Resource-bounded Measure on Probabilistic Classes

Philippe Moser

Department of Computer Science, National University of Ireland, Maynooth Co. Kildare, Ireland.

Abstract

We extend Lutz's resource-bounded measure to probabilistic classes, and obtain notions of resource-bounded measure on probabilistic complexity classes such as BPE and BPEXP. Unlike former attempts, our resource bounded measure notions satisfy all three basic measure properties, that is every singleton $\{L\}$ has measure zero, the whole space has measure one, and "enumerable infinite unions" of measure zero sets have measure zero.

Key words: Resource-bounded Measure, Probabilistic complexity classes.

1 Introduction

Resource-bounded measure was introduced by Lutz in [4,5] for both complexity classes EXP and E. It provides a means of investigating the sizes of various subsets of E and EXP. Given a subset C of EXP such as P, NP or BPP, one tries to determine whether C is a small subset of EXP, i.e. has measure zero, or is a large subset, i.e. has measure one. Resource-bounded measure has been successfully used to understand the structure of the exponential time classes E and EXP.

The first goal of Lutz's approach was to extend existence results, such as "there is a language in C satisfying property P", to abundance results such as "most languages in C satisfy property P", which is more informative since an abundance result reflects the typical behavior of languages in a class, whereas an existence result could as well correspond to an

Email address: pmoser(at)cs.nuim.ie (Philippe Moser).

exception in the class. For instance it was shown [3] that the set of $\leq_m^p$-complete languages for E has measure zero in E.

Plausible but unproven hypothesis such as $\mathsf{P} \neq \mathsf{NP}$ and "the polynomial time hierarchy does not collapse" are useful to provide information concerning complexity theoretical propositions. Resource-bounded measure can also be used to formulate new plausible working hypothesis such as "NP is not a small subset of E". For instance it was shown in [2], that under the hypothesis "NP does not have p-measure zero" full derandomization of AM is possible, i.e. $\mathsf{NP} = \mathsf{AM}$. For a more detailed survey on Lutz's resource bounded measure see [6].

Resource-bounded measure can be seen as a general framework which for many complexity classes C, yields a notion of "measure in C" which satisfies the following three basic properties. First, every singleton $\{L\}$ (where $L \in C$) has measure zero in C, second the whole space C has measure one in C, and finally "enumerable infinite unions" of measure zero sets have measure zero in C. These basic properties meet the essence of Lebesgue's measure and ensure that it is impossible for a subset of C to have both measure zero and one in C.

Unfortunately, Lutz's formulation only works for measure in $C \supseteq \mathsf{E}$. In [8,1,15,11] Lutz's measure was generalized to subexponential classes with the introduction of measure notions in classes such as P, SUBEXP and PSPACE. And what about probabilistic classes?

In [14], the notion of measure on probabilistic classes has been investigated. Probabilistic martingales were introduced in [14], where the overwhelming majority of the branches of a probabilistic computation compute values that are close approximations to the actual value of the martingale (different branches might produce different approximations). Several classes were shown to be small according to this notion in [14], including the classes that the "natural proofs" of [13] are useful against, the Turing-complete sets for EXP, and $\mathsf{BPTIME}(2^{cn})$ (for any constant c). Unfortunately the notion of [14] is not known to satisfy the three basic measure properties (and a proof thereof would imply settling some long-standing open questions namely the existence of a time-hierarchy theorem for probabilistic classes).

It was thus left open whether it is possible to define a measure on probabilistic classes which satisfies all three basic measure properties. We give an affirmative answer to this question by constructing a measure notion on both probabilistic classes BPEXP and BPE, which satisfies all three basic measure properties. The idea is to consider martingales for which the overwhelming majority of the branches of a probabilistic computation compute the *same* value that is a close approximation to the actual value of the martingale. This combined with standard techniques used to prove the three basic properties for Lutz measure on E, yields a measure notion on BPE that satisfies the three basic properties. The price to pay is that being same-valued probabilistically computable, our probabilistic martingales cannot

use random sampling (as opposed to the martingales in [14]), hence the measure of the classes shown to be small in [14] is not known with regard to our notion.

