Hausdorff Dimension in Exponential Time

Klaus Ambos-Spies Wolfgang Merkle Jan Reimann Frank Stephan
Mathematisches Institut, Universität Heidelberg
Im Neuenheimer Feld 294, 69120 Heidelberg, Germany
ambos|merkle|reimann|fstephan@math.uni-heidelberg.de

Abstract

In this paper we investigate effective versions of Hausdorff dimension which have been recently introduced by Lutz. We focus on dimension in the class E *of sets computable in linear exponential time. We determine the dimension of various classes related to fundamental structural properties including different types of autoreducibility and immunity. By a new general invariance theorem for resource-bounded dimension we show that the class of p-m-complete sets for* E *has dimension* 1 *in* E*. Moreover, we show that there are p-m-lower spans in* E *of dimension* $\mathcal{H}(\beta)$ *for any rational* β *between* 0 *and* 1*, where* $\mathcal{H}(\beta)$ *is the binary entropy function. This leads to a new general completeness notion for* E *that properly extends Lutz's concept of weak completeness. Finally we characterize resource-bounded dimension in terms of martingales with restricted betting ratios and in terms of prediction functions.*

1. Introduction

In 1919, HAUSDORFF [8] introduced a theory of dimension which generalizes Lebesgue measure and, in particular, ramifies the structure of measure zero sets. *Hausdorff dimension*, as it was called afterwards, found applications in many areas of mathematics such as number theory or dynamical systems (see for instance [7]). Probably best-known is the role Hausdorff dimension plays in fractal geometry, where it turned out to be a suitable concept for distinguishing fractal sets from sets of a rather "smooth" geometrical nature.

In the context of computability, originating from applications of Hausdorff dimension in information theory (see for example [4]), a close connection between Hausdorff dimension and Kolmogorov complexity was established [6, 16, 17, 18, 20, 21], and the notion of effective dimension was introduced [14]. Recently, LUTZ [13] has extended the theory of effective dimension to complexity theory by introducing resource-bounded dimension. Like for classical Hausdorff dimension, LUTZ's approach yields a generalization of resource-bounded measure and a refinement of measure zero classes. Hence resource-bounded dimension might help to obtain a more complete picture of quantitative aspects of structural properties.

In this paper, we focus on the exponential time class $\mathrm{E} = \bigcup_{k\in\mathbb{N}} \mathrm{DTIME}\,(2^{kn})$ and on the corresponding concepts of p-dimension and dimension in E, which have been introduced by LUTZ in terms of betting games computable in polynomial time. We continue the investigation of the dimension of measure-0-classes in E started by LUTZ [13], where we concentrate on relations between reducibility and dimension.

By a new general invariance theorem for resource-bounded dimension we show that (in contrast to p-measure), for any problem A in E, the class of problems p-m-reducible to A has the same p-dimension as the class of problems that are p-m-equivalent to A. In particular this shows that the measure-0-class of the p-m-complete problems for E has dimension 1 in E, which in turn implies that the small-span-theorem of JUEDES and LUTZ [9] for measure in E cannot be extended to dimension in E.

The further investigation of the p-dimension of the lower p-m-spans leads to another remarkable difference between p-measure and p-dimension. While any p-measurable lower p-m-span has either measure 0 or measure 1 in E, here we show that for any rational $\beta \in [0, 1]$ there is a lower p-m-span of dimension $\mathcal{H}(\beta)$ in E, where $\mathcal{H}(\beta)$ is the binary entropy function. This leads to a new completeness notion for E based on dimension, which properly extends LUTZ's concept of weak completeness based on measure.

The above investigations are supplemented by results on the p-dimension of some other interesting structural properties like different types of autoreducibility and immunity.

In the final part of the paper, based on previous work of LUTZ, SCHNORR, and STAIGER, we give some equivalent characterizations of resource-bounded dimension in terms of martingales and prediction functions.

The outline of the paper is as follows. In Section 2 we introduce resource-bounded Hausdorff dimension and state some useful facts on it. Our definition slightly differs from LUTZ's original concept (see Section 5) but it leads to the same notion of p-dimension and dimension in E. In Sections 3 and 4 we prove our main results on the p-dimension of lower p-m-spans. Finally, alternative characterizations of resource-bounded dimension are discussed in Section 5.

Our notation is fairly standard, for unexplained notation see [1, 12]. Strings are always over the alphabet $\{0,1\}$, and we write z_i for the ith string in length-lexicographical order, i.e., z_0 is the empty string λ, z_1 is the string 0, and so on. We identify the set of natural numbers $\mathbb{N}$ with the set of strings via the mapping $i \mapsto \mathrm{z}_i$. Unless explicitly stated otherwise, sets are sets of natural numbers and classes are sets of sets of natural numbers.

We identify a set with its characteristic sequence, i.e., with a function from $\mathbb{N}$ to $\{0,1\}$. In the context of computations that receive as input an initial segment of a set we write w or v for this prefix and m for its length, whereas if the input of a computation is meant as a possible member of a set, we use x, y, or z for the input and n for its length. Observe that in case of $w = A(0)\dots A(m)$, the length n of the string $x = \mathrm{z}_m$ is approximately $\log m$. We abbreviate $A(0)\dots A(m-1)$ by $A\restriction m$.

A set A is p-m-reducible to a set B, written $A \leq^{\mathrm{P}}_{\mathrm{m}} B$, if A is in P or if there is a polynomial-time computable function f such that for all x, $A(x) = B(f(x))$. The lower p-m-span of a set A is the class of all sets that are p-m-reducible to A, and likewise the upper p-m-span of a set is the class of all sets to which A p-m-reduces. The p-m-degree of a set is the intersection of its lower and upper p-m-span. We write $\mathrm{span}^{\mathrm{P}}_{\mathrm{m}}(A)$ and $\mathrm{deg}^{\mathrm{P}}_{\mathrm{m}}(A)$ for the lower p-m-span and the p-m-degree of a set A.

