Electronic Colloquium on Computational Complexity, Report No. 29 (2003)

BPP has effective dimension at most 1/2 unless BPP = EXP

Philippe Moser*

Abstract

We prove that BPP has Lutz's p-dimension at most $1/2$ unless BPP equals EXP. Next we show that BPP has Lutz's p-dimension zero unless BPP equals EXP on infinitely many input lengths. We also prove that BPP has measure zero in the smaller complexity class SUBEXP unless MA = EXP. Finally we show that under the plausible assumption DTIME(2^{dn}) is hard to approximate by SAT-oracle circuits of size q (for every fixed polynomial q) BPP has p-dimension zero.

1 Introduction

Lutz [Lut00] has recently introduced an effective generalization of Hausdorff dimension, by defining a resource-bounded Hausdorff dimension on exponential time complexity classes such as E and EXP, and on exponential space complexity classes. One of the motivation is to quantify the structure of sets that have resource-bounded measure zero, in the same way as classical Hausdorff dimension can be used to quantify many sets of Lebesgue measure zero. For instance Lutz proved in [Lut00], that for every real number $\alpha \in [0,1]$, the class SIZE($\alpha 2^n/n$) has dimension α in ESPACE.

Up to now, no results about the dimension of standard complexity classes were known. We give such a result by showing that BPP has p-dimension at most one half, unless BPP is intractable, i.e. BPP = EXP. Thus we improve the zero-one resource-bounded measure law for BPP from [Mel00], by showing that either BPP has p-dimension at most $1/2$, or else has p-measure one.

We also prove that BPP is a very small subset of E, unless BPP is intractable on infinitely many input lengths, i.e. BPP has p-dimension zero, unless BPP equals EXP infinitely often.

Next we investigate the measure of BPP in complexity classes smaller than E, such as SUBEXP, with the measure notion of [AS94]. We improve a result of [BFF97] by showing that BPP has measure zero in SUBEXP, unless MA = EXP.

One important issue in derandomization theory is to find plausible hypothesis implying P = BPP. More details on this topic can be found in [Kab02]. Still it is possible that BPP is a small subset of EXP whithout being equal to P. Therefore searching for some weaker hypothesis than those implying the P = BPP equality, that still imply that BPP is a small subset of EXP, is of great interest. We use a recent modified result of [GW02] to give such a hypothesis, which is not known to imply the P = BPP equality, namely that if for some $d > 0$, DTIME(2^{dn}) is hard to approximate by SAT-oracle circuits of size q for every fixed polynomial q, then BPP has p-dimension 0.

*Address: Computer Science Department, University of Geneva. Email: moser@cui.unige.ch

ISSN 1433-8092

2 Preliminaries

We use standard notation for traditional complexity classes; see for instance [BDG95] and [BDG90], or [Pap94]. Let us recall the definition of subexponential time classes. SUBEXP is the class $\bigcap_{\epsilon>0} \mathsf{DTIME}(2^{n^\epsilon})$, and for $\alpha > 0$, the slice E_α is defined as $\mathsf{E}_\alpha = \bigcup_{\delta<\alpha} \mathsf{DTIME}(2^{n^\delta})$. Two complexity classes C, D are said equal infinitely often, denoted $C \overset{i.o.}{=} D$, if for every language $A \in C$ there is a language $B \in D$, such that $A \cap \{0,1\}^n = B \cap \{0,1\}^n$ for infinitely many n. The symmetric difference of two languages A and B, denoted $A \triangle B$, is given by $A \triangle B = (A - B) \cup (B - A)$. For a polynomial q, denote by $\mathsf{SIZE}^{\mathrm{SAT}}(q)$ the class of languages decided by Boolean circuits of size q with oracle gates for SAT. We say that class C is hard to approximate by $\mathsf{SIZE}^{\mathrm{SAT}}(q)$ circuits, if any such circuits fails to guess the correct value of a random instance with success probability greater than $2/3$.