The idea of same-valued probabilistic computation carries over to measure on small probabilistic classes (using the approach of [1,15,11]) to yield measure notions on BPP.

2 Preliminaries

We use standard notation for traditional complexity classes, see for instance [12]. Let us fix some notation for strings and languages. A *string* is an element of $\{0,1\}^n$ for some integer n. For a string x, its length is denoted by $|x|$. $s_0, s_1, s_2 \ldots$ denotes the standard enumeration of the strings in $\{0,1\}^*$ in length-lexicographical order, where $s_0 = \lambda$ denotes the empty string. Note that $n = 2^{O(|s_n|)}$. A *sequence* is an element of $\{0,1\}^\omega$. If w is a string or a sequence and $1 \leq i \leq |w|$ then $w[i]$ and $w[s_i]$ denotes the ith bit of w. Similarly $w[i \ldots j]$ and $w[s_i \ldots s_j]$ denote the ith through jth bits. For two strings x, y, the concatenation of x and y is denoted xy.

A *language* is a set of strings. A *class* is a set of languages. We identify language L with its characteristic function χ_L, where χ_L is the sequence such that $\chi_L[i] = 1$ iff $s_i \in L$. Thus a language can be seen as a sequence in $\{0,1\}^\infty$.

2.1 Martingales

Lutz's [5] measure on E is obtained by imposing an appropriate resource-bound on a game theoretical characterization of the classical Lebesgue measure, via martingales. A martingale is a function $d : \{0,1\}^* \to \mathbb{R}_+$ such that, for every $w \in \{0,1\}^*$,

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

This definition can be motivated by the following betting game in which a gambler puts bets on the successive membership bits of a hidden language A. The game proceeds in infinitely many rounds where at the end of round n, it is revealed to the gambler whether $s_n \in A$ or not. The game starts with capital 1. Then, in round $n+1$, depending on the first n outcomes $w = \chi_A[0 \ldots n-1]$, the gambler bets a certain fraction $\epsilon_w d(w)$ of his current capital $d(w)$, that $s_{n+1} \in A$, and bets the remaining capital $(1 - \epsilon_w)d(w)$ on the complementary event $s_{n+1} \notin A$. The game is fair, i.e. the amount put on the correct event is doubled, the one put on the wrong guess is lost, as stated in Equation 1. The value of $d(w)$, where $w = \chi_A[0 \ldots n]$ equals the capital of the gambler after round $n+1$ on language A. The player wins on a language A if he manages to make his capital arbitrarily large during the game. We say

that a martingale d succeeds on a language A, if $d(A) := \limsup_{w \sqsubset A, w \to A} d(w) = \infty$, where we identify language A with its characteristic sequence χ_A. The success set $S^\infty[d]$ of a martingale d is the class of all languages on which d succeeds.

3 A Measure on BPE

Our measure on BPE is defined via the following probabilistic martingales.

Definition 1 *A martingale $d : \{0,1\}^* \to \mathbb{R}_+$ is* BPE*-approximable if there exists a family of approximations $\{\hat{d}_k\}_{k \geq 0}$, where $\hat{d}_k : \{0,1\}^* \to \mathbb{Q}_+$, and a probabilistic Turing machine M, such that for every $w \in \{0,1\}^*$ and every $k, n \in \mathbb{N}$*

$$|\hat{d}_k(w) - d(w)| \leq 2^{-k}, \text{ and}$$

$$\Pr[M(w,k,n) = \hat{d}_k(w)] \geq 1 - 2^{-n}$$

where the probability is taken over the internal coin tosses of M and the running time of M is polynomial in $|w| + k + n$.

Remark 2 *By using standard Chernoff bound arguments it is easy to show that Definition 1 is robust, i.e. the error probability can range from $\frac{1}{2} + \frac{1}{p(n)}$ to $1 - 2^{q(n)}$ for any polynomials p, q, without enlarging (resp. reducing) the class of functions defined this way.*

Definition 3 *A martingale $d : \{0,1\}^* \to \mathbb{Q}_+$ is said to be* BPE*-computable if there exists a probabilistic Turing machine M, such that for every $w \in \{0,1\}^*$ and every $n \in \mathbb{N}$*

$$\Pr[M(w,n) = d(w)] \geq 1 - 2^{-n}$$

where the probability is taken over the internal coin tosses of M and the running time of M is polynomial in $|w| + n$.