2. Hausdorff Dimension in Exponential Time

LUTZ [13] has shown that the classical concept of Hausdorff dimension can be expressed in terms of martingales. He then used this fact to derive a concept of resource-bounded dimension. In this section we give a definition of resource-bounded dimension that is easily seen to be equivalent to the one by LUTZ. First, we briefly review the concepts of martingale and betting strategy.

Definition 1 *A* betting strategy *b is a function*

$$b : \{0,1\}^* \to [0,1] \times \{0,1\}.$$

The (normed) martingale

$$d_b : \{0,1\}^* \to [0,\infty)$$

induced by a betting strategy *b is inductively defined by* $d_b(\lambda) = 1$ *and*

$$\begin{aligned} d_b(wi_w) &= d_b(w)(1+\alpha_w), & (1)\\ d_b(w(1-i_w)) &= d_b(w)(1-\alpha_w) & (2) \end{aligned}$$

for $w \in \{0,1\}^*$ and $b(w) = (\alpha_w, i_w)$. A martingale *is a martingale induced by some betting strategy. A martingale d* succeeds on a set *A if*

$$\limsup_{m\to\infty} d(A\restriction m) = \infty,$$

and d succeeds on a class $\mathcal{C}$ if d succeeds on every member A of $\mathcal{C}$.

This definition can be motivated by the following fair betting game in which a gambler puts bets on the successive bits of a hidden sequence $A \in \{0,1\}^{\mathbb{N}}$. The game proceeds in infinitely many rounds where at the end of round m the m-th bit of the sequence A is revealed to the player. The gambler starts with (normed) capital $d(\lambda) = 1$. Then, in round m, depending on the first m outcomes $w = A\restriction m$, following a betting strategy $b(w) = (\alpha_w, i_w)$ he bets a certain fraction $\alpha_w d(w)$ ($\alpha_w \in [0,1]$) of his current capital $d(w)$ on the event $A(m) = i_w$. If he guessed the outcome correctly, i.e. $A(m) = i_w$, his stake is doubled, otherwise it is lost. The martingale $d_b(w)$ induced by b will then describe the capital of the gambler in the course of this game. If this capital grows unboundedly, the gambler wins.

Note that fairness of the game underlying Definition 1 is reflected by the *fairness condition* for martingales,

$$d(w) = \frac{d(w0) + d(w1)}{2}. \qquad (3)$$

It has been shown that a class $\mathcal{C}$ has Lebesgue measure 0, $\mu(\mathcal{C}) = 0$, if some martingale succeeds on $\mathcal{C}$. By imposing resource bounds, martingales can be used for defining resource-bounded measure concepts. For recent surveys on this area see [12] and [1].

Definition 2 *Let $t : \mathbb{N} \to \mathbb{N}$ be a recursive function. A $t(m)$*-betting strategy *is a rational valued betting strategy b such that $b(w)$ can be computed in $\mathrm{O}(t(|w|))$ steps for all strings w. A $t(m)$*-martingale *d is a martingale induced by a $t(m)$-betting strategy.*

A p-martingale *d is a $q(m)$-martingale for some polynomial q. A class $\mathcal{C}$ has* p-measure 0, *$\mu_{\mathrm{p}}(\mathcal{C}) = 0$ for short, if some p-martingale succeeds on $\mathcal{C}$ and $\mu_{\mathrm{p}}(\mathcal{C}) = 1$ if $\mu_{\mathrm{p}}(\overline{\mathcal{C}}) = 0$. A class $\mathcal{C}$ has* measure 0 in E, *$\mu(\mathcal{C}|\,\mathrm{E}) = 0$, if $\mu_{\mathrm{p}}(\mathcal{C} \cap \mathrm{E}) = 0$ and $\mathcal{C}$ has* measure 1 in E, *$\mu(\mathcal{C}|\,\mathrm{E}) = 1$, if $\mu_{\mathrm{p}}(\mathrm{E} \setminus \mathcal{C}) = 0$.*

In order to obtain a description of Hausdorff dimension in terms of martingales, we do not just ask *whether* a martingale succeeds on a set A, but also *how fast* the capital increases.

Definition 3 *For a real number $s \geq 0$, a martingale d is* s-successful on a set $A \in \{0,1\}^{\mathbb{N}}$ *if*

$$\limsup_{m\to\infty} \frac{d(A{\restriction}m)}{2^{(1-s)m}} = \infty. \tag{4}$$

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

If appropriate, we extend notation introduced for betting strategies to the corresponding martingales and vice versa. For example, we say a betting strategy is s-successful on some class if the corresponding martingale is. It is clear from the definition that if for a class $\mathcal{C}$ there exists a martingale d that is s-successful on $\mathcal{C}$ for some $s \leq 1$, then $\mathcal{C}$ has Lebesgue measure 0. Furthermore, for every $\varepsilon > 0$, the martingale that never makes a bet $(1+\varepsilon)$-succeeds on all sets, whence, by the following proposition, no class has dimension greater than 1.

Theorem 4 [LUTZ] *For any class $\mathcal{C}$, the Hausdorff dimension of $\mathcal{C}$ is the infimum of all real numbers s such that there is a betting strategy which s-succeeds on $\mathcal{C}$.*

In [13], after proving a similar result for s-gales (a generalization of martingales, see Section 5 below) LUTZ, exploits the characterization of classical Hausdorff dimension in terms of betting games in order to define a resource-bounded version of this concept.