Let us fix some notations for strings and languages. Let $s_0, s_1, \ldots$ be the standard enumeration of the strings in $\{0,1\}^*$ in lexicographical order, where $s_0 = \lambda$ denotes the empty string. A sequence is an element of $\{0,1\}^\infty$. If w is a string or a sequence and $0 \leq i < |w|$ 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. We identify language L with its characteristic function χ_L, where χ_L is the sequence such that $\chi_L[i] = 1$ iff $s_i \in L$. We denote by $L|m$ the string consisting of the first m bits of the characteristic sequence of L. If w_1 is a string and w_2 is a string or a sequence extending w_1, we write $w_1 \sqsubseteq w_2$. Finally we denote by log the logarithm to the base 2.

2.1 Lutz's p-dimension

Lutz's [Lut92] measure on E is obtained by imposing 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, depending on the first $n-1$ 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 the nth word $s_n \in A$, and bets the remaining capital $(1-\epsilon_w)d(w)$ on the complementary event $s_n \notin A$. 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 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.

We sometimes relax Equation 1 by considering supermartingales. A supermartingale is a function $d : \{0,1\}^* \to \mathbb{R}_+$ such that, for every $w \in \{0,1\}^*$, $d(w) \leq \frac{d(w0)+d(w1)}{2}$, i.e. the associated strategy is allowed to throw money away.

Lutz's idea for defining a dimension notion via martingales, is to perceive taxes on the martingales' wins, so that only martingales whose capital grows quickly are considered. This

motivates the following definition.

Definition 1 *For a real number $s \geq 0$, a martingale is said s-successful on a language A, if*

$$\limsup_{m\to\infty} \frac{d(A|m)}{2^{(1-s)m}} = \infty. \tag{2}$$

A martingale is s-successful on a class if it is s-successful on every member of the class.

The dimension of a class is defined as the largest tax rate which can be perceived on the martingales' benefits, without preventing them from winning.

Definition 2 *Let C be any complexity class. The p-dimension of C is the infimum over all $s' \in [0,1]$, such that there exists a martingale d computable in polynomial time which s' succeeds on C.*

Lutz's proved in [Lut00] that the p-dimension notion satisfies all three standard measure axioms, namely that E has p-dimension one, every single language in E has p-dimension zero, and finally easy infinite unions of sets of p-dimension s have p-dimension s. More precisely,

Definition 3 *Let $X, X_0, X_1, X_2, \cdots$ be complexity classes. X is a p-union of the p-dimensioned sets $X_0, X_1, X_2, \cdots$ if $X = \bigcup_{k\geq 0} X_k$, and for each $s > \sup_{k\in\mathbb{N}} \dim_p(X_k)$ with 2^s rational, there is a function $d : \mathbb{N} \times \{0,1\}^* \to [0,\infty[$ with the following properties.*

1. *d is p-computable.*
2. *For each $k \in \mathbb{N}$, the function $d_k(w) := d(k,w)$ is a martingale.*
3. *For each $k \in \mathbb{N}$, d_k s-succeeds on X_k.*

The following Lemma states that the p-dimension of a p-union of sets is the supremum of the p-dimension of all sets.

Lemma 1 *[Lut00]*
Let $X, X_0, X_1, X_2, \cdots$, be a p-union of the p-dimensioned sets $X_0, X_1, X_2, \cdots$. Then

$$\dim_p(X) = \sup_{k\in\mathbb{N}} \dim_p(X_k).$$

2.2 Measure on SUBEXP

We will use the measure notion of [AS94] on the class SUBEXP. For the sake of completeness, let us recall the definitions of [AS94] adapted to the class SUBEXP. To define a measure on E_α, with $\alpha > 0$, supermartingales computed by Turing machines with random access to their inputs were considered in [AS94], that is on input w, the machine can query any bit of w to its oracle. In order to allow such Turing machines to compute the lengths of their inputs w without querying their oracles, they also have access to $s_{|w|}$; this convention is denoted by $M^w(s_{|w|})$.