We often consider indexed martingales. An indexed BPE-approximable martingale is a martingale d (where $d_i(w) := d(i,w)$) such that there exists a family of approximations $\{\hat{d}_{k,i}\}_{k,i \geq 0}$, where

$$\hat{d}_{k,i} : \{0,1\}^* \to \mathbb{Q}_+$$

and a probabilistic Turing machine M such that for every $w \in \{0,1\}^*$ and every $k, i, n \in \mathbb{N}$

$$|\hat{d}_{k,i}(w) - d_i(w)| \leq 2^{-k}, \text{ and}$$

$$\Pr[M(w,k,i,n) = \hat{d}_{k,i}(w)] \geq 1 - 2^{-n}$$

where the probability is taken over the internal coin tosses of M and the running time of M is polynomial in $|w| + k + i + n$.

Following Lutz [5] we say that a set has measure zero if there is a single martingale that succeeds on it.

Definition 4 *A language A has* BPE*-measure zero if there exists a* BPE*-approximable martingale $d : \{0,1\}^* \to \mathbb{R}_+$ such that*

$$\limsup_{n\to\infty} d(\chi_A[0\ldots n]) = \infty$$

We say that martingale d succeeds on A whenever this is the case.

The success set $S^\infty[d]$ of a martingale d is the class of all languages on which d succeeds.

In order to formalize the third basic property, we need to define what we mean by *enumerable infinite union* of measure zero sets.

Definition 5 *$X = \bigcup_{i\in\mathbb{N}} X_i$ is a* BPE*-union of* BPE*-measure zero sets if there exists an indexed* BPE*-approximable martingale d such that $X_i \subseteq S^\infty[d_i]$.*

The following Lemma states that any BPE-approximable martingale can be replaced by a BPE-computable martingale with the same success set. Its proof is similar to the standard exact computation lemma proof that is found in the literature, see [7] for instance.

Lemma 6 (Exact Computation Lemma) *Let $d : \{0,1\}^* \to \mathbb{R}_+$ be a* BPE*-approximable martingale. Then there exists a* BPE*-computable martingale $d' : \{0,1\}^* \to \mathbb{Q}_+$ such that $S^\infty[d] \subseteq S^\infty[d']$.*

PROOF. Let $\hat{d}$ be an approximation of d, and let M be a probabilistic Turing machine computing $\hat{d}$. Let us define $c(w) := \hat{d}_{|w|}(w)$. We construct the following martingale d' recursively.

$$d'(\lambda) = c(\lambda) + 2$$
$$d'(wb) = d'(w) + \frac{c(wb) - c(w\bar{b})}{2}$$

where $w \in \{0,1\}^*$ and $b \in \{0,1\}$.

Claim 7 *d' is* BPE*-computable.*

Indeed computing $d'(wb)$ requires computing $|w|$ recursive steps, each step requiring two computations of c. By computing c (via M) with error probability smaller than $2^{-s(n)}$ (where $s(n)$ is a polynomial to be determined later), we obtain a total error probability smaller than $2|w|2^{-s(n)}$. Putting $s(n) = \log(|w|) + n + 1$ yields a total error probability smaller than 2^{-n}.

Let us check that d' defines a martingale. It is easy to check that Equation 1 is satisfied. In order to check that $d'(w) \geq 0$ for every $w \in \{0,1\}^*$, we show by induction that

$$d'(w) \geq d(w) + 2^{-|w|}. \tag{2}$$

We have

$$d'(\lambda) = c(\lambda) + 2 \geq d(\lambda) - 2^0 + 2 \geq d(\lambda) + 2^0.$$

For $w \in \{0,1\}^*, b \in \{0,1\}$, we have

$$\begin{aligned} d'(wb) &= d'(w) + \frac{c(wb) - c(w\bar{b})}{2} \\ &\geq d(w) - 2^{-|w|} + \frac{c(wb) - c(w\bar{b})}{2} \\ &\geq d(w) + 2^{-|w|} + \frac{d(wb) - d(w\bar{b})}{2} - 2^{-|w|-1} \\ &= d(wb) + 2^{-|w|-1} \end{aligned}$$

where the first inequality holds by induction and the second holds because $|d(w) - c(w)| \leq 2^{-|w|}$ by definition of c. □

4 The Three Basic Properties

Let us prove that all three basic properties of Lutz measure hold for our measure on BPE.