Definition 5 *Let $\mathcal{C}$ be a class and t be a computable function. The* $t(m)$-dimension *of $\mathcal{C}$ is the infimum of all real numbers s such that there is a $t(m)$-betting strategy that is s-successful on $\mathcal{C}$. The* p-dimension *of $\mathcal{C}$, written* $\dim_{\mathrm{p}}(\mathcal{C})$, *is the infimum of all s such that there is a p-betting strategy that is s-successful on $\mathcal{C}$. The* dimension of $\mathcal{C}$ in E, *written* $\dim(\mathcal{C}|\mathrm{E})$, *is the p-dimension of $\mathcal{C} \cap \mathrm{E}$.*

LUTZ [13] established some basic properties of p-dimension that show that this concept is reasonable and might prove useful for investigating the structure of the class E. He showed that every slice $\mathrm{DTIME}(2^{kn})$ of E has p-dimension 0 while E itself has p-dimension 1. Moreover, for all classes $\mathcal{C}$ and $\mathcal{D}$

$$\dim_{\mathrm{p}}(\mathcal{C} \cup \mathcal{D}) = \max\{\dim_{\mathrm{p}}(\mathcal{C}), \dim_{\mathrm{p}}(\mathcal{D})\} \tag{5}$$

and in fact the latter assertion extends – with $\max$ replaced by $\sup$ – to unions of countably many classes that have an appropriate uniform representation.

For *constructive* dimension (defined via lower semicomputable martingales), LUTZ used the fact that there exist *universal* lower semicomputable martingales to show that the constructive dimension of a class is the supremum of the constructive dimension of its members, viewed as singleton classes (see [14], Lemma 4.5). Since there are no universal p-martingales, this observation has no exact counterpart for p-dimension. Still, using the fact that, for any number k, there is a p-martingale that is universal for the class of m^k-martingales, we obtain a result of similar flavor which will serve as a useful tool in our investigation of p-dimension.

Proposition 6 *For any class $\mathcal{C}$,*

$$\dim_{\mathrm{p}}(\mathcal{C}) \;=\; \inf_{k\geq 1}\, \sup_{A\in\mathcal{C}}\, \dim_{m^k}(\{A\}). \tag{6}$$

We conclude this section with another useful technical lemma, which shows that in the definition of p-dimension it suffices to consider betting strategies that are restricted to a finite set of non-zero betting ratios. Among other applications, we will use this fact in Section 5 in order to characterize the classes that have p-dimension less than 1.

Definition 7 *The* set of weights *of a betting strategy b is*

$$\mathrm{W}_b = \{\alpha : \, (\exists w, i)\, [b(w) = (\alpha, i)]\}.$$

A betting strategy b is simple *if W_b is a finite set of rational numbers, and b is* strict *if $0 \notin \mathrm{W}_b$.*

Lemma 8 *Let $k \geq 2$ and $s \in [0,1]$ and assume that the class $\mathcal{C}$ has m^k-dimension s. Then for any $\varepsilon > 0$ there is a strict and simple m^k-betting strategy b that $(s+\varepsilon)$-succeeds on $\mathcal{C}$.*

Proof. Fix a rational $\varepsilon > 0$. By assumption, there is an m^k-betting strategy b_0 that $(s+\varepsilon/2)$-succeeds on $\mathcal{C}$. Let $\tau = 2^{\varepsilon/2}$ and fix rationals $\gamma_1, \ldots, \gamma_{l+1}$ such that

$$\gamma_1 = 1 - (1/\tau) < \gamma_2 < \ldots < \gamma_{l+1} = 1$$

and $\gamma_{j+1} < \tau(1+\gamma_j) - 1$ for $j = 1, \ldots, l$. Next define a betting strategy b that basically works like b_0 except that on a string w with $b_0(w) = (\alpha_w, i)$ the betting ratio α_w is adjusted to some γ_j according to

$$b(w) \quad = \quad \begin{cases} (\gamma_1, i) & \text{if } \alpha_w \leq \gamma_1 \\ (\gamma_j, i) & \text{if } \gamma_j < \alpha_w \leq \gamma_{j+1} \end{cases}$$

Then a simple case analysis shows that on any single bet the gain of b_0 exceeds the gain of b by at most a factor of τ. Thus, for any A and m,

$$\begin{aligned} \frac{d_b(A \restriction m)}{2^{(1-(s+\varepsilon))m}} &\geq \frac{\tau^{-m} d_{b_0}(A \restriction m)}{2^{(1-(s+\varepsilon))m}} \\ &= \frac{2^{-\frac{\varepsilon}{2}m} d_{b_0}(A \restriction m)}{2^{(1-(s+\varepsilon))m}} = \frac{d_{b_0}(A \restriction m)}{2^{(1-(s+\frac{\varepsilon}{2}))m}}. \end{aligned} \tag{7}$$

Hence b $(s+\varepsilon)$-succeeds on $\mathcal{C}$ since by choice of b_0, for any set A in $\mathcal{C}$, the rightmost term in (7) is unbounded in m. □

3. The Dimension of Upper and Lower Spans

In this section we will begin the investigation of the dimension of upper and lower p-m-spans of sets in E. Our main result here will be that, for any set A, the p-m-degree and the lower p-m-span of A have the same p-dimension. To show this we will first prove a general invariance theorem for p-dimension. Some further applications of this theorem will be given at the end of this section. Before stating our invariance theorem we have to introduce some notation.