It is widely believed that random access subexponential time Turing machines are too strong to define a measure on subexponential time classes, because it is not clear whether the whole class has not measure zero relatively to subexponential-time computed supermartingales. Therefore the concept was weakened in [AS94] by bounding the number of recursive

queries such a Turing machine is allowed to make. Let M be a random access Turing machine and $n \in \mathbb{N}$. Define the dependency set $G_{M,n} \subseteq \{1, 2, \ldots, 2^{n+1} - 1\}$ such that for every string $w \in \{0,1\}^*$ coding for words of size up to n, M can compute $M^w(s_{|w|})$ querying only input bits in $G_{M,n}$.

A measure notion on SUBEXP was introduced in [AS94] by considering subexponential-time random access Turing machines with subexponential size dependency sets.

Definition 4 *Let $\alpha > 0$. A class A of languages is said to have E_α-measure zero if there exists a supermartingale d, such that $d(w)$ is computable in time 2^{n^δ}, with $\delta < \alpha$ and $n = |s_{|w|}|$, by a random access Turing machine with dependency set of size 2^{n^δ}, and such that $A \subseteq S^\infty[d]$.*

Such a supermartingale is called an E_α-computable supermartingale.

It is shown in [AS94] that this measure notion satisfies all three measure axioms. Let us formulate the third axiom more precisely.

Definition 5 *Let $\alpha > 0$. $X = \bigcup_{i \in \mathbb{N}} X_i$ is an E_α-union of E_α-measure zero sets if there exists an indexed supermartingale d such that $X_i \subseteq S^\infty[d_i]$, where $d_i(w) = d(i, w)$ is computable in time $2^{n^\delta} + q(i)$, for some polynomial q, with $\delta < \alpha$ and $n = |s_{|w|}|$, by a random access Turing machine with dependency set of size 2^{n^δ}.*

It is proven in [AS94] that the third axiom holds for the measure notion on SUBEXP.

Theorem 1 *[AS94]*
Let $X = \bigcup_{i \geq 1} X_i$ be an E_α-union of E_α-measure zero sets. Then X has E_α-measure zero.

3 BPP has dimension at most one half unless BPP = EXP

The next result states that the dimension of BPP is at most $1/2$, unless BPP in intractable.

Theorem 2 *If* BPP $\neq$ EXP *then* BPP *has p-dimension at most* $1/2$.

Proof. The proof relies on the following result.

Theorem 3 *Let C be any complexity class such that for every language $A \in C$ there exists a language $B \in \mathsf{DTIME}(2^n)$, such that*

$$\Pr_{|x|=m}[A(x) = B(x)] > 1 - 1/m, \tag{3}$$

for infinitely many lengths m. Then C has p-dimension at most $1/2$.

Proof. Let $B \in \mathsf{DTIME}(2^n)$ be any language and let $m > 0$. Consider the following betting strategy d_B, which divides its initial capital into infinitely many capitals $\{1/m^2\}_{m>0}$, where share $1/m^2$ will be bet on strings of size m, in the following way. d_B bets a fraction a (which will be determined later) of its current capital that the membership bits are the same as those of B.

Computing $d_B(w)$, where w is the characteristic sequence of some language for words up to length t, can be done by computing the memberships bits of B for all words of size less than t in lexicographical order. Since $B \in \mathsf{DTIME}(2^n)$, d_B is computable in time $t2^t \leq |w|^2$.

Moreover if A is a language such that Equation 3 holds, there are infinitely many lengths m on which d_B multiplies its initial capital $1/m^2$ by a a factor $1+a$ on at least a fraction $1-1/m$ of all 2^m bets it makes on words of size m. Consider $M(A)$ the infinite set of lengths such that Equation 3 holds. For every $m \in M(A)$ we have,

$$d_B(\chi_A|2^{m+1}) \geq \frac{1}{m^2}(1+a)^{(1-1/m)2^m}(1-a)^{1/m2^m} = \frac{1}{m^2}[(1+a)^{1-1/m}(1-a)^{1/m}]^{2^m} \tag{4}$$

