2, risking just $1/j^2$ of our capital but winning $j^3 \cdot 1/j^2 = j$ for infinitely many j's.
- Before starting to bet on R_{j+1}, "throw away" the wager and potential winnings of d_j, and assume that we have only $1/(j-1) - 1/j^2 \geq 1/j$, enough to continue inductively.

Continuing in this way our winnings will be unbounded, yet we will be able to keep dependency sets small.

Define $d(w)$ as follows. Determine j such that $s_{|w|} \in R_j$ (note $|w|/\log^2|w| \leq j \leq |w|$). Put

$$d(w) = \frac{1}{j} + \frac{d_j(w)}{j^2}.$$

Finally, let L be a language of density less than ϵ. Then the density of L is less than ϵ on R_j for infinitely-many j's, and for such j d climbs to $d_j/j^2 = j$ along L. ∎

Note that while $\limsup_{w \to L} d(w) = \infty$ for covered L's, it is not the case $\liminf_{w \to L} d(w) = \infty$ (i.e., d does not have a limit of infinity, and we say "X is not in the limit success set of d"). The amount of capital d has at the *starts* of blocks R_j is strictly decreasing. In [AS] it is shown that this is necessary: the limit success set of a dense martingale d is covered by a Γ-martingale d' (essentially d' bets only on the words in the transitive closure, under d's queries, of some fixed P-printable set, say 0^*). Since no Γ-martingale covers SPARSE, it follows that SPARSE is not in the limit success set of any dense martingale.

2.3 A Counting Argument

In several proofs we will use a counting argument similar to the following form of Markov's inequality.

Lemma 8 *Let f be a real-valued function of a finite set. If the average of f is at most 1, and $f \geq 1-\epsilon$, then for all $a > 1$ at least $1 - 1/a$ of the values of f are at most $1 + \epsilon a$.* ∎

2.4 Martingale Summary

Before moving on, we provide a summary of the three types of martingales defined in previous work, and their role in measure:

- p-martingales. A p-martingale $d(w)$ runs in time $|w|^{O(1)}$. The collection of p-covered sets satisfies the measure axioms and class E does not have p-measure zero.

- $\Gamma(\mathrm{P})$-martingales. A $\Gamma(\mathrm{P})$-martingale $d(w)$ has associated with it a P-printable set G. The martingale $d(w)$ runs in time $\log^{O(1)}|w|$ and only reads bits in w corresponding to words in G. The collection of $\Gamma(\mathrm{P})$-covered sets satisfies the measure axioms and class P does not have $\Gamma(\mathrm{P})$-measure zero.

- Dense martingales. A dense martingale $d(w)$ runs in time $\log^{O(1)}|w|$ and satisfies the bounded dependency-set property of Definition 6. The set P is not covered by a dense martingale. At this point in this paper no claim is made about the union of two sets covered by dense martingales.

  In Section 5 we will introduce a notion of measure called $\Gamma_{/}(\mathrm{P})$ based on dense martingales. The collection of $\Gamma_{/}(\mathrm{P})$-covered sets satisfies the measure axioms and the class P does not have $\Gamma_{/}(\mathrm{P})$-measure zero.

3 Bets versus Current Capital

In this section, we show that dense martingales become *still more* powerful if they return the amount of their current bet, rather than the amount of their current capital. This suggestion is due to Merkle [Mer95].

Formally, define a betting strategy as follows:

Definition 9 *A* betting strategy $\beta(w)$ *is a function* $\beta : \Sigma^* \to \mathbb{R}$ *such that* $\beta(w) = -\beta(w')$ *for* $w \neq \lambda$, *and for all* w $\sum_{z \sqsubseteq w} \beta(z) \geq 0$. *(Here* w' *denotes* w *with the last bit flipped.)*

One can easily see that starting with any betting strategy $\beta(w)$, one can put $d(w) = \sum_{z \sqsubseteq w} \beta(z)$, and get a well-formed martingale.

On the other hand, starting with a martingale $d(w)$, one can define a betting strategy $\beta(w) = \frac{d(w)-d(w')}{2}$, where w' is w with the last bit flipped, and by convention $\beta(\lambda) = d(\lambda)$. Intuitively, $\beta(w)$ is the amount bet on the last bit of w. To show this is a legitimate betting strategy, note that

$$\begin{aligned} \beta(w) &= \frac{d(w) - d(w')}{2} \\ &= d(w) - \frac{d(w) + d(w')}{2} \\ &\geq d(w) - d(w_-), \end{aligned}$$

so $\sum_{z \sqsubseteq w} \beta(z) \geq d(w) \geq 0$. (Here w_- denotes w with the last bit dropped.)

Starting with d, converting to β and then back to the capital formulation gives a martingale that is greater than or equal to d, with equality if and only if the martingale d satisfies $d(w) \geq (d(w0)+d(w1))/2$ with equality. A betting strategy is called a *dense computable betting strategy* if $\beta(w)$ is computed by a machine querying only bits in a transitively-closed dependency set (as in Definition 6). It is clear that starting with a dense computable martingale $d(w)$, the betting strategy $\beta(w) = (d(w) - d(w'))/2$ is also dense computable. The advantage of outputting $\beta(w)$ instead of $d(w)$ is we avoid charging our polynomial time machines with making an exponential sum $d(w) = \sum_{z \sqsubseteq w} \beta(z)$.

We regard β simply as an alternate representation for d. We will continue to refer to the martingale/betting strategy by d rather than β, for compatibility with other literature.

The proof of Theorem 7 relies on the fact that each ϵ-SPARSE language is ϵ-SPARSE on infinitely many of the R_j's. The property of being ϵ-SPARSE on R_j is a property of the contiguous block of words in R_j, and one can formulate similar properties of non-contiguous words. One would expect to cover similarly the set of languages meeting infinitely many of these conditions. We show now that this cannot, in general, be done by martingales outputting their current capital.

Theorem 10 *There is a set A covered by a dense martingale that outputs the amount of its bet, but not by a dense martingale that outputs its current capital.*

Proof. Partition Σ^n into blocks of $(3/4)n$ words. Suppose there are $3N$ blocks. Then label the blocks in the following order:

$$R_1^n S_1^n R_2^n S_2^n \ldots R_N^n S_N^n \quad T_1^n T_2^n \ldots T_N^n.$$

That is, each R_j^n, S_j^n and T_j^n has length $3n/4$. All the R's and S's alternate, then come all the T's.