Theorem 8 *Let L be any language in* BPE*. Then the singleton $\{L\}$ has* BPE*-measure zero.*

PROOF. Let $L \in$ BPE be any language and let M be a Turing machine deciding it. We construct a probabilistic Turing machine T computing martingale d yielded by the following game strategy; On input $w = w_0 w_1 \dots w_{N-1}$ the martingale d will have value 2^N if w is a prefix of χ_L, and 0 otherwise. d is BPE-computable since on input (w, n), T simply computes $\chi_L(s_1), \chi_L(s_1), \dots, \chi_L(s_N)$, (each with error probability smaller than $2^{-(n+N)}$) and checks whether w is a prefix of χ_L. The total error probability is smaller than $N2^{-(n+N)}$ which is less than 2^{-n}. □

The second basic property is proved using the Exact Computation Lemma.

Theorem 9 BPE *does not have* BPE*-measure zero.*

PROOF. Let d be a BPE-approximable martingale. By Lemma 6 we can suppose that d is BPE-computable. We construct a language $L \in \mathsf{BPE}$ such that

$$d(\chi_L[0 \dots N]) \leq d(\lambda)$$

for every $N \geq 1$, i.e. $L \notin S^\infty[d]$. For $N > 0$, let

$$L(s_N) = 1 \text{ iff } d(L(s_0)L(s_1)\dots L(s_{N-1})1) \leq d(L(s_0)L(s_1)\dots L(s_{N-1})0)$$

where d is computed with error probability $2^{-s(n)}$ (where $s(n)$ is a polynomial to be determined later). $L \in \mathsf{BPE}$ because each of the N recursive steps to compute $L(s_N)$ requires two computations of d. This yields a total error probability smaller than $2N2^{-s(n)}$. Putting

$$s(n, N) = \log(N) + n + 1$$

yields a total error probability smaller than 2^{-n}. Moreover d never increases its initial capital along L which ends the proof. □

Finally let us prove the third basic property.

Theorem 10 *Let $X = \bigcup_{i \geq 1} X_i$ be a* BPE*-union of* BPE*-measure zero sets. Then X has* BPE*-measure zero.*

PROOF. Let d be a BPE-approximable indexed martingale such that $X_i \subseteq S^\infty[d_i]$, and let $\hat{d}$ be an approximation of d. We construct a BPE-approximable indexed martingale D such that for every $j \in \mathbb{N}$,

$$S^\infty[d_j] \subseteq S^\infty[D_j]$$

and

$$D_j(\lambda) \leq 2^{-j} \ .$$

Let $w \in \{0,1\}^*$ and $j, k \in \mathbb{N}$. Consider

$$D_j(w) = 2^{\min(0, -\log(\hat{d}_{j,1}(\lambda)) - 2 - j)} d_j(w) \text{ and}$$
$$\hat{D}_{j,k}(w) = 2^{\min(0, -\log(\hat{d}_{j,1}(\lambda)) - 2 - j)} \hat{d}_{j,k}(w).$$

We have

$$|\hat{D}_{j,k}(w) - D_j(w)| \leq |\hat{d}_{j,k}(w) - d_j(w)| \leq 2^{-k}$$

i.e. D is BPE-approximable.

Consider the following martingale

$$d'(w) := \sum_{j=0}^{\infty} D_j(w).$$

The function d' is a well defined martingale because

$$d'(\lambda) \leq \sum_{j=0}^{\infty} 2^{-j} < \infty$$

and

$$d'(w) \leq \sum_{j=0}^{\infty} 2^{|w|} D_j(\lambda) = 2^{|w|} d'(\lambda)$$

where the last inequality holds because a martingale's value at most doubles in each step. It is clear that $X \subseteq S^{\infty}[d']$. Let us show that d' is BPE-approximable. Consider