Consider the set C_B of all languages A satisfying Equation 3. Let us show that C_B has p-dimension at most $1/2$. Let $s > 1/2$, and $A \in C_B$ be any language. Consider the martingale $d = d_{(s,B)}$ as above, where the betting fraction a depends on s and will be determined later. Equation 4 implies,

$$\limsup_{m\to\infty} \frac{d(\chi_A|2^{m+1})}{2^{(1-s)2^{m+1}}} \geq \limsup_{m\to\infty} \frac{1}{m^2} \cdot [\frac{(1+a)^{1-1/m}(1-a)^{1/m}}{2^{2(1-s)}}]^{2^m}$$

Consider $F(a,m) := \frac{(1+a)^{1-1/m}(1-a)^{1/m}}{2^{2(1-s)}}$. Let us show that there exist $0 < a_0 < 1$, $M_0 \geq 1$ and $c > 1$, such that for every $m \geq M_0$, $F(a_0,m) \geq c$. This immediately implies $\limsup_{m\to\infty} \frac{d(\chi_A|2^{m+1})}{2^{(1-s)2^{m+1}}} = \infty$. Since $s > 1/2$, let $\delta > 0$ be such that $2(1-s) = 1-\delta$. Let $0 < a_0 < 1$ and $M \geq 1$ be such that for every $m \geq M$, $\frac{m-1}{m}\log(1+a_0) \geq 1-\delta/4$. Let $M' \geq 1$ be such that for every $m \geq M'$, $|\frac{1}{m}\log(1-a_0)| < \delta/4$. Consider

$$T(a_0,m) = \frac{m-1}{m}\log(1+a_0) + \frac{1}{m}\log(1-a_0),$$

and let $M_0 = \max(M, M')$. For every $m \geq M_0$, we have $T(a_0,m) \geq 1-\delta/2 > 2(1-s)$. Therefore there exists $\delta' > 0$, such that $T(a_0,m) \geq 2(1-s)+\delta'$, which implies $\frac{2^{T(a_0,m)}}{2^{2(1-s)}} \geq 2^{\delta'}$. Let $c = 2^{\delta'} > 1$, thus for every $m \geq M_0$, $F(a_0,m) \geq c$.

Let $M_1, M_2, \cdots$ be a standard enumeration of Turing machines running in deterministic time 2^n, where M_i runs in time polynomial in $i+2^n$, and denote by B_i the language decided by M_i. We will apply Lemma 1, with $X_i = C_{B_i}$. Let $s > 1/2$ be such that 2^s is rational. The indexed martingale $d_s(k,w) := d_{(s,B_k)}(w)$ satisfies Definition 3, therefore the class $\cup_{i\geq 1} C_{B_i}$ has p-dimension at most $1/2$ by Lemma 1. Since $C \subseteq \cup_{i\geq 1} C_{B_i}$, C has p-dimension at most $1/2$, which ends the proof of Theorem 3.

Theorem 3 combined with the following result from [IW98] ends the proof.

Theorem 4 *If* $\mathsf{BPP} \neq \mathsf{EXP}$ *then for every language* $A \in \mathsf{BPP}$ *and every* $\epsilon > 0$*, there is a language* $B \in \mathsf{DTIME}(2^{n^\epsilon})$ *such that the following holds: For any constant* $d > 0$ *and any length-preserving randomized polynomial time Turing machine* M*,*

$$\Pr[A(M(1^m)) = B(M(1^m))] > 1 - m^{-d}$$

for infinitely many m*, where the probability is taken over the internal coin tosses of* M*.*

Consider the following length-preserving randomized polynomial time Turing machine M, which on input 1^m and m-sized random string w outputs w. Applying Theorem 4 with $\epsilon = 1$ and $d = 1$ yields

$$\Pr_{|x|=m}[A(x) = B(x)] > 1 - \frac{1}{m}. \tag{5}$$

Thus by Theorem 3, $\mathsf{BPP} \neq \mathsf{EXP}$ implies that BPP has p-dimension at most $1/2$, which ends the proof. □

3.1 BPP has p-dimension zero unless BPP $\stackrel{i.o.}{=}$ EXP

It is possible to reduce the 1/2 bound of Theorem 2 to zero under the stronger hypothesis BPP be intractable on infinitely many input lengths.