Let

$$A = \{L : \forall n\, \exists j\; L[R_j^n] = L[S_j^n] = L[T_j^n]\}.$$

Then A is covered by a dense martingale d' that returns the amount bet: the martingale d' risks $2^{-5n/4}$ of its capital that the $(3/2)n$ words in S_j^n and T_j^n match R_j^n. If successful d' wins $2^{-5n/4} \cdot 2^{3n/2} = 2^{n/4} \nearrow \infty$, and if unsuccessful d' loses only $2^{-5n/4}$ on each of the $\leq 2^n$ blocks corresponding to n, a total of $2^{-n/4}$. Since $\sum 2^{-n/4} < \infty$, d' never runs out of money. Clearly the dependency sets for this procedure have size $|R| + |S| + |T| = 9n/4$.

On the other hand, A is not covered by a dense martingale that outputs its current capital.

First, for each n, we want to construct a large set J_n of j's such that for any $j' < j \in J_n$, the first point of S_j^n has no dependency on $S_{j'}^n$.

Start by *collecting* the largest j' into J_n. Next, *cancel* all the $n^{O(1)}$-many j's such that the first point of $S_{j'}^n$ has a dependency on S_j^n. Repeat the procedure: collect the largest remaining uncanceled j', then cancel the j's such that S_j^n contains a point in the dependency set of the first point of the most recently collected $S_{j'}^n$. By repeating the procedure while any $j \in \Sigma^n$ remains, we will collect J_n of size $2^n/n^{O(1)}$.

We first give an overview of the proof:

Given a martingale d, we wish to construct an uncovered language $L \in A$. For most j's, d bets just a little on S_j^n since there are too many j's to risk a lot on each. Construct L so that most S's match their corresponding R's, and d may win, but very little, on each particular j. The lack of dependencies among j's insures that d can not gather its winnings from all j's (the total that an unrestricted martingale can accumulate from *all* the j's would be large). Thus d has to start betting on the T's with a bounded amount of capital. But the T's are too short, and thus present too few betting opportunities, for d to earn significant capital.

Now quantitatively:

Suppose a martingale has unit capital at the start of Σ^n. Consider the words of Σ^n in turn. Set $L[R_j^n]$ to defeat d (i.e., so that $d(L[0..k])$ does not rise in k in this range), and if $j \notin J_n$, then set $L[S_j^n]$ to defeat d.

Now consider $L[S_j^n]$ for $j \in J_n$. If some setting of S_j^n makes d rise by at least $2^{-n/8}$ then this winning mass must be distributed over $2^{3n/4} - 1$ other losing settings, and thus some setting σ makes d fall by at least $2^{-7n/8}$. Put $L[S_j^n] = \sigma$, and note that this action can only be taken $2^{7n/8}$ times while $|J_n| = 2^{n-O(\log n)}$. Thus for $2^{n-O(\log n)} - 2^{7n/8} \in 2^{n-o(n)}$ of the $j \in J_n$, every setting of S_j^n makes d rise by at most $2^{-n/8}$. For such j, put $L[S_j^n] = L[R_j^n]$. Let m be the earliest point following S_j^n such that m has no dependency on S_j^n. Then by the average law and definition of dependency set, the capital that d has at m is at most 1, the capital d had at the *start* of S_j^n. Let j' be the next element in J_n after j, so m occurs at the start of $S_{j'}^n$ or earlier. The bits between S_j^n and m are set to defeat the martingale, so d's capital is at most $1 + 2^{-n/8}$ there, and the bits between m and $S^n_{j'}$ are also set to defeat the martingale so the capital is at most 1 there. We conclude that the capital at the start of $S^n_{j'}$ is 1.

Continue setting the R's and S's this way, and let $J'_n = \{j \in J_n : L[R^n_j] = L[S^n_j]\}$. Thus $|J'_n| \in 2^{n-o(n)}$. Note that d's capital grows by at most $2^{-n/8}$ on the R's and S's.

Now the T^n_j's. One can show directly that $\{L : \exists^\infty n \exists j \in J'_n\ L[T^n_j] = L[R^n_j]\}$ has Lebesgue measure $1 - o(1)$, so no martingale having bounded capital at the start of the T's succeeds on A; we give a martingale-style proof. For $j \notin J'_n$, set $L[T^n_j]$ to defeat d. For $j \in J'_n$, if some setting of $L[T^n_j]$ makes d rise by at least $2^{-n/8}$, then some other setting $L[T^n_j] = \sigma$ makes d drop by at least $2^{-7n/8}$. Set $L[T^n_j] = \sigma$, and note this action only occurs $2^{7n/8}$ times. Finally, assume that $j \in J'_n$ and no setting of $L[T^n_j]$ makes d rise by more than $2^{-n/8}$. Put $L[T^n_j] = L[R^n_j]$, and set the rest of the T's to defeat d (we do not need more than one match). This way the language we have constructed meets the condition at n for membership in A, but d's capital grows by at most $2^{-n/8}$ on Σ^n. Since $\sum 2^{-n/8} < \infty$, we have constructed a language $L \in A$ such that d remains bounded on L. ∎

The difficulty in covering this set by a martingale appears to be summarized by the following intuition. Suppose $x < y < z$ are words such that the martingale wants to win money on x and use it to bet on z. The martingale formulation forces the martingale to know about how it fared at x when deciding what to output at y. There may be exponentially many of these irrelevant previous "x's" to keep track of at y.

Above we mentioned that a martingale returning its current bet can succeed on A. Note that "if some setting makes d rise by ϵ" in the above proof becomes "if b bets ϵ on some setting" in the betting formulation, so the betting formulation is not only more powerful than the current capital formulation but also captures a different intuition.

In Section 5, we will give a formulation in which martingales can bet on the words in any (feasible) ordering they prefer (instead of the lexicographic ordering chosen once and for all). In particular, the martingales can order the words so that desired blocks of words become contiguous, and thus such martingales have a mechanism for betting on discontiguous words. On the other hand, there may be other agenda in choosing the ordering of words, so we will continue to let martingales bet on discontiguous words via the mechanism of returning an amount bet rather than current capital.