$$\hat{d'}_k(w) := \sum_{j=0}^{k+|w|+1} \hat{D}_{j,j+k+2}(w)$$

where each $\hat{D}_{j,j+k+2}(w)$ is computed with probability $2^{-s(n)}$ where $s(n)$ is a polynomial to be determined later. We have

$$\begin{aligned}
|\hat{d'}_k(w) - d'(w)| &\leq \sum_{j=0}^{k+|w|+1} |\hat{D}_{j,j+k+2}(w) - D_j(w)| + \sum_{j=|w|+k+2}^{\infty} D_j(w) \\
&\leq \sum_{j=0}^{k+|w|+1} 2^{-(j+k+2)} + \sum_{j=|w|+k+2}^{\infty} 2^{|w|} D_j(\lambda) \\
&\leq \sum_{j=0}^{k+|w|+1} 2^{-(j+k+2)} + \sum_{j=|w|+k+2}^{\infty} 2^{|w|} 2^{-j} \leq 2^{-k}.
\end{aligned}$$

Since computing $\hat{d'}_k(w)$ requires computing $k+|w|+1$ terms $\hat{D}_{j,j+k+2}$, each being computed with error probability smaller than $2^{-s(n)}$, $\hat{d'}_k(w)$ can be computed with error probability smaller than $(k+|w|+1)2^{-s(n)}$. Letting

$$s(n) := \log(k+|w|+1) + n$$

yields a total error probability smaller than 2^{-n}, thus d' is BPE-approximable which ends the proof. □

Remark 11 • *Replacing the time bounds in Definition 3 by* $2^{\log^k |w|} + poly(n)$ *where* k *is a constant yields a measure on the probabilistic class* BPEXP.

- *Several measure notions on* P *were introduced in the last decade [1,15,11]. One can show that the idea of same-valued probabilistic computable martingales carries over to these notions thus yielding measure notions on* BPP.

5 Open Question

Although we now have measure notions on two types of complexity classes: deterministic and probabilistic, the nondeterministic case is still unsettled. We believe that a measure notion on nondeterministic classes would be of some interest. We anticipate that the measure notions we have developed here will be useful in future work.

References

[1] E. Allender and M. Strauss. Measure on small complexity classes, with application for BPP. *Proc. of the 35th Ann. IEEE Symp. on Found. of Comp. Sci.*, pages 807–818, 1994.

[2] R. Impagliazzo and P. Moser. A zero-one law for RP. *Proceedings of the 18th Conference on Computational Complexity*, pages 48–52, 2003.

[3] D. Juedes and J. Lutz. The complexity and distribution of hard problems. *Proceedings of the 34th FOCS Conference*, pages 177–185, 1993.

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

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

[6] J.H. Lutz. The quantitative structure of exponential time. In L.A. Hemaspaandra and A.L. Selman, editors, *Complexity Theory Retrospective II*, pages 225–260. Springer, 1997.

[7] E. Mayordomo. *Contributions to the study of Resource-Bounded measure.* PhD thesis, Universitat Politecnica Catalunya, 1994.

[8] Elvira Mayordomo. Measuring in PSPACE. *Proceedings of the 7th International Meeting of Young Computer Scientists (IMYCS'92). Gordon-Breach Topics in Computer Science 6*, 136:93–100, 1994.

[9] P. Moser. *Derandomization and Quantitative Complexity.* PhD thesis, University of Geneva, 2004.

[10] P. Moser. Baire categories on small complexity classes and meager-comeager laws. *Inform. Comput.*, 2007.

[11] Philippe Moser. Martingale families and dimension in P. In Arnold Beckmann, Ulrich Berger, Benedikt Löwe, and John V. Tucker, editors, *CiE*, volume 3988 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 2006.

[12] C. Papadimitriou. *Computational complexity.* Addisson-Wesley, 1994.

[13] Alexander A. Razborov and Steven Rudich. Natural proofs. *J. Comput. Syst. Sci.*, 55(1):24–35, 1997.

[14] K. Regan and D. Sivakumar. Probabilistic martingales and BPTIME classes. *In Proc. 13th Annual IEEE Conference on Computational Complexity*, pages 186–200, 1998.

[15] M. Strauss. Measure on P- strength of the notion. *Inform. and Comp.*, 136:1:1–23, 1997.