Theorem 5 *Either* BPP *equals* EXP *infinitely often, or* BPP *has p-dimension* 0.

Proof. The proof relies on the following result.

Theorem 6 *Let C be any complexity class such that for every language $A \in C$ there exists a language $B \in \mathsf{DTIME}(2^n)$, such that*

$$\Pr_{|x|=m}[A(x) = B(x)] > 1 - 1/m, \tag{6}$$

for almost every lengths m. Then C has p-dimension 0.

Proof. Similar to Theorem 3.

Theorem 6 combined with the following slightly modified version of Theorem 4 ends the proof.

Theorem 7 *If* BPP $\stackrel{i.o.}{\neq}$ EXP *then for every language $A \in$ BPP and every $\epsilon > 0$, there is a language $B \in \mathsf{DTIME}(2^{n^\epsilon})$ such that the following holds: For any constant $d > 0$ and any length-preserving randomized polynomial time Turing machine M,*

$$\Pr[A(M(1^m)) = B(M(1^m))] > 1 - m^{-d}$$

for almost every m, where the probability is taken over the internal coin tosses of M.

□

4 BPP has SUBEXP-measure zero unless MA = EXP

The next result states that BPP is small compared to SUBEXP, under the assumption MA $\neq$ EXP.

Theorem 8 *For every $\alpha > 0$,* BPP *has E_α-measure zero, unless* MA = EXP.

Proof. The proof relies on the following result.

Theorem 9 *Let C be any complexity class such that for every language $A \in C$ and for every $\epsilon > 0$, there exists a language $B \in \mathsf{DTIME}(2^{n^\epsilon})$, such that*

$$A \cap \{0,1\}^n = B \cap \{0,1\}^n \tag{7}$$

for infinitely many input lengths. Then C has E_α-measure 0*, for every $\alpha > 0$.*

Proof. Let $\alpha > 0$ and let $\delta = \alpha/2$. Let $B \in \mathsf{DTIME}(2^{n^\delta})$ be any language and let $m > 0$. Consider the following betting strategy, which starts with initial capital $1/m^2$ for words of size m, and on the first m words of size m, bets its current capital that the membership bits are the same as those of B.

The dependency set of d_B has polynomial size. Computing $d_B(w)$, where w is the characteristic sequence of some language for words up to length m, can be done by computing the memberships bits of B for the t first words of size t, for every $t = 1, 2, \cdots, m$. Since $B \in \mathsf{DTIME}(2^{n^\delta})$, d_B is computable in time $m^2 2^{m^\delta}$ which is less than 2^{m^α}.

Let A be a language satisfying Equation 7. There are infinitely many lengths m on which d_B multiplies its initial capital $1/m^2$ by a a factor 2^m. Consider $M(A)$ the infinite set of lengths m such that Equation 7 holds. For every $m \in M(A)$ we have, $d(\chi_A|2^{m+1}) \geq \frac{1}{m^2}2^m$, which implies

$$\lim_{m\to\infty} d(\chi_A|2^{m+1}) = \infty. \tag{8}$$

Consider the set C_B of all languages A satisfying Equation 7. Equation 8 implies that C_B has E_α-measure zero.

Let $M_1, M_2, \cdots$ be a standard enumeration of Turing machines running in deterministic time 2^{n^δ}, where M_i runs in time polynomial in $i+2^{n^\delta}$, and denote by B_i the language decided by M_i. The classes $C_{B_1}, C_{B_2}, \cdots$, satisfy Definition 5 with the following indexed martingale $d(k, w) := d_{B_k}(w)$. Therefore the class $\cup_{i\geq 1} C_{B_i}$ has E_α-measure zero by Theorem 1. Choosing $\epsilon = \delta$ implies that $C \subseteq \cup_{i\geq 1} C_{B_i}$, thus C has E_α-measure zero. This ends the proof of Theorem 9.