4 Unions

The dense martingales cover many intuitively small sets that are not covered by Γ-martingales. It is therefore natural to attempt to define measure via these, by calling a set null if it is covered by a dense martingale. It is erroneously claimed, in [AS95], that a notion of measure does result, but unfortunately, as we show in this section, coverage by martingales does not satisfy the Union Axiom **M 3**. This will be rectified in the following section.

We will present two covered sets A and B whose union is not covered. But first we need to examine the structure of dependency sets and betting strategies in more detail.

The collection of dependency sets $\{\tilde{G}_{d,k}\}$ has a natural directed acyclic graph structure (also to be called $\tilde{G}$) whose nodes are the numbers j such that $s_j \in \tilde{G}_{d,s_j}$. Put an arc from i to j when $i \neq j$ and $s_i \in \tilde{G}_{d,s_j}$; this records a dependency. We will also include the node $-\infty$, and put an arc from $-\infty$ to each other node (this represents that the martingale knows its starting capital and knows some fixed apportionment of the starting capital to each node). A *dependency chain* in $\tilde{G}_d$ is a path in $\tilde{G}_d$. Let $I \subseteq \tilde{G}_d$ be the set of *initial bets,* i.e., nodes with just one path (a single edge) from $-\infty$.

In [Lut92] it is noted that $d(w) \leq 2^{|w|} d(\lambda)$, since the martingale can at most double its capital on each of $|w|$ bets. A dense martingale can only double its capital once per edge along any dependency chain within a dependency graph.

Lemma 11 *Let d (or β) be a martingale, k a number, and $\tilde{G}_{d,s_k}$ be the dependency graph for d. Let h denote the length of the longest dependency chain of $\tilde{G}_{d,s_k}$. Then d is bounded* above *by $2^h d(\lambda)$ on w of length at most k.*

Proof. We will show by induction that for betting strategy $\beta(z) = \frac{d(z)-d(z')}{2}$ with dependency chains of length at most h, $\sum_{z \sqsubseteq w} \beta(z) \leq 2^h \beta(\lambda) = 2^h d(\lambda)$.

We will proceed by induction on h. For $h = 1$, we are considering some k with $j \in I$ for all $j \leq k$. Thus $|\beta(w[0..j])|$ depends on at most j and $w[j]$, for all such j. Fix v of length k to minimize $d(v)$. For all w of length k,

$$\begin{aligned}
\beta(\lambda) - \sum_{\lambda \neq z \sqsubseteq w} \beta(z) &= \beta(\lambda) + \sum_{\lambda \neq z \sqsubseteq w} \beta(z') \\
&= \beta(\lambda) + \sum_{\lambda \neq z \sqsubseteq \overline{w}} \beta(z) \\
&\geq \beta(\lambda) + \sum_{\lambda \neq z \sqsubseteq v} \beta(z) \\
&= \sum_{z \sqsubseteq v} \beta(z) \\
&\geq 0,
\end{aligned}$$

where z' denotes the result of flipping the last bit of z, and $\overline{w}$ denotes the result of flipping all the bits of w. Therefore $\beta(\lambda) \geq \sum_{\lambda \neq z \sqsubseteq w} \beta(z)$, and

$$\begin{aligned}
\sum_{z \sqsubseteq w} \beta(z) &= \beta(\lambda) + \sum_{\lambda \neq z \sqsubseteq w} \beta(z) \\
&\leq 2\beta(\lambda).
\end{aligned}$$

Now consider $h > 1$. We can win at most $\beta(\lambda)$ on the bets in I, and the longest chain not counting edges from $-\infty$ into I has length $h-1$. We will assume we doubled our money betting on I, and by induction we double at most $h-1$ more times.

Define function $\tilde{\beta}$ as follows:

$$\tilde{\beta}(w) = \begin{cases} 2\beta(\lambda), & w = \lambda \\ 0, & |w| \in I \\ \beta(w), & |w| \notin I \end{cases}$$

One easily verifies (as above) that $\tilde{\beta}$ is a legitimate betting strategy, i.e., $\sum_{z \sqsubseteq w} \tilde{\beta}(z) \geq 0$. The function $\tilde{\beta}$ has an associated acyclic graph structure formed by consolidating $-\infty$ and I in which the longest chain has length at most $h-1$. Then, as above, $\beta(\lambda) \geq \sum_{j \in I \setminus \{-\infty\}} \beta(w[0..j])$. Also, by induction,

$$\sum_{z \sqsubseteq w} \tilde{\beta}(w) \leq 2^{h-1} \tilde{\beta}(\lambda)$$

We conclude

$$\begin{aligned}
d(w) &= \sum_{z \sqsubseteq w} \beta(z) \\
&= \beta(\lambda) + \sum_{\substack{z \sqsubseteq w \\ |z| \in I}} \beta(z) + \sum_{\substack{z \sqsubseteq w \\ |z| \notin I}} \beta(z) \\
&\leq 2\beta(\lambda) + \sum_{\substack{z \sqsubseteq w \\ |z| \notin I}} \beta(z) \\
&\leq \sum_{z \sqsubseteq w} \tilde{\beta}(z) \\
&\leq 2^{h-1}\tilde{\beta}(\lambda) \\
&\leq 2^{h}\beta(\lambda) \\
&\leq 2^{h}d(\lambda).
\end{aligned}$$

■

Theorem 12 *There are sets A and B, each covered by a dense martingale, such that $A \cup B$ is not covered by any such martingale.*

Proof. For each n, partition the words of Σ^n into consecutive blocks of $.6n$ consecutive words of length n. Let R_j denote the j^{th} block (so $2^n/n \leq j \leq 2^n$, and R_j has about $.6 \log j$ words). Define

$$A = \{L : \exists^\infty j \; L[R_{2j}] = L[R_{2j+1}] \in 0^*\},$$

and

$$B = \{L : \exists^\infty j \; L[R_{2j-1}] = L[R_{2j}] \in 0^*\}.$$

Thus, e.g., A is the set of languages L such that for infinitely many even indexes $2j$, R_{2j} and R_{2j+1} have no words.

By an argument similar to the proof of Theorem 7, one sees that each of the sets A and B is covered by a martingale (in fact, by a martingale returning its current capital). We show that $A \cup B$ is not covered, even by a martingale returning the amount of its bet.

