Available online at www.sciencedirect.com

ScienceDirect

Information Processing Letters 106 (2008) 241–245

Information Processing Letters

www.elsevier.com/locate/ipl

Resource-bounded measure on probabilistic classes

Philippe Moser

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

Received 23 April 2007; received in revised form 9 November 2007; accepted 12 November 2007

Available online 8 December 2007

Communicated by P.M.B. Vitányi

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.

Keywords: Resource-bounded measure; Probabilistic complexity classes; Computational complexity; Randomized algorithms

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 exception in the class. For instance, it was shown [3] that the set of $\leqslant_m^p$-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

E-mail address: pmoser@cs.nuim.ie.

0020-0190/$ – see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.ipl.2007.11.019

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 [8,1,14,10] 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 [13], the notion of measure on probabilistic classes has been investigated. Probabilistic martingales were introduced in [13], 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 [13], including the classes that the "natural proofs" of [12] are useful against, the Turing-complete sets for EXP, and $\mathsf{BPTIME}(2^{cn})$ (for any constant c). Unfortunately the notion of [13] 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 [13]), hence the measure of the classes shown to be small in [13] 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 [1,14,10]) to yield measure notions on BPP. For a notion of probabilistic Baire categories, see [9].

2. Preliminaries

We use standard notation for traditional complexity classes, see for instance [11]. 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 $1 \leqslant i \leqslant |w|$ 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 $\varepsilon_w d(w)$ of his current capital $d(w)$, that $s_{n+1} \in A$, and bets the remaining capital $(1 - \varepsilon_w) d(w)$ 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 Eq. (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.