Electronic Colloquium on Computational Complexity, Report No. 29 (2004)

Scaled dimension and the Kolmogorov complexity of Turing hard sets*

John M. Hitchcock†, María López-Valdés‡, and Elvira Mayordomo‡

Abstract

Scaled dimension has been introduced by Hitchcock et al (2003) in order to quantitatively distinguish among classes such as SIZE($2^{\alpha n}$) and SIZE(2^{n^α}) that have trivial dimension and measure in ESPACE.

This paper gives an exact characterization of effective scaled dimension in terms of resource-bounded Kolmogorov complexity. We can now view each result on the scaled dimension of a class of languages as upper and lower bounds on the Kolmogorov complexity of the languages in the class.

We prove a Small Span Theorem for Turing reductions that implies the class of $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard sets for ESPACE has $(-3)^{\mathrm{rd}}$-pspace dimension 0.

As a consequence we have a nontrivial upper bound on the Kolmogorov complexity of all hard sets for ESPACE for this very general nonuniform reduction, $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$. This is, to our knowledge, the first such bound. We also show that this upper bound does not hold for most decidable languages, so $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard languages are unusually simple.

1 Introduction

The relationship between uniform and nonuniform complexity measures is one of the main sources of open problems in computational complexity. In this context it is very informative to quantify the difference in size of nonuniform and uniform complexity classes and this has been possible so far for space-bounded complexity classes. Lutz started in [20] by showing that the Boolean circuit-size complexity class SIZE($\frac{2^n}{n}$) has measure 0 in

*This research was supported in part by Spanish Government MEC project TIC 2002-04019-C03-03

†Department of Computer Science, University of Wyoming, USA. jhitchco@cs.uwyo.edu Part of this research was done while this author was visiting the Universidad de Zaragoza

‡Departamento de Informática e Ingeniería de Sistemas, María de Luna 1, Universidad de Zaragoza, 50018 Zaragoza, SPAIN. marlopez@unizar.es, elvira@unizar.es

ISSN 1433-8092

ESPACE (linear exponential space). In 2000, Lutz [21] defined resource-bounded dimension as an effectivization of Hausdorff dimension, and he further refined his previous result by proving that SIZE($\alpha\frac{2^n}{n}$) has dimension α in ESPACE, for each $\alpha \in [0, 1]$.

But classes such as SIZE($2^{\alpha n}$) or SIZE (2^{n^α}) resisted the dimension approach because they had trivial dimensions, and in 2003 the definition of scaled dimension [9] made it possible to precisely quantify the difference between those circuit-size classes. Several results on scaled dimension of other classes have also been proven [9, 8].

In this paper we explore the interpretation of space-bounded scaled dimension as an information content measure. Space-bounded Kolmogorov complexity has been investigated extensively [15, 6, 22, 16, 19, 4, 12]. Roughly speaking, for $A \subseteq \{0,1\}^*$, $m \in \mathbb{N}$ and space bound t, the space-bounded Kolmogorov complexity $KS^t(A[0 \ldots m-1])$ is the length of the shortest program that prints the m-bit prefix of characteristic sequence of A using at most t units of workspace. In this setting $KS^t(A[0 \ldots m-1])$ is the amount of information of $A[0 \ldots m-1]$ that is accessible by a t-bounded space computation.

Here we obtain an exact characterization of space-bounded scaled dimension in terms of space-bounded Kolmogorov complexity for the cases where such a characterization is possible. For example, the $(-1)^{\text{st}}$-scaled pspace-dimension of a class X is the minimum s for which there is a c such that for every $A \in X$,

$$KS^{m^c}(A[0 \ldots m-1]) \leq m - m^{1-s} \text{ i.o. } m$$

Equivalently, $(-1)^{\text{st}}$-scaled pspace-dimension of X is the the minimum s for which there is a c that for every $A \in X$,

$$KS^{2^{cn}}(A_{\leq n}) \leq 2^{n+1} - 2^{n(1-s)} \text{ i.o. } n$$

This means that the $(-1)^{\text{st}}$-scaled pspace-dimension of X is directly related to the best i.o. upper bound (equivalently, to the worse a.e. lower bound) of the form $2^{n+1} - 2^{n\alpha}$ on the space-bounded Kolmogorov complexity of all languages in X.

We can now interpret each scaled dimension result as a Kolmogorov complexity (tight) upper bound.

Juedes and Lutz in [14] prove a measure Small Span Theorem for $\leq_{\text{T}}^{\text{P/poly}}$-reductions in ESPACE. This result says that for each $A \in$ ESPACE, either the class of languages reducible to A (lower span) or the class of problems to which A can be reduced (upper span) has pspace-measure 0. Here, we improve this result by showing that, for $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-reductions, for each $A \in$ ESPACE, either the lower span or the upper span of A has $(-3)^{\mathrm{rd}}$-scaled pspace-dimension 0. This result also improves the scaled dimension Small Span Theorem for polynomial-time many-one reductions given by Hitchcock in [8].

In particular, the class of $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard sets for ESPACE has $(-3)^{\mathrm{rd}}$-scaled pspace-dimension 0 and therefore unusually low space-bounded Kolmogorov complexity.