The idea is that if a martingale d bets an appropriately small amount on condition $2j$ or $2j+1$ and still wins, then it must make a lot of dependencies. The dependencies for A and B overlap, so the transitive closure becomes too big.

Note that the set $A \cup B$ can be written as

$$\{L : \exists^\infty j \; L[R_j] = L[R_{j+1}] \in 0^*\},$$

and we will find this characterization convenient.

Inductively suppose we have defined our language L through words of length less than n. We will show how to extend the language through Σ^n, making at least one match, and only increasing d by $2^{-\Omega(n)}$. Since $\sum_{n=0}^{\infty} 2^{-\Omega(n)} < \infty$, we conclude that d remains bounded on L.

Set $j = 1$, and start in Phase 1.

Phase 1: If more than half the $x \in R_{j+1}$ have dependency sets that includes more than half of R_j, then set $L[R_j]$ to defeat d and remain in phase 1; otherwise go to phase 2. One can show, by induction on the number l of such j's in an uninterrupted run, that more than half the words in such an R_{j+1} have dependency set of size at least l. Thus we can remain in phase 1 without interruptions for a number $l < n^{O(1)}$ of j's, and we are in phase 1 at most $2^n(1 - 1/n^{O(1)})$ of the time. Call the other at-least-$\left(2^n/n^{O(1)}\right)$ j's *dependency breaks.*

Phase 2: We are considering a dependency break j such that at most half of the words in R_{j+1} have in their dependency set more than half the $x \in R_j$. If some setting of R_j and R_{j+1} makes d drop by $2^{-.95n}$, extend L by that setting, and return to phase 1. Note that this can only happen $2^{.95n}$ times before d runs out of money, but that leaves $2^{n-o(n)}$ dependency breaks (in particular, at least one) in which no setting makes d drop by $2^{-.95n}$ (phase 3).

Phase 3: At most half of the $x \in R_{j+1}$ have a dependency set that includes more than half of the $x \in R_j$, and no setting of R_j and R_{j+1} makes d drop by as much as $2^{-.95n}$. In particular, no setting of any prefix of R_j and R_{j+1} makes d drop that much, since one can diagonalize against d for the rest of the words. Note that no point in R_j or R_{j+1} has dependency chain whose intersection with $R_j \cup R_{j+1}$ has length greater than $\frac{3}{4}(|R_j| + |R_{j+1}|) \approx .9n$, since otherwise more than half of the $x \in R_{j+1}$ would have dependency set including more than half of R_j. It follows from Lemma 11 and Markov's inequality that no setting of $L[R_j \cup R_{j+1}]$ makes d rise by more than $2^{-.05n}$. Extend L through R_j and R_{j+1} by all zeros, then extend L through the rest of Σ^n to diagonalize against d.

Thus, on Σ^n, the value of d rises by at most $\approx 2^{-.05n}$. Since $\sum_n 2^{-.05n} < \infty$, the martingale remains bounded. ∎

Since we showed that A and B are each covered by dense martingales that return their capital while $A \cup B$ is not covered even by a dense martingale that returns the amount bet (a more generous class of martingales), we have shown that neither notion satisfies **M 3**.

Above we took two martingales whose dependency sets have a lot of overlap. We should note that if a pair or sequence of martingales have compatible dependency sets (e.g., if all the dependency sets are the same), then the usual union theorem holds (e.g., the sum of two such martingales is again a martingale with the same small dependency sets). It will sometimes be useful, in the formulation of Section 5 based on dense martingales, to construct martingales with compatible dependency graphs, just so that we can add them.

The fact that the union of two intuitively small sets is not small is a serious flaw. Yet, one can make a weak case for considering a quick fix of this notion anyway. In formulating resource-bounded measure, one has to fix some enumeration of Σ^*, and the lexicographic enumeration has been chosen, but the reverse lexicographic order (for each n, list the words of length n backwards) is an equally suitable enumeration. For measure at E, we can not presently prove that there are no sets A and B such that A is covered by a martingale in lexicographic order, B is covered in reverse-lexicographic order, yet $A \cup B$ (which has Lebesgue measure zero) is not covered by a martingale in any order. By fixing the lexicographic enumeration ahead of time and considering only martingales in that enumeration, one gets a notion of measure closed under unions, but this may make the set B unmeasurable. Further, with this approach, it is consistent with what we know that there's a p-random sequence $\omega = B_0B_1B_2\ldots$ where B_i is a block of 2^i bits, such that the sequence $B_0^RB_1^RB_2^R\ldots$ formed by reversing the blocks is *not* p-random.

It is far less natural, but nevertheless possible, to develop measure at P by deciding ahead of time which are the allowable dependency sets, and considering only corresponding martingales. The resulting notion of measure would be awkward, but it would include more null sets than the $\Gamma(\mathrm{P})$ notion of [AS], and in fact include some sets not measurable by the notion of measure to be presented in Section 5. The resulting notion of resource-bounded pseudorandomness would be far less natural even than the notion of pseudorandomness at E (for example, there might be a random sequence ω such that the sequence 1ω formed by prepending a 1 is not random in this sense). Generally, the choice of dependency sets for measure at P seems to be more critical than the choice of ordering is for measure at E, and there does not seem to be any natural way to fix dependency sets ahead of time.

Another option is to restrict what is meant by "appropriate unions." If a single machine $M(j, w)$ computes $d_j(w)$, and the dependency sets for d_j obey some uniformity conditions in j making the dependency sets compatible, then there is a single martingale covering $\bigcup_j S^\infty[d_j]$. As we saw above, this notion of union does not include all finite unions.

In the next section we present a notion of measure that balances these requirements.

5 Quotient Formulation

To remedy the flaws with the martingale measure discussed previously, in this section we propose a new notion of measure. First we give the relevant definitions and show that the measure axioms are satisfied. Next we show that desired properties of resource-bounded measure are, to a large degree, preserved: We look at resource-bounded pseudorandomness and the "density of a random language." The notion of measure presented now balances a need to satisfy measure axioms with a desire to have as many null sets as possible.