Theorem 9, combined with the following result from [BFNW93] ends the proof.

Theorem 10 *[BFNW93] If* $\mathsf{MA} \neq \mathsf{EXP}$ *then for every language* $A \in \mathsf{BPP}$ *and every* $\epsilon > 0$, *there is a language* $B \in \mathsf{DTIME}(2^{n^\epsilon})$ *such that* $A \cap \{0,1\}^n = B \cap \{0,1\}^n$, *for infinitely many lengths* n.

By Theorem 10 the hypothesis of Theorem 9 are satisfied, which ends the proof. □

5 Plausible assumption implying the smallness of BPP

The following result states that BPP is a small subset of E if $\mathsf{DTIME}(2^{dn})$ is hard to approximate by polynomial-size circuits with SAT oracle gates, for some $d > 0$.

Theorem 11 *Suppose there exists* $d > 0$ *such that for every polynomial* q *there exists a set in* $\mathsf{DTIME}(2^{dn})$ *that is hard to approximate in* $\mathsf{SIZE}^{\mathrm{SAT}}(q)$, *then* BPP *has p-dimension zero.*

Proof. The proof relies on the following result.

Theorem 12 *Let* $d > 0$. *Let* C *be any complexity class such that for every language* $A \in C$ *and for every* $\epsilon > 0$, *there exists a language* $B \in \mathsf{DTIME}(2^{dn})$, *such that*

$$(A \cap \{0,1\}^n) \triangle (B \cap \{0,1\}^n) \leq 2^{n^\epsilon}. \tag{9}$$

for every $n \in \mathbb{N}$. *Then* C *has p-dimension* 0.

Proof. Let $s > 0$ and $d > 0$. For a language $B \in \mathsf{DTIME}(2^{dn})$, the martingale $d_{(s,B)}$ (denoted d_B) starts with initial capital C_0, and bets a fraction a (with $0 < a < 1$) of its current capital according to the membership bit of B. It is easy to check that d_B is computable in polynomial

time. Let A be any language satisfying Equation 9, where ϵ will be determined later. Let $m \in \mathbb{N}$. Since $\chi_A|m+1$ codes A up to strings of size $\log m$, we have

$$d_B(\chi_A|m+1) = C_0 \cdot (1+a)^{J(m+1)} \cdot (1-a)^{F(m+1)}$$

where $J(m+1)$ is the number of strings of size at most $\log m$ not in $A \triangle B$, and $F(m+1)$ is the number of strings of size at most $\log m$ in $A \triangle B$. Equation 9 implies $F(m+1) \leq \sum_{j=1}^{\log m} 2^{j^\epsilon} \leq \log m 2^{\log^\epsilon m}$. Thus $J(m+1) \geq \sum_{j=1}^{\log m}(2^j - 2^{j^\epsilon}) \geq m - \log m 2^{\log^\epsilon m}$. This implies

$$d_B(\chi_A|m+1) \geq C_0 \cdot (1+a)^{m-\log m 2^{\log^\epsilon m}} \cdot (1-a)^{\log m 2^{\log^\epsilon m}} \geq C_0 \cdot (1+a)^m \cdot (\frac{1-a}{1+a})^{m^{2\epsilon}}$$

Define $0 < a < 1$ such that $b := (1+a)/2^{(1-s)} > 1$. Putting $\epsilon = 1/4$ yields

$$\frac{d_B(\chi_A|m+1)}{2^{(1-s)(m+1)}} \geq \frac{C_0}{2} \cdot b^m \cdot (1/c)^{\sqrt{m}}$$

where $c = \frac{1+a}{1-a} > 1$. Thus

$$\frac{d_B(\chi_A|m+1)}{2^{(1-s)(m+1)}} \geq \frac{C_0}{2} \cdot 2^{(m \log b)} \cdot 2^{(-\sqrt{m} \log c)} = 2^{(m \log b - \sqrt{m} \log c)}$$

Since $\lim_{m\to\infty}(m \log b - \sqrt{m} \log c) = \infty$, we have

$$\lim_{m\to\infty} \frac{d_B(\chi_A|m+1)}{2^{(1-s)(m+1)}} = \infty \tag{10}$$

i.e. d_B s-succeeds on A.