Juedes and Lutz extensively study in [14] upper and lower bounds on $KS(A_{=n})$. Their best results for hard languages are for the $\leq_{\mathrm{m}}^{\mathrm{P/poly}}$-reductions, that is, non-uniform but many-one reductions. Our result is the first non-trivial upper bound on the Kolmogorov complexity of $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard sets.

We also show that the upper bound we have obtained on the Kolmogorov complexity of these (very general) hard languages is very unusual, because it does not hold for most decidable languages (in the sense of both measure and scaled dimension).

The paper is organized as follows. Section 2 contains notation and preliminaries. Section 3 reviews the main concepts in scaled dimension. Section 4 contains our characterization and section 5 our results for the Kolmogorov complexity of hard sets.

2 Preliminaries

The Cantor space $\mathbf{C}$ is the set of all infinite binary sequences. If $w \in \{0,1\}^*$ and $x \in \{0,1\}^* \cup \mathbf{C}$, $w \sqsubseteq x$ means that w is a prefix of x. For $0 \leq i \leq j$, we write $x[i \ldots j]$ for the string consisting of the i-th trough the j-th bits of x.

If $s_0, s_1, s_2 \ldots$ is the standard enumeration of $\{0,1\}^*$ in lexicographical order, we identify each language with its characteristic sequence $\chi_A \in \mathbf{C}$ where

$$\chi_A[i] = \begin{cases} 1 & \text{if } s_i \in A \\ 0 & \text{if } s_i \notin A \end{cases}$$

Abusing this identification, for each $n \in \mathbb{N}$, we will use both

$$\begin{array}{lcl} A_{=n} = A \cap \{0,1\}^n & \text{and} & A_{=n} = A[2^n - 1 \ldots 2^{n+1} - 2] \\ A_{\leq n} = A \cap \{0,1\}^{\leq n} & \text{and} & A_{\leq n} = A[0 \ldots 2^{n+1} - 2] \end{array}$$

For each $i \in \mathbb{N}$ we define a class G_i of functions from $\mathbb{N}$ to $\mathbb{N}$ as follows.

$$\begin{array}{rcl} G_0 & = & \{f \mid (\exists k)(\forall^\infty n) f(n) \leq kn\} \\ G_{i+1} & = & \{f \mid (\exists g \in G_i)(\forall^\infty n) f(n) \leq 2^{g(\log n)}\} \end{array}$$

We also define the functions $\widehat{g}_i \in G_i$ by $\widehat{g}_0(n) = 2n$, $\widehat{g}_{i+1}(n) = 2^{\widehat{g}_i(\log n)}$. We regard the functions in these classes as growth rates. In particular, G_0 contains the linearly bounded growth rates and G_1 contains the polynomially bounded growth rates. Each G_i is closed under composition, each $f \in G_i$ is $o(\widehat{g}_{i+1})$ and each $\widehat{g}_i$ is $o(2^n)$. Thus, G_i contains superpolynomial growth rates for all $i > 1$, but all growth rates in the G_i-hierarchy are subexponential.

Within the class of all decidable languages, we are interested in the exponential space complexity classes $\mathrm{E}_i\mathrm{SPACE}=\mathrm{DSPACE}(2^{G_{i-1}})$ for $i \geq 1$. In particular $\mathrm{E}_1\mathrm{SPACE} = \mathrm{ESPACE} = \mathrm{DSPACE}(2^{O(n)})$ and $\mathrm{E}_2\mathrm{SPACE} = \mathrm{DSPACE}(2^{n^{O(1)}})$.

We use the following classes of total functions.

$$\begin{aligned} \text{all} &= \{f \mid f : \{0,1\}^* \to \{0,1\}^*\} \\ \text{comp} &= \{f \in \text{all} \mid f \text{ is computable}\} \\ \mathrm{p}_i\text{space} &= \{f \in \text{all} \mid f \text{ is computable in } G_i \text{ space}\} \ (i \geq 1) \end{aligned}$$

(Then length of the output is included as part of the space used in computing f). We write pspace for $\mathrm{p}_1$space. Throughout this paper, Δ denotes one of the classes comp, $\mathrm{p}_i$space (for some $i \geq 1$).

A constructor is a function $\delta : \{0,1\}^* \to \{0,1\}^*$ that satisfies $x \sqsubseteq \delta(x)$ for all x. The result of a constructor δ (i.e. the language constructed by δ) is the unique language $R(\delta)$ such that $\delta^n(\lambda) \sqsubseteq R(\delta)$ for all $n \in \mathbb{N}$. Our interest in the above-defined classes of functions is because of the following facts.

$$\begin{aligned} R(\text{all}) &= \mathbf{C} \\ R(\text{comp}) &= \mathrm{DEC} \\ R(\mathrm{p}_i\text{space}) &= \mathrm{E}_i\mathrm{SPACE} \ \text{ for } i \geq 1 \end{aligned}$$

If D is a discrete domain, then a function $f : D \to [0,\infty)$ is Δ-computable if there is a function $\widehat{f} : \mathbb{N} \times D \to \mathbb{Q} \cap [0,\infty)$ such that $|\widehat{f}(r,x) - f(x)| \leq 2^{-r}$ for all $r \in \mathbb{N}$ and $x \in D$ and $\widehat{f} \in \Delta$ (with r coded in unary and the output coded in binary). We say that f is exactly Δ-computable if $f : D \to \mathbb{Q} \cap [0,\infty)$ and $f \in \Delta$.