5.1 Basic Definitions and Properties

Definition 13 *The* quotient *of a language L by a word y is the language*

$$L/y = \{x \mid xy \in L\}.$$

The direct product *of a sequence $\{L_i\}$ of languages is the language*

$$\bigotimes L_i = \{x10^i \mid x \in L_i\}.$$

We say a set A is closed under quotients if $L \in A$ implies for all x $L/x \in A$. The quotient by 10^i and direct product are (essentially) inverse operations: $(\bigotimes_j L_j)/10^i = L_i$, and $\bigotimes_i (L/10^{i-1}) = L \setminus 0^*$. We will often consider quotients by 10^{i-1}, so, for convenience, for an integer i we write L/i for $L/10^i$. Quotients can be composed: $(L/x)/y = L/yx$. For every set A of languages, therefore, one can define the *interior* $\breve{A}$ of A by $\{L \in A | \forall x\, L/x \in A\}$; then $\breve{A}$ is the largest subset of A closed under quotients. One can also take the *closure* $\overline{A}$ of the set of all quotients of languages in A; this is the smallest superset of A closed under quotients. Note that the characteristic sequence $\chi_{(L/y)}$ is a subsequence of the characteristic sequence χ_L, formed by taking the bits indexed by an arithmetic progression of difference $2^{|y|}$.

Finally, note that L/y can be reduced to L by extremely weak reductions, and if a machine $M(0^i, y) \in$ P decides $y \in L_i$ then $\bigotimes L_i \in$ P.

Definition 14 *A* $\Gamma_/(\mathrm{P})$*-*subbasic null set *is a set closed under quotients that is covered by a dependency-set size bounded betting strategy.*

A $\Gamma_/(\mathrm{P})$*-*basic null set *is the enumerated union of subbasic null sets. By "enumerated union," we mean a single machine $M(i, w) = M^w(i, |w|)$, that runs in time polynomial in $|(i, |w|)|$, such that $M(i, \cdot)$ computes a martingale d_i that covers the subbasic null set A_i (together with M implicitly comes* *a machine to compute the dependency set $\tilde{G}_{d_i}$ for d_i). Note that the dependency sets for the various d_i's can be different.*

A $\Gamma_/(\mathrm{P})$-null set *is a subset of a basic null set.*

Each subbasic null set has its own martingale, with its individual dependency set. These martingales return a bet $\beta(w)$, not their current capital $d(w) = \sum_{z \sqsubseteq w} \beta(z)$ (see Definition 9.) It will be convenient also to allow a function $M(i, \cdot)$ in the enumeration to be any function at all, provided $M(i, w) = 0$ for sufficiently long w and, correspondingly, $A_i = \emptyset$. A $\Gamma_/(\mathrm{P})$-*cover* of a null set in this formulation is the machine M enumerating the subbasic null sets.

This formulation has precedent in classical mathematics. Forming a basic-null set from a subbasic null set has precedent in the theory of Baire category, where a meager set is defined to be the countable union of nowhere-dense sets, and taking subsets of basic null sets has precedent in the *completion* of a measure: a Lebesgue-null set is defined to be a subset of a Borel-null set. The advantage is that satisfaction of **M 3** is trivial. Our main task, then, is to show the analog of the Baire category theorem, that P is not $\Gamma_/(\mathrm{P})$-null. The closure under quotients was contrived solely to make this go through:

Theorem 15 P *is not a* $\Gamma_/(\mathrm{P})$*-null set.*

Proof. Suppose $\mathrm{P} \subseteq \bigcup_i A_i$, for an enumeration of subbasic null sets A_i. Since this is an enumerated union, there is a number c and a sequence d_i of martingales such that d_i covers A_i and all the martingales have bound n^c. For each martingale d_i, find a language $L_i \in \mathrm{DTIME}(n^{2c+1})$ not covered by d_i, and put $L = \bigotimes L_i$. Then, again using the uniformity in the union, L is seen to be in P, but $L/i = L_i \notin A_i$ by construction, so for all i we have $L \notin A_i$ since A_i is closed under quotients. ∎

Theorem 16 *For each c, the set* $\mathrm{DTIME}(n^c)$ *is* $\Gamma_/(\mathrm{P})$*-null.*

Proof. We show $\mathrm{DTIME}(n^c)$ is a subbasic null set. Clearly $\mathrm{DTIME}(n^c)$ is closed under quotients. The set $\mathrm{DTIME}(n^c)$ is covered by a dense martingale [AS]: Let $M(i, x)$ be a P-time machine that is universal for $\mathrm{DTIME}(n^c)$. For each i, there is a martingale d_i that succeeds on $L(M(i, \cdot))$ such that d_i has dependency set in 0^*. Finally, we can add the martingales $2^{-i} d_i$, getting a dependency set in 0^*. ∎

In particular,

Corollary 17 *For each $L \in \mathrm{P}$, the set $\{L\}$ is* $\Gamma_/(\mathrm{P})$*-null.* ∎

5.2 Resource-Bounded Randomness

Next we look at **M 5**, the reason for allowing non-martingales into the enumeration.

A useful property of measure at E is the resulting property of pseudorandomness. A language L is p-random if no p-martingale covers $\{L\}$. The current formulation of measure at E was chosen so that a martingale d computable in just more than 2^{cn} time covers all languages covered by *any* (2^{cn})-bounded martingale d_i. To do this, d enumerates all *functions* f_i computable in 2^{cn} time, checks the first $|w|$ functions to see if they are legitimate martingales, and sums the legitimate ones.

The difficulty in extending this to subexponential time measure lies in detecting when a function is a legitimate martingale (i.e., satisfies the average inequality). Our solution here is to allow non-legitimate martingales into the enumeration, but these martingales must not have an infinite limsup on any language (so they each cover the empty set).

With this convention, we have

Theorem 18 *For each c, almost every language is* $(\log^c |w|)$*-random.*

Proof. Let $\left\{\widehat{G_i}\right\}$ enumerate the possible machines printing dependency sets $\{\tilde{G}_i\}$, and let M_j enumerate functions from Σ^* to the postitive dyadic rationals. Define the martingale $d_{i,j}$ as follows: To compute $d_{i,j}(w[0..k])$, first simulate $d_{i,j}(w[0..l])$, for each $l < |(i,j,s_k)|^c$. If

- M_j tries to query something outside of G_i, or
- M_j runs longer than $|(i,j,s_k)|^c$, or
- $|G_i|$ becomes larger than $|(i,j,s_k)|^c$, or
- d violates the average law,

then throw all money away; otherwise $d_{i,j}$ returns the value computed by M_j. If X is covered by any n^c martingale, it is covered by one of the $d_{i,j}$'s; we note the union $\bigcup_{i,j} S^\infty[d_{i,j}]$ is an enumerated union. ∎

5.3 Finite Variants

In this section we show that if a set X is null, then the closure of X under finite variants is null.