Definition 9 *For any set D, let*

$$\mathrm{cens}_D(m) = |\{j \in D : j \leq m\}|$$

be the census function *of D and say that D has* sublinear density *if* $\mathrm{cens}_D(m)$ *is in* $\mathrm{o}(m)$*. Furthermore, let*

$$\mathrm{z}_i^D = \min\{m \in \mathbb{N} : \mathrm{cens}_D(m) = i\}$$

be the $(i+1)$*th element of D. The* D-join $(A \oplus_D B)$ *of sets A and B is defined by*

$$(A \oplus_D B)(\mathrm{z}_i^{\bar{D}}) = A(i) \qquad \text{and} \qquad (A \oplus_D B)(\mathrm{z}_i^D) = B(i),$$

i.e., for all i, $A(i)$ *and* $B(i)$ *are coded into the* $(i+1)$*th element of the complement of D and of D, respectively.*

Definition 10 *The class* $\mathcal{C}_1$ contains a stretched version of *the class* $\mathcal{C}_0$ *if there is a number* $k \in \mathbb{N}$ *such that for every* $C \in \mathcal{C}_0$ *there are sets D and H computable in time* $\mathrm{O}(2^{kn})$ *where D has sublinear density and* $(C \oplus_D H) \in \mathcal{C}_1$*. The classes* $\mathcal{C}_0$ *and* $\mathcal{C}_1$ *are* close *if for* $i = 0, 1$*, the class* $\mathcal{C}_i$ *contains a stretched version of* $\mathcal{C}_{1-i}$*.*

Theorem 11 *Let* $\mathcal{C}_0, \mathcal{C}_1$ *be classes such that* $\mathcal{C}_1$ *contains a stretched version of* $\mathcal{C}_0$*. Then* $\dim_{\mathrm{p}}(\mathcal{C}_1) \geq \dim_{\mathrm{p}}(\mathcal{C}_0)$ *and* $\dim(\mathcal{C}_1|\mathrm{E}) \geq \dim(\mathcal{C}_0|\mathrm{E})$*. Hence, in particular, any two close classes have identical p-dimension, as well as identical dimension in* E*.*

Proof. As one can easily show, for any class $\mathcal{C}_1$ that contains a stretched version of a class $\mathcal{C}_0$, the intersection $\mathcal{C}_1 \cap \mathrm{E}$ of $\mathcal{C}_1$ with E contains a stretched version of $\mathcal{C}_0 \cap \mathrm{E}$. Hence it suffices to prove the assertion on p-dimension. Let $s_i = \dim_{\mathrm{p}}(\mathcal{C}_i)$. We show that $s_1 \geq s_0$. By Proposition 6, it suffices to show that for any rational $t > s_1$ there is a number $k \in \mathbb{N}$ such that every set $C_0 \in \mathcal{C}_0$ has m^k-dimension at most t.

So fix such a t. Pick s with $s_1 < s < t$ and let b_1 be a p-betting strategy that s-succeeds on every set in $\mathcal{C}_1$. Then for every $C_1 \in \mathcal{C}_1$, there are infinitely many numbers m such that

$$d_{b_1}(C_1 \upharpoonright m) \; > \; 2^{(1-s)m}. \tag{8}$$

Next fix a number k_0 that witnesses that $\mathcal{C}_1$ contains a stretched version of $\mathcal{C}_0$, let k_1 be such that b_1 is an m^{k_1}-betting strategy, and let $k = \max(k_0, k_1) + 1$. Finally, let C_0 be any set in $\mathcal{C}_0$. Then it suffices to show that there is an m^k-betting strategy b_0 that t-succeeds on C_0.

By choice of k_0 choose sets D and H computable in time $\mathrm{O}(2^{k_0 n})$ such that D has sublinear density and $(C_0 \oplus_D H)$ is in $\mathcal{C}_1$, and define a betting strategy b_0 by

$$b_0(X \upharpoonright m) \; = \; b_1((X \oplus_D H) \upharpoonright \mathrm{z}_m^{\bar{D}}). \tag{9}$$

Roughly speaking, b_0 mimics the bets of b_1 but b_0 skips all bets on elements of D. The bet of b_0 on $X(m)$ corresponds to the bet of b_1 on place $\mathrm{z}_m^{\bar{D}}$ of $(X \oplus_D H)$, i.e., to the bet of b_1 on the element of $\bar{D}$ at which $X(m)$ has been coded into $(X \oplus_D H)$.

To show that the betting strategy b_0 has the required properties, we first show that b_0 t-succeeds on C_0. Let $\varepsilon = t - s > 0$. By sublinear density of D fix m_0 such that, for all $m > m_0$, there are less than εm elements of D that are smaller than m. Moreover, for $m \geq \min \bar{D}$ let m' be the greatest number in $\{i < m : i \notin D\}$. Then while betting on $C_0(0)$ through $C_0(m')$, b_0 gains up to a factor of at most $2^{\varepsilon m}$ the same capital as b_1 gains by betting on $(C_0 \oplus_D H)(0)$ through $(C_0 \oplus_D H)(m)$. Thus, by choice of ε, for every $m > m_0$ that satisfies (8) for $C_1 = (C_0 \oplus_D H)$ we obtain

$$\begin{aligned} d_{b_0}(C_0 \upharpoonright m') \;&\geq\; 2^{-\varepsilon m} d_{b_1}((C_0 \oplus_D H) \upharpoonright m) \\ &\geq\; 2^{(1-s-\varepsilon)m} = 2^{(1-t)m} > 2^{(1-t)m'}. \end{aligned}$$

Since there are infinitely many such numbers m', b_0 t-succeeds on C_0.