We use $\log^{(i)}$ for the i-times iterated application of log, $\log^{(i)}(x) = \overbrace{\log(\ldots \log}^{i} x)$.

The binary entropy is the function $\mathcal{H} : [0,1] \to [0,1]$ defined as $\mathcal{H}(x) = -x\log(x) - (1-x)\log(1-x)$, with $\mathcal{H}(0) = 0$ and $\mathcal{H}(1) = 0$.

3 Scaled Dimension

Hitchcock, Lutz and Mayordomo [9] introduced resource-bounded scaled dimension. In this section we review the essentials of this theory and state some useful properties.

A scale is a function $g : H \times [0, +\infty) \to \mathbb{R}$ where $H = (a, \infty)$ for some $a \in \mathbb{R} \cup \{-\infty\}$. A scale must satisfy certain properties stated in [9]. Here we concentrate in the following family of scales.

Definition. We define $g_i : H_i \times [0, \infty) \to \mathbb{R}$ and $g_{-i} : H_i \times [0, \infty) \to \mathbb{R}$ by recursion on $i \in \mathbb{N}$ as follows:

$$g_0(m, s) = ms.$$

$$g_{i+1}(m, s) = 2^{g_i(\log m, s)}$$

$$g_{-i}(m, s) = \begin{cases} m + g_i(m, 0) - g_i(m, 1 - s) & \text{for } 0 \leq s \leq 1 \\ g_i(m, s) & \text{for } s > 1 \end{cases}$$

The domain of g_i coincides with that of g_{-i} and is of the form $H_i = (a_i, \infty)$, where $a_0 = -\infty$ and $a_{i+1} = 2^{a_i}$. We write $m_i = m_{-i} = \max\{0, a_i\}$. □

Example 3.1 *For* $0 \leq s \leq 1$,

$$g_3(m, s) = 2^{2^{(\log\log m)^s}}$$

$$g_2(m, s) = 2^{(\log m)^s}$$

$$g_1(m, s) = m^s$$

$$g_0(m, s) = ms$$

$$g_{-1}(m, s) = m + 1 - m^{1-s}$$

$$g_{-2}(m, s) = m + 2 - 2^{(logm)^{1-s}}$$

$$g_{-3}(m, s) = m + 2^2 - 2^{2^{(\log\log m)^{1-s}}}$$

Scaled dimension is defined using functions called scaled gales [9]. Particular cases of this concept are gales and martingales.

Definition. Let $k \in \mathbb{Z}$ and $s \in [0, \infty)$.

1. An $s^{(k)}$-gale is a function $d : \{0, 1\}^* \to [0, \infty)$ satisfying

$$d(w) = 2^{-g_k(|w|+1,s)+g_k(|w|,s)}[d(w0) + d(w1)]$$

for all $w \in \{0, 1\}$ with $|w| \geq m_k$.

2. An s-gale is a $s^{(0)}$-gale, that is, a function $d : \{0,1\}^* \to [0,\infty)$ satisfying

$$d(w) = 2^{-s}[d(w0) + d(w1)]$$

for all $w \in \{0,1\}^*$.

3. A martingale is a 0-gale, that is, a function $d : \{0,1\}^* \to [0,\infty)$ satisfying

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

for all $w \in \{0,1\}^*$.

□

Definition. Let $k \in \mathbb{Z}$, $s \in [0,+\infty)$ and d be an $s^{(k)}$-gale.

1. We say that d succeeds on a sequence $S \in \mathbf{C}$ if

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

2. The success set of d is

$$S^\infty[d] = \{S \in \mathbf{C} \mid d \text{ succeeds on } S\}$$

□

Definition. Let $X \subseteq \mathbf{C}$ and $k \in \mathbb{Z}$.

1. $\mathcal{G}_\Delta^{(k)}(X)$ is the set of all $s \in [0,\infty)$ such that there is a Δ-computable $s^{(k)}$-gale d such that $X \subseteq S^\infty[d]$.

2. The k^{th}-order scaled Δ-dimension of X is

$$\dim_\Delta^{(k)}(X) = \inf \mathcal{G}_\Delta^{(k)}(X)$$

3. The k^{th}-order scaled dimension of X in $R(\Delta)$ is

$$\dim^{(k)}(X|R(\Delta)) = \dim_\Delta^{(k)}(X \cap R(\Delta))$$

□

For the scale $g_0(m,s) = ms$ we have the resource-bounded dimensions defined in [21].

$$\begin{aligned}\dim_\Delta(X) &= \dim_\Delta^{(0)}(X)\\ \dim(X|R(\Delta)) &= \dim^{(0)}(X|R(\Delta))\end{aligned}$$

For every X, k and Δ, $\dim_\Delta^{(k)}(X)$ is in $[0,1]$, and $\dim_\Delta^{(k)}(R(\Delta)) = 1$ [9].

For this reason Δ is the right resource bound for dimension in $R(\Delta)$. If $\Delta \in \{\text{comp}, \text{p}_i\text{space}\}$,

$$\dim_\Delta^{(k)}(X) \leq \dim_\Delta^{(k+1)}(X)$$

We are particularly interested in the case $\Delta = \text{pspace}$, that is, $\dim_{\text{pspace}}^{(k)}(X)$ and $\dim^{(k)}(X|\text{ESPACE})$.