Theorem 19 *Let X be a* $\Gamma_/(\mathrm{P})$*-null set. Then the closure of X under finite variants is also* $\Gamma_/(\mathrm{P})$*-null.*

Proof. Let Δ denote the symmetric difference. For a set A of languages and a finite set F of words, let $A\Delta F$ denote the variants of A by F, i.e.,

$$A\Delta F = \{L\Delta F : L \in A\}.$$

Suppose $X \subseteq \bigcup_i A_i$, where each $A_i \subseteq S^\infty[d_i]$ is a subbasic null set, and the union is a $\Gamma_/(\mathrm{P})$-enumerated union. For each word v and each A_i, we will uniformly construct a subbasic set $B_{i,v}$ containing $A_i \cup (A_i\Delta\{v\})$. It follows that for any finite set F we can construct a subbasic $C_{i,F}$ containing $A_i \cup (A_i\Delta F)$, and the closure of X under finite variants is contained in the $\Gamma_/(\mathrm{P})$-union of $C_{i,F}$ over all i and all F. The main observation is that Δ distributes over $/$.

Fix i and a word v; we construct subbasic $B_{i,v} \supseteq A_i \cup (A_i\Delta\{v\})$. For each subset S of the set of prefixes of v, one can construct a dense martingale $d_{i,S}$ covering $A_i\Delta S$. Note that for all the subsets S, S' of prefixes of v, the dense martingales $d_{i,S}$ and $d_{i,S'}$ have the same dependency sets. Thus $d_{i,v} = \sum_S 2^{-|v|} d_{i,S}$ is a well-formed dense martingale, with the same dependency set as all the summands, and $S^\infty[d_{i,v}] = \bigcup_S S^\infty[d_{i,S}]$. Put $B_{i,v} = \bigcup_S A_i\Delta S$, so $B_{i,v}$ is covered by a dense martingale; to show $B_{i,v}$ is a subbasic null set we need to show that $B_{i,v}$ is closed under quotients.

Let y be a word, and let L be a language in $B_{i,v}$. Then, for some S, L is in $A_i\Delta S$, so $L\Delta S$ is in A_i. It is straightforward to show that $L/y = ((L\Delta S)/y)\Delta(S/y)$ (distributivity).

The language $L\Delta S$ is in A_i, and since A_i is closed under quotients, $(L\Delta S)/y$ is in A_i. It follows that $L/y = ((L\Delta S)/y)\Delta(S/y)$ is in $A_i\Delta(S/y) \subseteq B_{i,v}$, since S/y is a set of prefixes of v. ∎

5.4 Density

Now we consider the density of a "random language," and compare the quotient formulation to the martingale formulation of [AS]. We also compare these to coverage by a dense computable martingale. With high probability, a (Lebesgue) random language has $(1/2 - o(1))2^n$ words of length n, and this property is captured by dense martingales in Theorem 7. At the other extreme, no Γ-martingale covers even the set of all polynomially sparse languages[AS]. The quotient formulation is much better than the martingale formulation in this regard, but not quite so good as the dense martingales.

Theorem 20 *The set A of languages having $o(2^n)$ words of length n has $\Gamma_/(\mathrm{P})$-measure zero.*

Proof. The set A is the interior of the set covered in Theorem 7. ∎

This theorem shows that, in regard to density, the quotient formulation is midway between the $\Gamma(\mathrm{P})$-martingales and dense martingales (and much closer to dense martingales). In several contexts, the interior of a set satisfying a condition "infinitely often" is a set satisfying a similar condition "with density $1 - o(1)$." A similar observation applies to the sets in Theorem 12.

Earlier we contrasted $\Gamma(\mathrm{P})$-martingales, that bet on only a SPARSE set of words, with dense martingales, that can bet everywhere. The $\Gamma_/(\mathrm{P})$ formulation falls somewhere between these notions: Note that $\chi_{L/x}$ is a subsequence of χ_L formed by the bits of the latter appearing in positions of some arithmetic sequence of difference $2^{|x|}$. The $\Gamma_/(\mathrm{P})$-martingales can bet everywhere, but by requiring a martingale d to become unbounded not only on L but also on every quotient of L, we are requiring some sort of growth on each dyadic arithmetic progression, no matter how sparse.

5.5 Immunity

A property of measure at E is that almost every language L is P-bi-immune, i.e., neither L nor L^C contains, as a subset, an infinite language in P (in fact, for each c, almost every language is $\mathrm{DTIME}(2^{cn})$-bi-immune)[May94]. In particular, for every easy-to-compute infinite set A, for almost every language $L \in \mathrm{E}$, we have $L \cap A \notin \mathrm{DTIME}(2^{cn})$ (the idea is that a martingale can double its money at each "easy instance:" each word in A). The weak $\Gamma(\mathrm{P})$-martingales of [AS] also can succeed given an infinite set of easy instances (suitably defined), but as we now observe, this is not the case for the quotient measure of this paper. In the following, L' has an infinite set of easy instances in an intuitive sense, but $\{L'\}$ does not have $\Gamma_/(\mathrm{P})$-measure zero.

Proposition 21 *Let L be p-pseudorandom. Then for $L' = L \cup 0^*$, $\{L'\}$ is not $\Gamma_/(\mathrm{P})$-null.*

Proof. The hypothesis says that no p-martingale covers L.

Suppose $\{L'\}$ is null. Then $\{L'\} \subseteq \bigcup A_i$, i.e., L' is in some A_i, where A_i is closed under quotients and covered by a martingale. But it is easy to see that $L'/1$ is p-pseudorandom, so no martingale covers $L'/1$, or hence $\overline{\{L'\}}$, or hence A_i. ∎

Instead of a result about immunity, we have the following degenerate, weakened version, replacing "infinite" with "density $1 - o(1)$" (whereas martingales at E succeed if given infinitely many easy instances, martingales under the quotient formulation need the easy instances to have density 1). Call a set L *weakly $f(n)$-immune* if L contains no set in $\mathrm{DTIME}(f(n))$ having $2^n(1 - o(n))$ words of length n. If L and L^C are both weakly-$f(n)$-immune, then L is weakly-$f(n)$-bi-immune.