It remains to show that b_0 is an m^k-betting strategy. In order to compute $b_0(X \upharpoonright m)$, we first compute $\mathrm{z}_m^{\bar{D}}$ and $w_m = (X \oplus_D H) \upharpoonright \mathrm{z}_m^{\bar{D}}$. By sublinear density of D, $|w_m|$ is at most $2m$ for almost all m. Hence w_m can be computed by successively computing for $i = 0, \ldots, 2m$ the values $\mathrm{cens}_D(i)$, $\mathrm{cens}_{\bar{D}}(i)$, and, in case of $i = \mathrm{z}_j^{\bar{D}}$, the value $H(j)$. Hence, except for updating some counters and some other negligible computations, it suffices to evaluate D and H for all arguments up to $2m$. Since these sets are computable in time $\mathrm{O}(2^{k_0 n})$, this can be done in time $\mathrm{O}(4m 2^{k_0|2m|})$ and hence in time $\mathrm{O}(m^{k_0+1})$. Finally, we have to compute $b_1(w_m)$. Since b_1 is an m^{k_1}-betting strategy and since $|w_m| \leq 2m$ this can be done in $\mathrm{O}(m^{k_1})$ steps, hence the total time required for computing $b_1(X \upharpoonright m)$ is bounded by $\mathrm{O}(m^{\max(k_0+1,k_1)})$. So b_1 is an m^k-betting strategy by choice of k. □

Corollary 12 *Let A be in* E*. Then the lower p-m-span of A and the p-m-degree of A have the same p-dimension, as well as the same dimension in* E*.*

Proof. By Theorem 11, we are done if we can show that the lower p-m-span and the p-m-degree of A are close. As the latter class is contained in the former one, it suffices to show that the p-m-degree of A contains a stretched version of the lower p-m-span of A. So let $D = \{0^{|y|}y : y \in \mathbb{N}\}$ and – by $A \in \mathrm{E}$ – fix a set $\widetilde{A}$ in the p-m-degree of A that is computable in time $\mathrm{O}(2^n)$. Then D has sublinear density and for every set $X \leq_{\mathrm{m}}^{\mathrm{P}} A$, the set $(X \oplus_D \widetilde{A})$ is in the p-m-degree of A. □

In Corollary 12 we can replace p-m-reducibility by most of the common resource-bounded reducibilities. Corollary 12 implies that the p-dimension of the degree of a set is growing with the relative complexity of the set.

Corollary 13 *Let A, B be sets in* E *with $A \leq_{\mathrm{m}}^{\mathrm{P}} B$. Then*

$$\dim_{\mathrm{p}}(\deg_{\mathrm{m}}^{\mathrm{P}}(A)) \leq \dim_{\mathrm{p}}(\deg_{\mathrm{m}}^{\mathrm{P}}(B))$$

and

$$\dim(\deg_{\mathrm{m}}^{\mathrm{P}}(A)|\mathrm{E}) \leq \dim(\deg_{\mathrm{m}}^{\mathrm{P}}(B)|\mathrm{E}).$$

Other interesting consequences of Corollary 12 include the following.

Corollary 14 *(a) The class of p-m-complete sets for* E *has dimension* 1 *in* E.

(b) The upper p-m-span of any set in E *has dimension* 1 *in* E.

(c) The class of p-m-complete sets for NP *has the same dimension in* E *as* NP.

MAYORDOMO [15] has shown that the class of p-m-complete sets has measure 0 in E, hence this class is an interesting example of a measure-0-class in E that has dimension 1 in E. MAYORDOMO's result was extended by JUEDES and LUTZ [9] who have shown that for any set $A \in \mathrm{E}$, the lower p-m-span of A or the upper p-m-span of A has measure 0 in E. Corollary 14 shows that this small-span theorem fails with measure replaced by dimension.

We conclude this section by giving two more examples of dimension 1 results that can be derived from Theorem 11. First we show that the property of p-immunity yields a partition of E into four classes each having dimension 1 in E.

Corollary 15 *The following classes have dimension* 1 *in* E.

$$\begin{aligned}
\mathcal{C}_1 &= \{A : A \textit{ is p-immune and } \bar{A} \textit{ is p-immune}\},\\
\mathcal{C}_2 &= \{A : A \textit{ is p-immune and } \bar{A} \textit{ is not p-immune}\},\\
\mathcal{C}_3 &= \{A : A \textit{ is not p-immune and } \bar{A} \textit{ is p-immune}\},\\
\mathcal{C}_4 &= \{A : A \textit{ is not p-immune and } \bar{A} \textit{ is not p-immune}\}.
\end{aligned}$$

Proof. MAYORDOMO [15] has shown that $\mathcal{C}_1$ has measure 1 in E, hence dimension 1 in E. To show that $\mathcal{C}_2$, $\mathcal{C}_3$, and $\mathcal{C}_4$ have dimension 1 in E, too, it suffices to show that these classes contain stretched versions of $\mathcal{C}_1$. But this is witnessed by the pairs (D, H_i), $i = 1, 2, 3$, where $D = \{0^{|y|}y : y \in \mathbb{N}\}$ and H_i is any infinite and coinfinite set in $\mathcal{C}_i$ that is computable in time $\mathrm{O}(2^n)$. □

Recall that for any reducibility r, a set A is r-autoreducible if there is an r-reduction from A to itself that does not allow to query the oracle on the input. The measure of the p-T-autoreducible sets in E is not known (see [5]). For more restrictive reducibilities, however, the class of autoreducible sets has measure 0 in E. Examples are the classes of the p-m-autoreducible sets and of the sets that are p-T-autoreducible via order-decreasing reductions, i.e., by reductions that on input x can only query their oracle at places $y < x$. Dimension in E allows us to distinguish the size of these two measure-0-classes in E.