We will use pspace-measure and measure in ESPACE when referring to results in [14].

Definition. A class $X \subseteq \mathbf{C}$ has pspace-measure 0 (denoted by $\mu_{\text{pspace}}(X) = 0$) iff there exists a martingale $d \in \text{pspace}$ such that, $X \subseteq S^\infty[d]$.

A class $X \subseteq \mathbf{C}$ has pspace-measure 1 (denoted by $\mu_{\text{pspace}}(X) = 1$) iff X^c has pspace-measure 0.

A class $X \subseteq \mathbf{C}$ has measure 0 in ESPACE iff $X \cap \text{ESPACE}$ has pspace-measure 0. This is denoted by $\mu(X|\text{ESPACE}) = 0$.

A class $X \subseteq \mathbf{C}$ has measure 1 in ESPACE iff X^c has measure 0 in ESPACE. This is denoted by $\mu(X|\text{ESPACE}) = 1$. □

A basic result relating measure and dimension is the following

Proposition 3.2 *[21, 9] Let $X \subseteq \mathbf{C}$, $k \in \mathbb{Z}$*

1. *If $\dim_{\text{pspace}}^{(k)}(X) < 1$, then $\mu_{\text{pspace}}(X) = 0$.*
2. *If $\dim^{(k)}(X|\text{ESPACE}) < 1$, then $\mu(X|\text{ESPACE}) = 0$.*

Finally, we will use the following inverses of g_k.

Definition. Let $i \in \mathbb{N}$. We define $f_i : \mathbb{N}\times[0,\infty) \to \mathbb{R}$ and $f_{-i} : \mathbb{N}\times[0,\infty) \to \mathbb{R}$ by

$$\begin{aligned} f_i(n,x) &= \frac{\log^{(i)} x}{\log^{(i)} n} \\ (f_{-i})(n,x) &= 1 - \frac{\log^{(i)}(n-x)}{\log^{(i)} n} \end{aligned}$$

□

Notice that for each $k \in \mathbb{Z}$, $x \in [0,\infty)$, f_k tends to the inverse of g_k, that is,

$$g_k(n, f_k(n,x)) = x + \epsilon(n)$$

where $\lim_n \epsilon(n) = 0$.

We end this section with a few technical properties of scaled dimension that will be useful in our proofs.

Definition. Let d an $s^{(k)}$-gale. The unitary success set of d is

$$S^1[d] = \{S \in \mathbf{C} \mid \exists n\ d(S[0 \ldots n-1]) \geq 1\}$$

A series $\sum_{n=0}^{\infty} a_n$ of nonnegative real numbers a_n is Δ-convergent if there is a function $h : \mathbb{N} \to \mathbb{N}$ such that $h \in \Delta$ and

$$\sum_{n=h(r)}^{\infty} a_n \leq 2^{-r}$$

for all $r \in \mathbb{N}$. Such a function h is called a modulus of the convergence. Adding a layer of uniformity, a sequence

$$\sum_{n=0}^{\infty} a_{j,n}\ (j = 0, 1, 2, \ldots)$$

of series of nonnegative real numbers is uniformly Δ-convergent if there is a function $m : \mathbb{N}^2 \to \mathbb{N}$ such that $m \in \Delta$ and, for all $j \in \mathbb{N}$, m_j is a modulus of the convergence of the series $\sum_{n=0}^{\infty} a_{j,n}$. □

The scaled-dimension version of Borel-Cantelli Lemma [9] is the following.

Lemma 3.3 *Let $k \in \mathbb{Z}$ and $s \in [0, \infty)$. If $d : \mathbb{N}^2 \times \{0,1\}^* \to [0, \infty)$ is a Δ-computable function such that for each $j, n \in \mathbb{N}$, $d_{j,n}$ is an $s^{(k)}$-gale, and such that for each w with $|w| = m_i$ the series*

$$\sum_{n=0}^{\infty} d_{j,n}(w)\ (j = 0, 1, 2 \ldots)$$

are uniformly Δ-convergent, then

$$\dim_{\Delta}^{(k)}(\bigcup_{j=0}^{\infty} \bigcap_{t=0}^{\infty} \bigcup_{n=t}^{\infty} S^1[d_{j,n}]) \leq s.$$

Proposition 3.4 *Let $0 < s' < s \leq 1$ and $i, j \in \mathbb{N}$ with $i \leq j$.*

1. *$g_i(n, s)$ and $g_{-i}(n, s)$ are* pspace*-computable for $s < 1$ and* $\mathrm{p}_i$space*-computable for $s \geq 1$.*

2. $\sum_{n=m_i}^{\infty} 2^{g_i(n,s')-g_i(n,s)}$ *is* p$_j$space-*convergent.*

3. $\sum_{n=m_i}^{\infty} 2^{g_{-i}(n,s')-g_{-i}(n,s)}$ *is* p$_j$space-*convergent.*

Proof. Part 1. follows by induction on i.

Notice that $g_{-i}(n,s')-g_{-i}(n,s) = g_i(n,1-s)-g_i(n,1-s')$, so 3. follows from 2.

To prove 2, let $s' < s'' < s$. Then $g_i(n,s'') = o(g_i(n,s) - g_i(n,s'))$.