Let $M_1, M_2, \cdots$ be a standard enumeration of $\mathsf{DTIME}(2^{dn})$, where machine M_i runs in time $2^{dn} + q(i)$ for some fixed polynomial q. Define $d_i := d_{(s,B_i)}$ with initial capital $C_0 = 1/i^2$. Denote by X_i the set of languages on which d_i s-succeeds. Since s is a arbitrary, $X_1, X_2, \cdots$ satisfy the hypothesis of Lemma 1, therefore $\bigcup_{i\geq 1} X_i$ has p-dimension 0. Since for every language $A \in \mathsf{BPP}$ there exists a language $B \in \mathsf{P}$ such that Equation 9 holds, we have $\mathsf{BPP} \subseteq \bigcup_{i\geq 1} X_i$, which implies that BPP has p-dimension zero. This ends the proof of Theorem 12. Theorem 12 combined with the following modified result from [GW02] ends the proof. It is easy to verify that the results in [GW02] can be modified to obtain the following theorem.

Theorem 13 *Under the assumption of Theorem 11, it holds that for every $\epsilon > 0$, every language in BPP can be decided by a deterministic algorithm running in time $2^{(d+2)n}$ that errs on at most 2^{n^ϵ} of the n-bit long inputs.*

Finally with the use of Theorem 13, the hypothesis of Theorem 12 are satisfied, which ends the proof. □

6 Final Remark

Obtaining a zero-one dimension law for BPP, by reducing the 1/2 bound to zero, deserves further investigation. One way to obtain such a result would be to improve the uniform derandomization of BPP of Theorem 4, by either obtaining an almost everywhere result, or by reducing the error bound from $1 - m^{-d}$ to some quasi-polynomial bound. Improving the zero-one law for RP from [IM03] to the resource-bounded dimension setting, would also be interesting.

References

[AS94] E. Allender and M. Strauss. Measure on small complexity classes, with application for BPP. *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 807–818, 1994.

[BDG90] J. L. Balcazar, J. Diaz, and J. Gabarro. *Structural Complexity II.* EATCS Monographs on Theorical Computer Science Volume 22, Springer Verlag, 1990.

[BDG95] J. L. Balcazar, J. Diaz, and J. Gabarro. *Structural Complexity I.* EATCS Monographs on Theorical Computer Science Volume 11, Springer Verlag, 1995.

[BFF97] H. Buhrman, S. Fenner, and L. Fortnow. Results on resource-bounded measure. *Proceedings of the 24th International Colloquium on on Automat, Languages and Programming*, pages 188–194, 1997.

[BFNW93] L. Babai, L. Fortnow, N. Nissan, and A. Widgerson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Complexity*, 3:307–318, 1993.

[GW02] O. Goldreich and N. Widgerson. Derandomization that is rarely wrong from short advice that is typically good. *to be published*, 2002.

[IM03] R. Impagliazzo and P. Moser. A zero-one law for RP. *to be published in computational complexity conference*, 2003.

[IW98] R. Impagliazzo and A. Widgerson. Randomness vs time de-randomization under a uniform assumption. *Proceedings of the 39th IEEE Symposium on Foundations of Computer Science*, pages 734–743, 1998.

[Kab02] V. Kabanets. derandomization: a brief overview. Technical Report 02-08, Electronic Colloquium on Computational Complexity, January 2002.

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

[Lut00] J.H. Lutz. Dimension in complexity classes. *Proceedings of the 15th Annual IEEE Conference on Computational Complexity*, pages 158–169, 2000.

[Mel00] D. Melkebeek. The zero one law holds for BPP. *Theoretical Computer Science*, 244(1-2):283–288, 2000.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms.* Cambridge University Press, New York, 1995.

[Pap94] C. Papadimitriou. *Computational complexity.* Addisson-Wesley, 1994.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'