Corollary 16 *The class of p-m-autoreducible sets has dimension* 1 *in* E *while the class of sets that are p-T-autoreducible via order-decreasing reductions has dimension* 0 *in* E.

Proof. To show that the class of the p-m-autoreducible sets has dimension 1, we show that this class contains a stretched version of E. Given any set $X \in \mathrm{E}$, let $D = \{0^{|y|}y : y \in \mathbb{N}\}$ and let $\widetilde{X}$ be any set in $\mathrm{DTIME}(2^n)$ that is p-m-equivalent to X. Then the set $X \oplus_D \widetilde{X}$ is p-m-autoreducible.

On the other hand, to show that the class of sets that are p-T-autoreducible via order-decreasing reductions has dimension 0 in E, fix a set A in E and a polynomially time-bounded oracle Turing machine M such that $A(x) = M^{A \upharpoonright x}(x)$ for all x. By Proposition 6 it suffices to define an m^2-betting strategy b that s-succeeds on A for all $s > 0$. As one can easily check, the strategy b defined by $b(X \upharpoonright m) = (1, M^{X \upharpoonright m}(m))$ will do. □

4. Lower spans of intermediate dimension in E

In this section we continue the investigation of the dimension of the lower p-m-spans of sets in E by discussing the question of which dimensions can occur for such spans. Trivially, the dimension in E of the lower p-m-span of a set is 0 if the set is computable in polynomial time and is 1 if the set is p-m-complete. For resource-bounded measure there are lower p-m-spans that have neither measure 0 nor measure 1 in E (see LUTZ [11]). LUTZ calls a set *weakly complete* if its lower p-m-span does not have measure 0 because one can reduce to any such set a nonnegligible part of E. In particular, a weakly complete set is intractable, i.e., is not in P. For the latter, however, it suffices that the lower p-m-span does not have *dimension* 0 in E. We call a set with this property *partially complete*. Obviously, every weakly complete set is partially complete. As we show below, however, the converse fails. In fact there is a large variety of partially complete sets that are not weakly complete. For any rational number $\beta \in (0,1)$ there is a set A in E such that the lower p-m-span of A has dimension $\mathcal{H}(\beta)$ in E. Here the function

$$\mathcal{H}(\beta) = \beta \log(1/\beta) \; + \; (1-\beta)\log(1/(1-\beta)) \qquad (10)$$

is the binary entropy function and its range is dense in the interval $(0,1)$.

In fact we will show that for any m^2-β-random set R_β in E, the lower p-m-span of R_β has dimension $\mathcal{H}(\beta)$ in E. This result was motivated by the the observation of AMBOS-SPIES, TERWIJN, and ZHENG [3] that a set A is weakly complete if the lower p-m-span of A contains an m^2-random set $R \in \mathrm{E}$, and by the more recent result by LUTZ [14] that any constructively β-random set has constructive dimension $\mathcal{H}(\beta)$. We first review the definition of m^k-β-random sets.

Definition 17 *Let β be a rational number in $(0,1)$. A set R is* m^k-β-random *if no m^k-betting strategy b succeeds on R under the modified payoff function d_b^β where for $b(w) = (\alpha_w, i_w)$ and $\mu_\beta(1) = \beta$ and $\mu_\beta(0) = 1-\beta$ we have*

$$d_b(wi_w) = d_b(w)(1 + \alpha_w \frac{\mu_\beta(1-i_w)}{\mu_\beta(i_w)}) \qquad (11)$$

and

$$d_b(w(1-i_w)) = d_b(w)(1-\alpha_w). \qquad (12)$$

Note that for $\beta = 1/2$, the payoff function (11) coincides with the usual payoff function from (1). Hence the m^k-$1/2$-random sets are just the m^k-random sets.

Lemma 18 *For any natural number $k \geq 2$ and for any rational number $\beta \in (0,1)$, there is an m^2-β-random set in E.*

An m^2-β-random set as in Lemma 18 can be constructed by a standard construction that diagonalizes against an appropriately weighted sum of all m^2-betting strategies. We omit the details of the proof. Now our result can be stated as follows.

Theorem 19 *Let R be an m^2-β-random set in E for some rational $\beta \in (0,1)$. Then the lower p-m-span of R has p-dimension and dimension in E equal to $\mathcal{H}(\beta)$.*

Using Corollary 12 and Lemma 18, Theorem 19 implies the following corollary.

Corollary 20 *For any rational number $\beta \in (0,1)$, there is a set A in E such that*

$$\dim_{\mathrm{p}}(\mathrm{span}_{\mathrm{m}}^{\mathrm{P}}(A)) \; = \; \dim_{\mathrm{p}}(\deg_{\mathrm{m}}^{\mathrm{P}}(A)) \; = \; \mathcal{H}(\beta). \qquad (13)$$

The assertion remains valid if we replace in (13) *p-dimension by dimension in* E.

Using bias sequences of rational numbers, the third author shows that Corollary 20 can be extended from rational to Δ_2^0-computable real numbers. As the Δ_2^0-computable real numbers are closed under taking logarithms, and the function $\mathcal{H}$ is a surjective, continous mapping of the unit interval to itself, this yields the existence of lower spans of arbitrary Δ_2^0-computable dimension, including lower spans of rational dimension.

The proof of Theorem 19 is based on the following three lemmas.