Notice that $g_i(g_i(m,\frac{1}{s''}),s'') = m$ for each $m > m_i$.

Let n_0 be such that for each $n \geq n_0$

$$g_i(n,s'') < g_i(n,s) - g_i(n,s')$$

and

$$g_i(n,\frac{1}{s''}) < 2^{\frac{n}{2}}.$$

We define $h(k) = n_0 + g_i(2k+2n_0+4,\frac{1}{s''})$. Then

$$\begin{aligned}\sum_{n=h(k)}^{\infty} 2^{g_i(n,s')-g_i(n,s)} &\leq \sum_{n=h(k)}^{\infty} 2^{-g_i(n,s'')} \\ &\leq \sum_{m=k+n_0+2}^{\infty} 2^{-2m}(g_i(2m+2,\frac{1}{s''}) - g_i(2m,\frac{1}{s''})) \\ &\leq \sum_{m=k+2}^{\infty} 2^{-2m+m+1} = 2^{-k}\end{aligned}$$

□

4 Characterization

In this section we examine the relationship between scaled dimension and space-bounded Kolmogorov complexity. We start with a brief summary of definitions and notation for resource-bounded Kolmogorov complexity.

Definition. Given a Turing machine M, $t : \mathbb{N} \to \mathbb{N}$, $S \in \mathbf{C}$ and $n \in \mathbb{N}$

1. The t-space-bounded Kolmogorov complexity of $S[0\ldots n-1]$ is,

$$KS_M^{t(n)}(S[0\ldots n-1]) = \min\left\{|\pi| \;\middle|\; M(\pi) = S[0\ldots n-1] \text{ in } \leq t(n) \text{ space}\right\}$$

2. The t-time-bounded Kolmogorov complexity of $S[0\ldots n-1]$ is,

$$K_M^{t(n)}(S[0\ldots n{-}1]) = \min\left\{|\pi| \;\middle|\; M(\pi) = S[0\ldots n{-}1] \text{ in } \leq t(n) \text{ time}\right\}$$

□

Well-know techniques [17] show that there is a machine U that is optimal in the sense that for each machine M there is a constant c such that for all total computable t, $S \in \mathbf{C}$ and $n \in \mathbb{N}$, we have

$$KS_U^{ct(n)+c}(S[0\ldots n-1]) \leq KS_M^{t(n)}(S[0\ldots n-1]) + c$$

$$K_U^{ct(n)\log(t(n))}(S[0\ldots n-1]) \leq K_M^{t(n)}(S[0\ldots n-1]) + c$$

As usual, we fix an optimal machine U and omit it from the notation.

Our characterization will use the following notation.

Definition. Let $S \in \mathbf{C}$, $k \in \mathbb{Z}$, t a resource bound.

$$\mathcal{KS}^t_{(k)}(S) = \liminf_n f_k(n, KS^{t(n)}(S[0\ldots n-1]))$$

$$\mathcal{K}^t_{(k)}(S) = \liminf_n f_k(n, K^{t(n)}(S[0\ldots n-1]))$$

□

For instance, for k between -2 and 2 we have

$$\mathcal{KS}^t_{(2)}(S) = \liminf_n \frac{\log\log(KS^{t(n)}(S[0\ldots n-1]))}{\log\log n}$$

$$\mathcal{KS}^t_{(1)}(S) = \liminf_n \frac{\log(KS^{t(n)}(S[0\ldots n-1]))}{\log n}$$

$$\mathcal{KS}^t_{(0)}(S) = \liminf_n \frac{KS^{t(n)}(S[0\ldots n-1])}{n}$$

$$\mathcal{KS}^t_{(-1)}(S) = \liminf_n \left(1 - \frac{\log(n - KS^{t(n)}(S[0\ldots n-1]))}{\log n}\right)$$

$$\mathcal{KS}^t_{(-2)}(S) = \liminf_n \left(1 - \frac{\log\log(n - KS^{t(n)}(S[0\ldots n-1]))}{\log\log n}\right)$$

The following observation states the precise meaning of $\mathcal{KS}$ in terms of i.o. upper bounds.

Observation 4.1 *Let $k \in \mathbb{Z}$ and $S \in \mathbf{C}$. Let t be a resource bound. Then,*

$$\mathcal{KS}^t_{(k)}(S) = \inf\{s \in [0,\infty) | \exists^\infty n\, KS^{t(n)}(S[0\dots n-1]) < g_k(n,s)\}$$

For example, $\mathcal{KS}^t_{(-1)}(S)$ is the smallest s for which

$$KS^{t(n)}(S[0\dots n-1]) < n - n^{1-s} \text{ i.o. } n$$

For classes of languages we take the worse case upper bound.
Definition. Let $X \subseteq \mathbf{C}$, $k \in \mathbb{Z}$ and $j \in \mathbb{N}$

$$\mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(k)}(X) = \inf_{t \in \mathrm{p}_j\mathrm{space}} \sup_{S \in X} \mathcal{KS}^t_{(k)}(S)$$

$$\mathcal{K}^{\mathrm{comp}}_{(k)}(X) = \inf_{t \in \mathrm{comp}} \sup_{S \in X} \mathcal{K}^t_{(k)}(S)$$

□

The main result in this section is the following characterization of scaled-dimension.