Theorem 22 *For every c, almost every set in* P *is weakly-n^c-bi-immune.*

Proof. This follows from Theorem 20. ∎

5.6 Ordering Σ^*

Earlier we noted that if two exponential time martingales d and d' work under incompatible orderings of Σ^*, it is not clear that $S^\infty[d] \cup S^\infty[d']$ is covered by any exponential time martingale, working in any order. That is, it is not clear how to combine these two martingales into a third. Generally, for measure at E, we want to consider reorderings of the following sort:

Definition 23 *A p-reordering π of Σ^* is a permutation of Σ^* satisfying*

- *π is length preserving, i.e., $\pi_n = \pi|_{\Sigma^n}$ is a permutation of Σ^n, and*
- *A single machine M computes $\pi(x)$ in time exponential in $|x|$, and another machine M^{-1} similarly computes $\pi^{-1}(x)$. (Thus $\pi(s_i)$ returns the i'th word in the ordering.)*

We also similarly define P-reorderings, substituting polynomial time for exponential time. Such reorderings preserve the exponential number of predecessors of each word, and are computable within the resources available to the martingales.

Our present $\Gamma_/(\mathrm{P})$ formulation sidesteps the need to combine martingales in covering unions: given subbasic null sets A and A' covered by $\Gamma(\mathrm{P})$-martingales d and d' working in incompatible orders, one can construct languages L_A and $L_{A'}$ separately, and $L_A \otimes L_{A'} \notin A \cup A'$. The primary benefit is that the union $S^\infty[d] \cup S^\infty[d']$ is $\Gamma_/(\mathrm{P})$-null, even if d and d' have incompatible dependency sets. We note here that even if two martingales d and d' (or an enumerated infinite sequence of martingales) work under incompatible P-reorderings of Σ^*, the union $S^\infty[d] \cup S^\infty[d']$ is $\Gamma_/(\mathrm{P})$-null, and this is automatic in our formulation. By contrast, it is conceivable that such a $\Gamma_/(\mathrm{P})$-null set would not even have p-measure zero.

5.7 Space

In this section we note that our definitions hold for space bounds as well as time bounds. We then compare our PSPACE measure, denoted $\Gamma_/(\mathrm{PSPACE})$, to that of [May94], which we denote by $\Phi(\mathrm{PSPACE})$. A set is $\Phi(\mathrm{PSPACE})$-null if it is covered by a martingale that works in polylog space, reads its input once from left to right, and is given the allowable workspace (but not the input length).

This section is based on [AS95], where it is shown that coverage by dense martingales is incomparable with $\Phi(\mathrm{PSPACE})$-measure zero. Here we summarize that work, indicating that it generalizes from dense martingales to $\Gamma_/(\mathrm{PSPACE})$-measure.

Note that PSPACE is enough to compute $d(w) = \sum_{z \sqsubseteq w} \beta(w)$, so there is no issue about whether martingales return the amount bet or the current capital.

Definition 24 *Let* ODD *denote the set of languages L such that for each n, L has an odd number of words of length n.*

Note that ODD has Lebesgue measure zero.

Theorem 25 *The set* ODD *has* $\Phi(\mathrm{PSPACE})$*-measure zero.*

Proof. Immediate; also see [May94]. ∎

Theorem 26 *The set* $\mathrm{ODD} \cap \mathrm{PSPACE}$ *does not have* $\Gamma_/(\mathrm{PSPACE})$*-measure zero.*

Proof.

To show that no enumeration covers ODD, let d_i be an enumeration of martingales. For each i, form a language L_{i+1} that defeats d_i (leaving L_1 unspecified). Put $L = \bigotimes L_i$, and now set L_1 so that L is in ODD. ∎

In the above proof, we took advantage of the quotient-closure requirement, i.e., we constructed an ODD language L such that for each martingale d, *some* quotient of L is uncovered by d. It is also possible [AS95] to construct a single language L that is itself both ODD and uncovered.

We now present a set measurable in our measure at PSPACE but not in the sense of [May94].

Definition 27 *Partition Σ^n into blocks of n^2 words. Label the first half of the blocks R_j^n, for $j = 1 \ldots 2^n/2n^2$, and label the second half of the blocks S_j^n:*

$$R_1 R_2 \ldots R_{\frac{2^n}{2n^2}} \quad S_1 S_2 \ldots S_{\frac{2^n}{2n^2}}.$$

Let MATCH *be the set of sequences ω such that for infinitely many pairs (n, j), $\omega[R_j^n] = \omega[S_j^n]$. Let* $\breve{\text{MATCH}}$ *denote the interior of* MATCH.

Theorem 28 *The set* $\breve{\text{MATCH}}$ *has* $\Gamma_/(\text{PSPACE})$*-measure zero.*

Proof. Similar to Theorem 7 above. In fact, $\breve{\text{MATCH}}$ has $\Gamma_/(\text{P})$-measure zero. ∎

Theorem 29 *The set* MATCH $\cap$ PSPACE *does not have* $\Phi(\text{PSPACE})$*-measure zero.*

Proof. See [AS95]. The full proof appears in [AS]. ∎

Now we show that Theorem 29 generalizes to the quotient formulation.

Theorem 30 *The set* $\breve{\text{MATCH}} \cap$ PSPACE *does not have* $\Phi(\text{PSPACE})$*-measure zero.*

Proof. First we briefly sketch the proof of Theorem 29 (the proof is related to the proof of Theorem 10). The idea is that a Φ(PSPACE)-martingale does not have enough space to store the data in all the R_j's, and it does not have enough capital to bet more than a small amount on most R_j-S_j pairs. Given any Φ(PSPACE)-martingale d, the following sketch shows how to construct a language section $L \subseteq \Sigma^n$ that has a match, yet d wins only a tiny amount (e.g., d wins less than $1/n^2$, while $\sum 1/n^2 < \infty$). This shows that no Φ(PSPACE)-martingale covers MATCH.