Lemma 21 *Let β be a rational in $(0,1)$ and let the set R be m^k-β-random for some $k \geq 2$. Then $\dim_{m^k}(\{R\}) \geq \mathcal{H}(\beta)$.*

Lemma 22 *Let β be a rational in $(0,1)$ and let R be an m^2-β-random set in* E*. Then for any $k \geq 2$, there is an m^k-β-random set R_k in* E *that is p-m-reducible to R.*

Lemma 23 *Let β be a rational in $(0,1)$ and let R be an m^2-β-random set in* E*. There is a number $k \in \mathbb{N}$ such that $\dim_{m^k}(\{A\}) \leq \mathcal{H}(\beta)$ for any set A that is p-m-reducible to R.*

Note that Lemmas 21 and 22 imply that $\dim(\mathrm{span}_{\mathrm{m}}^{\mathrm{P}}(R)|\mathrm{E}) \geq \mathcal{H}(\beta)$ while, by Lemma 23 and Proposition 6, $\mathcal{H}(\beta) \geq \dim_{\mathrm{p}}(\mathrm{span}_{\mathrm{m}}^{\mathrm{P}}(R))$.

Now Theorem 19 follows, since for any set R, $\dim_{\mathrm{p}}(\mathrm{span}_{\mathrm{m}}^{\mathrm{P}}(R)) \geq \dim(\mathrm{span}_{\mathrm{m}}^{\mathrm{P}}(R)|\mathrm{E})$. We omit the proofs of Lemmas 21 through 23. Lemma 21 is a resource-bounded version of LUTZ's result on the constructive dimension of constructively β-random sets [14], while Lemma 22 extends an observation of AMBOS-SPIES, TERWIJN and ZHENG [3] on m^2-random sets.

We conclude this section with some remarks on the notion of partial completeness.

Definition 24 *A set A is* partially complete for E *if $A \in \mathrm{E}$ and*

$$\dim(\mathrm{span}_{\mathrm{m}}^{\mathrm{P}}(A)|\mathrm{E}) > 0.$$

The following implications hold, from left to right, because E does not have measure 0 in E, because any class of measure in E different from 0 has dimension 1 in E, and finally because the class P has dimension 0 in E.

$$A \text{ complete } \Rightarrow A \text{ weakly complete } \Rightarrow A \text{ partially complete } \Rightarrow A \text{ intractable} \qquad (14)$$

In fact, all three implications in (14) are proper. For the first implication this has been shown by Lutz [11]. Concerning the third one, it suffices to observe that there are tally sets in $\mathrm{E} \setminus \mathrm{P}$ whereas the lower p-m-span of any tally set is easily shown to have p-dimension 0. The strictness of the second implication follows from Theorem 19.

Corollary 25 *There is a set that is partially but not weakly complete for* E.

Proof. Fix a rational $\beta \neq 1/2$ in $(0, 1)$. Observe that $\mathcal{H}(\beta)$ differs from 0 and 1. Thus by Theorem 19 the lower p-m-span of any m^2-β-random set in E has dimension $\mathcal{H}(\beta) \notin \{0, 1\}$ and hence, in particular, has measure 0 in E. □

5. Alternative Characterizations of Resource-Bounded Dimension

In this final section we shortly discuss (without giving proofs) some alternative characterizations of resource-bounded dimension. First we review definitions of dimension that have been given by LUTZ and STAIGER and relate them to our definition in Section 2. LUTZ [13] introduced *gales* as a generalization of martingales, by modifying the fairness condition (3).

Definition 26 *For $s \in \mathbb{R}_0^+$, an s-*gale *is a function g mapping strings to nonnegative integers satisfying*

$$g(w) = \frac{g(w0) + g(w1)}{2^s} \qquad \text{for all } w \in \{0,1\}^*. \quad (15)$$

For gales the notion of *success* is defined in the same way as for martingales (which are, of course, 1-gales). STAIGER [21, 22] observed the close relation between martingales and Hausdorff dimension, too. He defined a parameter $\lambda_d(A)$, the *exponent of the increase* of a martingale d on a set A, by

$$\lambda_d(A) = \limsup_{m \to \infty} \frac{\log(d(A \restriction m))}{m}.$$

As the following proposition shows, s-succeeding martingales, LUTZ' s-gales, and the exponent of increase defined by STAIGER all yield the same concept of dimension.

Proposition 27 *For any class $\mathcal{C}$ and any rational number $s > 0$, the following conditions are equivalent:*

(a) $s > \dim_H(\mathcal{C})$.

(b) There is an s-gale succeeding on $\mathcal{C}$.

(c) There is a martingale d with $\lambda_d(A) \geq 1 - s$ for all $A \in \mathcal{C}$.

The equivalence remains valid if we restrict all statements either to computable or to polynomial-time computable martingales and gales.

In the remainder of this section we characterize the classes of p-dimension less than 1 in terms of p-martingales with restricted sets of betting ratios and in terms of p-prediction functions. These characterizations are related to previous results of SCHNORR on computable martingales (in particular Theorems 14.5 and 18.4 in [19]) and to characterizations of resource-bounded stochasticity notions in terms of simple martingales by AMBOS-SPIES, MAYORDOMO, WANG and ZHENG [2].

The first approach to randomness due to VON MISES, which is now commonly called stochasticity, can be described in terms of (partial) prediction functions (see e.g. [2] for details). The special case of a total p-prediction function and a corresponding concept of predictability are defined as follows.