Theorem 4.2 *Let $X \subseteq \mathbf{C}$*

1. *For all $i, j \in \mathbb{N}$ with $i \leq j$*

$$\dim^{(i)}_{\mathrm{p}_j\mathrm{space}}(X) = \mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(i)}(X)$$

$$\dim^{(-i)}_{\mathrm{p}_j\mathrm{space}}(X) = \mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(-i)}(X)$$

2. *For all $k \in \mathbb{Z}$*

$$\dim^{(k)}_{\mathrm{comp}}(X) = \mathcal{K}^{\mathrm{comp}}_{(k)}(X)$$

A similar characterization for the cases $\dim^{(-i)}_{\mathrm{p}_j\mathrm{space}}$ $(i > j)$ is not possible because it is known (Theorem 3.3 in [14]) that for each $A \in \mathrm{ESPACE}$ there is an $\epsilon > 0$ such that $KS^{2^{2n}}(A_{\leq n}) < 2^{n+1} - 2^{\epsilon n}$ a.e. n, therefore

$$\mathcal{KS}^{\mathrm{pspace}}_{(-2)}(\mathrm{ESPACE}) = 0$$

whereas we know that $\dim^{(-2)}_{\mathrm{pspace}}(\mathrm{ESPACE}) = 1$ [21].

The case $i = 0$ corresponds to resource-bounded dimension and is proven in [7].

A dual version of Theorem 4.2 can be proven for the packing or strong dimension as characterized in [3].

Theorem 4.2 is proven from the next two lemmas. The first one states that dimension is smaller that $\mathcal{KS}$, and it only holds for $i \leq j$ in the space-bounded case.

Lemma 4.3 *Let $X \subseteq \mathbf{C}$*

1. *For all $i, j \in \mathbb{N}$ with $i \leq j$*

$$\dim^{(i)}_{\mathrm{p}_j\mathrm{space}}(X) \leq \mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(i)}(X)$$

$$\dim^{(-i)}_{\mathrm{p}_j\mathrm{space}}(X) \leq \mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(-i)}(X)$$

2. *For all $k \in \mathbb{Z}$*

$$\dim^{(k)}_{\mathrm{comp}}(X) \leq \mathcal{K}^{\mathrm{comp}}_{(k)}(X)$$

Proof. We start with the first part of case 1. The proof is based in Lemma 3.3.

Let $s > s' > \mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(i)}(X)$ be rational and let $t \in \mathrm{p}_j\mathrm{space}$ with $t(n) \geq n$ such that

$$\exists^\infty n \; KS^{t(n)}(S[0 \dots n-1]) < g_i(n, s')$$

for all $S \in X$. Such a t exists by Observation 4.1.

For all $n \in \mathbb{N}$, if we define

$$Y_n = \{A \in \mathbf{C} \mid KS^{t(n)}(A[0 \dots n-1]) < g_i(n, s')\}$$

then

$$X \subseteq \bigcap_{m=0}^{\infty} \bigcup_{n=m}^{\infty} Y_n.$$

Let a be such that $2g_i(n, s') < g_i(n, s) + a$ for every $n \in \mathbb{N}$.

For all $n \in \mathbb{N}$ define $d_n : \{0,1\}^* \to [0, \infty)$ by

$$d_n(w) = \begin{cases} 2^{-g_i(n,s')+a+g_i(m_i,s)} & \text{if } |w| \leq m_i \\ 2^{g_i(|w|,s)-g_i(m_i,s)} d_n(w[0 \dots m_i - 1])\rho(w) & \text{if } m_i < |w| \leq n \\ 2^{g_i(|w|,s)-g_i(n,s)-|w|+n} d_n(w[0 \dots n-1]) & \text{if } |w| > n \end{cases}$$

where

$$\rho(w) = \frac{\#\{\pi \mid |\pi| < g_i(n, s'),\ w \sqsubseteq U(\pi) \text{ in } \leq t(n) \text{ space}\}}{2^{g_i(n,s')} - 1}$$

Then, d_n is an $s^{(i)}$-gale computable in $O(t(n))$-space for all $n \in \mathbb{N}$, and for all $w \in \{0,1\}^{m_i}$,

$$\sum_{n=0}^{\infty} d_n(w)$$

is $\mathrm{p}_j$space-convergent. Moreover, for all $n \in \mathbb{N}$, $Y_n \subseteq S^1[d]$. By Lemma 3.3, $\dim^{(i)}_{\mathrm{p}_j\mathrm{space}}(X) \leq s$. Since this holds for each $s > \mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(i)}(X)$ it follows that $\dim^{(i)}_{\mathrm{p}_j\mathrm{space}}(X) \leq \mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(i)}(X)$.

The proof for the second part of case 1. can be done by substituting g_i by g_{-i} in the proof of the first part, with the exception of the definition of $d_n(w)$ for $|w| \leq m_i$ that is now

$$d_n(w) = 2^{-g_i(n,s')+a+g_{-i}(m_i,s)}.$$

The proof of case 2. is analogous and easier, since we don't have to worry about resource-bounds.

□

The second inequality, $\mathcal{KS}$ smaller than dimension, holds without restriction on the scale used. This will be useful in the next section.