Fix n. First find a configuration C of the martingale such that for most j, C stores little information about R_j. Thus most settings of the R_j for most j's are consistent with taking the martingale to configuration C. The expected value of d at C (over randomly set R_j's) is bounded, since the martingale satisfies an average law. Therefore, by Markov's inequality, we can find a C such that, in addition, the martingale has not won much money at C. For most j's and most settings σ of S_j, the martingale proceeding from configuration C risks an appropriately small amount and wins little on S_j. Putting this all together, one can find a C, j and a setting σ for R_j and S_j such that (1) setting R_j to σ takes the martingale to C, (2) d does not have much capital at C, and (3) d does not win much on S_j.

Our goal here is not only to show d fails to cover MATCH, but also to show d fails to cover the interior $\breve{\text{MATCH}}$ of MATCH. Given any string x and large enough n, we can, as above, construct a language section $L \cap \Sigma^n$ such that d wins little on L but L/x has a match (i.e., for some j, $(L/x)[R_j^{n-|x|}] = (L/x)[S_j^{n-|x|}]$). Let $\{x_n\}$ be a sequence in which each word appears infinitely often, and $|x_n| \leq n$. For each n in turn, construct $L \cap \Sigma^n$ so that d barely rises on L and L/x_n has a match. We conclude that d remains bounded on L, and since for each x the language L/x has infinitely many matches, we conclude $L/x \in$ MATCH. ∎

Note that under some ordering of Σ^*, namely the ordering in which S_j^n immediately follows R_j^n, the set MATCH is Φ(PSPACE)-null. Thus Φ(PSPACE) measure is not robust under PSPACE-reorderings.

6 Conclusions

We presented a notion of measure at P that, compared with previous notions, provides more measurable sets while satisfying the intuitive properties of measure. There are three main changes from Lutz's presentation. First, martingales do not have free access to their input, but must satisfy a dependency set restriction. Second, the martingales can return the amount of their bet, rather than the amount of their current capital. And third, null sets must satisfy the "closure under quotients" restriction.

The dependency set restriction seems to be necessary in order that P itself not have measure zero. The betting formulation is in some regards more natural than the current capital formulation, and provides many more null sets than the latter. In any case, at Lutz's exponential time setting these changes are transparent, so these aspects of the current work are generalizations of Lutz's work.

How hard, in practice, will it be to satisfy the "closure under quotients" restriction? Often, as in [CSS95] where AC^0 is covered by a $\Gamma_/(\mathrm{P})$ martingale, one wants to cover by a single martingale a complexity class already closed under quotients, and in this case the machinery concerning enumerated unions and quotient closures can be disregarded altogether. In other situations, such as Theorem 19 concerning finite variants, one wants to cover a set whose structure is compatible with closure under quotients, and so the quotient closure requirement is not an obstacle here, either. In still other situations, such as Theorems 20 and 22 concerning density and immunity, one wants to cover a set A but must instead settle for the interior $\breve{A}$ of A, a proper subset that can be viewed merely as a numerically weakened version of A. Thus it is hoped that the same types of null sets (sometimes numerically weaker) will be available in the $\Gamma_/(\mathrm{P})$ formulation as are available in Lutz's formulation.

Conversely, how hard is it to show that a set A does *not* have measure zero? If A is closed under products, as in Theorem 15, then it is sufficient to show that A is not covered by any *single* dense martingale.

It is hoped that the quotient closure formulation will give a theoretical basis for this stronger notion of measure but that the requirements will not figure prominently in the construction of martingales.

Acknowledgments

Thanks to Wolfgang Merkle for suggesting martingales return the amount they bet, rather than their current capital. Thanks to Steve Fenner for suggesting that we show that a collection of martingales fails to cover P, and not that a collection is equivalent to some other single martingale. Thanks to Ken Regan for pointing out that closure under finite variants is important, but not trivial, under the quotient formulation.

I thank Eric Allender, Merkle, Regan, and D. Sivakumar for helpful discussions.

References

[ALM$^+$92] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and hardness of approximation problems. In *Proc. 33rd FOCS Conference*, pages 14–23, 1992.

[AR88] E. Allender and R. Rubinstein. P-printable sets. *SIAM Journal on Computing*, 17:1193–1202, 1988.

[AS] E. Allender and M. Strauss. Measure on small complexity classes, with applications for BPP. Journal version; in preparation.

[AS95] E. Allender and M. Strauss. Measure in P: Robustness of the notion. In *Proc. 20th Mathematical Foundations of Computer Science Conference*, volume 969 of *Lecture Notes in Computer Science*, pages 129–138. Springer, 1995.

[BFLS91] L. Babai, L. Fortnow, L. Levin, and M. Szegedy. Checking computations in polylogarithmic time. In *Proc, 23rd STOC Conference*, pages 21–31, 1991.

[CSS95] J.-Y. Cai, D. Sivakumar, and M. Strauss. Constant-depth circuits and the Lutz hypothesis, 1995. Submitted for publication.

[HY84] J. Hartmanis and Y. Yesha. Computation times of NP sets of different densities. *Theoretical Computer Science*, 34:17–32, 1984.

[Lut90] J. Lutz. Category and measure in complexity classes. *SIAM Journal on Computing*, 19:1100–1131, 1990.

[Lut92] J. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44:220–258, 1992.

[Lut96] Jack Lutz. The quantitative structure of exponential time. In Lane Hemaspaandra and Alan Selman, editors, *Complexity Theory Retrospective II*. Springer-Verlag, 1996. to appear.

[May94] E. Mayordomo. *Contributions to the Study of Resource-Bounded Measure*. PhD thesis, Universitat Politècnica de Catalunya, Barcelona, 1994.

[Mer95] W. Merkle, 1995. Personal Communication.

[RSC95a] K. Regan, D. Sivakumar, and J.-Y. Cai. Pseudorandom generators, measure theory, and natural proofs. Technical Report UB-CS-TR 95-02, Computer Science Dept., University at Buffalo, January 1995.

[RSC95b] K. Regan, D. Sivakumar, and J.-Y. Cai. Pseudorandom generators, measure theory, and natural proofs. In *Proc. of the 36th FOCS conference*, pages 26–35. IEEE Computer Society Press, 1995.