Definition 28 *A (total)* p-prediction function *is a function $f : \{0,1\}^* \to \{0,1\}$ such that f can be computed in polynomial time. The function f* predicts *a set A if there is an $\varepsilon > 0$ such that for infinitely many numbers m*

$$\frac{|\{m' < m : \ f(A \restriction m') = A(m')\}|}{|\{m' < m : \ f(A \restriction m') \neq A(m')\}|} > 1 + \varepsilon. \quad (16)$$

A set A is p-predictable *if there is a p-prediction function that predicts A, and a class $\mathcal{C}$ is* p-predictable *if there is a p-prediction function predicting every set in $\mathcal{C}$.*

KO [10] proposed p-unpredictability as a formalization of polynomial time randomness. In [2], where p-unpredictable sets are called Ko-p-stochastic, it was shown that these sets are just the sets on which strict and simple p-martingales cannot succeed. The following theorem which in part parallels the latter observation reveals some fundamental relations between p-dimension and p-predictability.

Theorem 29 *Let $\mathcal{C}$ be a class. Then the following are equivalent.*

(a) The class $\mathcal{C}$ has p-dimension less than 1.

(b) There is a strict and simple p-betting strategy that succeeds on $\mathcal{C}$.

(c) There is a rational number ε and a strict p-betting strategy b that succeeds on $\mathcal{C}$ such b succeeds on $\mathcal{C}$ and $\alpha \geq \varepsilon$ for all weights α of b.

(d) $\mathcal{C}$ is the union of finitely many p-predictable classes.

Note that the implication (a)⇒(b) follows from Lemma 8. There is a similar characterization of the classes of p-dimension 0.

Theorem 30 *Let $\mathcal{C}$ be a class. Then the following are equivalent.*

(a) The class $\mathcal{C}$ has p-dimension 0.

(b) For every rational number $\varepsilon \in (0, 1)$ there is a strict p-betting strategy b such that b succeeds on $\mathcal{C}$ and ε is the only weight of b.

(c) For every rational number $\varepsilon \in (0, 1)$ there is a strict p-betting strategy b such that b succeeds on $\mathcal{C}$ and $\alpha \geq \varepsilon$ for all weights α of b.

Note, however, that there is no one-one correspondence between p-dimension and highest possible minimum betting weight, for one can construct classes with identical allowable betting weight but distinct p-dimensions.

References

[1] K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In A. Sorbi, editor, *Complexity, logic, and recursion theory*, pages 1–47. Marcel Dekker, 1997.

[2] K. Ambos-Spies, E. Mayordomo, Y. Wang, and X. Zheng. Resource-bounded balanced genericity, stochasticity and weak randomness. In C. Puech and R. Reischuk, editors, *STACS 1996, 13th Annual Symposium on Theoretical Aspects of Computer Science, Grenoble, France*, pages 63–74. Springer, 1996.

[3] K. Ambos-Spies, S. A. Terwijn, and X. Zheng. Resource bounded randomness and weakly complete problems. *Theor. Comput. Sci.*, 172(1-2):195–207, 1997.

[4] P. Billingsley. *Ergodic theory and information*. Wiley, 1965.

[5] H. Buhrman, D. van Melkebeek, K. W. Regan, D. Sivakumar, and M. Strauss. A generalization of resource-bounded measure, with application to the BPP vs. EXP Problem. *SIAM J. Comput.*, 30(2):576–601, 2000.

[6] J.-Y. Cai and J. Hartmanis. On Hausdorff and topological dimensions of the Kolmogorov complexity of the real line. *J. Comput. Syst. Sci.*, 49(3):605–619, 1994.

[7] K. Falconer. *Fractal geometry: mathematical foundations and applications.* Wiley, 1990.

[8] F. Hausdorff. Dimension und äußeres Maß. *Math. Ann.*, 79:157–179, 1919.

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

[10] K.-I. Ko. On the notion of infinite pseudorandom sequences. *Theor. Comput. Sci.*, 48(1):9–33, 1986.

[11] J. H. Lutz. Weakly hard problems. *SIAM J. Comput.*, 24(6):1170–1189, 1995.

[12] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra, editor, *Complexity theory retrospective II*, pages 225–260. Springer, 1997.

[13] J. H. Lutz. Dimension in complexity classes. In *Proceedings of the Fifteenth Annual IEEE Conference on Computational Complexity*, pages 158–169. IEEE Computer Society, 2000.

[14] J. H. Lutz. Gales and the constructive dimension of individual sequences. In U. Montanari, J. D. P. Rolim, and E. Welzl, editors, *Proceedings of the Twenty-Seventh International Colloquium on Automata, Languages, and Programming*, pages 902–913. Springer, 2000.

[15] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theor. Comput. Sci.*, 136(2):487–506, 1994.

[16] B. Y. Ryabko. Noiseless coding of combinatorial sources, Hausdorff dimension, and Kolmogorov complexity. *Probl. Inf. Transm.*, 22:170–179, 1986.

[17] B. Y. Ryabko. Algorithmic approach to the prediction problem. *Probl. Inf. Transm.*, 29(2):186–193, 1993.

[18] B. Y. Ryabko. The complexity and effectiveness of prediction algorithms. *J. Complexity*, 10(3):281–295, 1994.

[19] C. P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie.* Springer, 1971.

[20] L. Staiger. Kolmogorov complexity and Hausdorff dimension. *Inf. Comput.*, 103(2):159–194, 1993.

[21] L. Staiger. A tight upper bound on Kolmogorov complexity and uniformly optimal prediction. *Theory Comput. Syst.*, 31(3):215–229, 1998.

[22] L. Staiger. How much can you win when your adversary is handicapped? In I. Althoefer, N. Cai, G. Dueck, L. Khachatrian, M. S. Pinsker, A. Sarkoezy, I. Wegener, and Z. Zhang, editors, *Numbers, information and complexity*, pages 403–412. Kluwer, 2000.