Lemma 4.4 *Let $X \subseteq \mathbf{C}$. For all $j \in \mathbb{N}$, $k \in \mathbb{Z}$*

$$\mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(k)}(X) \leq \dim^{(k)}_{\mathrm{p}_j\mathrm{space}}(X)$$

$$\mathcal{K}^{\mathrm{comp}}_{(k)}(X) \leq \dim^{(k)}_{\mathrm{comp}}(X)$$

Proof. Let $s > \dim^{(k)}_{\mathrm{p}_j\mathrm{space}}(X)$. Let d be a $\mathrm{p}_j$space-computable $s^{(k)}$-gale with $X \subseteq S^{\infty}[d]$. Let $t \in \mathrm{p}_j\mathrm{space}$ be such that $t(n) \geq n$ and d can be computed in space t. Assume without loss of generality that $d(w) < 1$ for all $|w| = m_k$. For all $n \geq m_k$, we have that by the Kraft's inequality (Lemma 3.6 in [9]) for $C = 2^{-g_k(m_k,s)}$

$$\sum_{w\in\{0,1\}^n} d(w) \leq C2^{g_k(n,s)}.$$

Define $A = \{w \mid d(w) > 1\}$. Then, for all $n \geq m_k$, $|A_{=n}| < C2^{g_k(n,s)}$ and $A \in \mathrm{E}_j\mathrm{SPACE}$.

Each $w \in A_{=n}$ can be described by giving n and its index within a list of $A_{=n}$ in lexicographical order. By reusing space, w can be computed from this description in $3t(n)$ space. Therefore, for all $w \in A_{=n}$ $(n \geq m_k)$,

$$KS^{3t(n)}(w) \leq \log(|A^{=n}|) + O(\log n) < g_k(n,s) + O(\log n)$$

Let $S \in X$. Then

$$\exists^\infty n \;\; S[0 \ldots n-1] \in A_{=n}$$

therefore

$$\exists^\infty n \;\; KS^{3t(n)}(S[0 \ldots n-1]) < g_k(n,s) + O(\log n)$$

Therefore, $\mathcal{KS}^{3t}_{(k)}(S) \leq s$ and $\mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(k)}(X) \leq s$. Since this holds for each $s > \dim^{(k)}_{\mathrm{p}_j\mathrm{space}}(X)$ it follows that $\mathcal{KS}^{\mathrm{p}_j\mathrm{space}}_{(k)}(X) \leq \dim^{(k)}_{\mathrm{p}_j\mathrm{space}}(X)$.

The proof of the second part is analogous.

□

Lemma 4.4 holds for the polynomial time scaled dimension and the corresponding polynomial-time-bounded Kolmogorov complexity. This can be proven by using the techniques in [11] and [10].

Our characterization also holds when restricting to Kolmogorov complexity of prefixes of the form $A_{\leq n}$, except for the 0^{th}-scale case.

Theorem 4.5 *Let $X \subseteq \mathbf{C}$,*

1. *For all $i, j \in \mathbb{N}$ with $0 < i \leq j$,*

   $$\dim^{(i)}_{\mathrm{p}_j\mathrm{space}}(X) < s$$

   iff there is a $t \in \mathrm{p}_j\mathrm{space}$ such that for any $A \in X$

   $$KS^{t(2^{n+1})}(A_{\leq n}) < g_i(2^{n+1}, s) \text{ i.o. } n.$$

2. *For all $i, j \in \mathbb{N}$ with $0 < i \leq j$,*

   $$\dim^{(-i)}_{\mathrm{p}_j\mathrm{space}}(X) < s$$

   iff there is a $t \in \mathrm{p}_j\mathrm{space}$ such that for any $A \in X$

   $$KS^{t(2^{n+1})}(A_{\leq n}) < g_{-i}(2^{n+1}, s) \text{ i.o. } n.$$

3. *For all $k \in \mathbb{Z}$, $k \neq 0$,*

   $$\dim^{(k)}_{\mathrm{comp}}(X) < s$$

   iff there is a $t \in \mathrm{comp}$ such that for any $A \in X$

   $$KT^{t(2^{n+1})}(A_{\leq n}) < g_k(2^{n+1}, s) \text{ i.o. } n.$$

Proof. In all cases, the second implication follows directly from Theorem 4.2.

For the proof of case 1., let s' be such that $\dim^{(-i)}_{\mathrm{p}_j\mathrm{space}}(X) < s' < s$. From Theorem 4.2 we know that there is a $t \in \mathrm{p}_j\mathrm{space}$ such that for every $A \in X$ and infinitely many m,

$$KS^{t(m)}(A[0 \dots m-1]) < g_{-i}(m, s') = m - g_i(m, 1-s'). \tag{1}$$

Let $A \in X$, $m \in \mathbb{N}$ be such that (1) holds, with m big enough to have $g_i(2m, 1-s) + \log(m+1) \leq g_i(m, 1-s')$. Let n be the smallest such that $2^{n+1} - 1 \geq m$.

$$\begin{aligned} KS^{t(2^{n+1})+2^n}(A[0 \dots 2^{n+1}-2]) &< m - g_i(m, 1-s') + (2^{n+1} - m) + n \\ &= 2^{n+1} - g_i(m, 1-s') + \log(m+1) \\ &\leq 2^{n+1} - g_i(2^{n+1}, 1-s) = g_{-i}(2^{n+1}, s) \end{aligned}$$

If $t'(m) = t(m) + m/2$ then $t' \in \mathrm{p}_j\mathrm{space}$, so the first implication holds.

For case 2., repeat the argument but this time using the biggest n such that $2^{n+1} - 1 \leq m$.

Case 3. is a combination of the other two.

□

For example for the pspace case, $\dim^{(-1)}_{\mathrm{pspace}}(X) < s$ iff there is a c such that for any $A \in X$

$$KS^{2^{c(n+1)}}(A_{\leq n}) < 2^{n+1} - 2^{(n+1)(1-s)} \text{ i.o. } n.$$

As a final remark, notice that it is not equivalent in general to consider $KS(A_{=n})$ and $KS(A_{\leq n})$. Whereas $KS^{2^{cn}}(A_{=n}) < 2^n - 2^{\epsilon n}$ implies that $KS^{2^{c'n}}(A_{\leq n}) < 2^{n+1} - 2^{\epsilon n}$, the quantity $KS^{2^{cn}}(A_{\leq n})$ can be much lower than $KS(A_{=n})$, relative to the corresponding length. Juedes and Lutz extensively study $KS(A_{=n})$ in [14], mainly for languages in ESPACE and languages that are $\leq^{\mathrm{P/poly}}_{\mathrm{m}}$-hard, that is, hard for many-one non-uniform reductions.

5 The Kolmogorov complexity of hard and weakly hard sets

In this section we are interested in adaptive nonuniform reductions in the class ESPACE, namely P/poly-Turing reductions ($\leq^{\mathrm{P/poly}}_{\mathrm{T}}$) which are nonuniform Turing reductions that can be computed by polynomial-size circuits.

The lower and upper spans are defined as follows.

Definition. Let $A \subseteq \{0,1\}^*$

1. The $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$- lower span of A is

$$(\mathrm{P/poly})_{\mathrm{T}}(A) = \{B \subseteq \{0,1\}^* | B \leq_{\mathrm{T}}^{\mathrm{P/poly}} A\}$$

2. The $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$- upper span of A is

$$(\mathrm{P/poly})_{\mathrm{T}}^{-1}(A) = \{B \subseteq \{0,1\}^* | A \leq_{\mathrm{T}}^{\mathrm{P/poly}} B\}$$

□

Juedes and Lutz [14] prove the following Small Span Theorem for these reductions.

Theorem 5.1 *[14] For every* $A \in \mathrm{ESPACE}$

$$\mu((\mathrm{P/poly})_{\mathrm{T}}(A)|\mathrm{ESPACE}) = 0$$

or

$$\mu_{\mathrm{pspace}}((\mathrm{P/poly})_{\mathrm{T}}^{-1}(A)) = 0.$$

This theorem states that for each $A \in \mathrm{ESPACE}$, at least one of the lower and upper spans of A is small in the sense of resource-bounded measure.

Small Span Theorems for the class of exponential time languages and polynomial time reductions have been studied for both measure and dimension [13, 1, 18, 2, 5, 8].

Here we prove the following generalization of Theorem 5.1.

Theorem 5.2 *For every* $A \in \mathrm{ESPACE}$*,*

$$\dim^{(1)}(\,(\mathrm{P/poly})_{\mathrm{T}}(A) \mid \mathrm{ESPACE}) = 0$$

or

$$\dim^{(-3)}_{\mathrm{pspace}}(\,(\mathrm{P/poly})_{\mathrm{T}}^{-1}(A)\,) = 0.$$

The proof is based in the following lemma.

Lemma 5.3

$$\dim^{(1)}\Big(\ \Big\{A \subseteq \{0,1\}^* \ \Big|\ \dim^{(-3)}_{\mathrm{pspace}}(\ (\mathrm{P/poly})_{\mathrm{T}}^{-1}(A)\ ) > 0\Big\}\ \Big|\mathrm{ESPACE}\Big) = 0.$$

We defer the proof of Lemma 5.3 for a moment; first we use the lemma to establish our Small Span Theorem.

Proof. Let $Z = \Big\{A \subseteq \{0,1\}^* \ \Big|\ \dim^{(-3)}_{\mathrm{pspace}}(\ (\mathrm{P/poly})_{\mathrm{T}}^{-1}(A)\ ) > 0\Big\}$. We consider two cases.

1. Suppose that $(\mathrm{P/poly})_{\mathrm{T}}(A) \cap \mathrm{ESPACE} \subseteq Z$. Then it follows from Lemma 5.3 that $\dim^{(1)}((\mathrm{P/poly})_{\mathrm{T}}(A) \mid \mathrm{ESPACE}) = 0$.

2. Otherwise there is a language $B \in (\mathrm{P/poly})_{\mathrm{T}}(A) \cap \mathrm{ESPACE} \cap Z^c$. Then we have $(\mathrm{P/poly})_{\mathrm{T}}^{-1}(A) \subseteq (\mathrm{P/poly})_{\mathrm{T}}^{-1}(B)$ and

$$\dim^{(-3)}_{\mathrm{pspace}}(\ (\mathrm{P/poly})_{\mathrm{T}}^{-1}(A)\ ) \leq \dim^{(-3)}_{\mathrm{pspace}}(\ (\mathrm{P/poly})_{\mathrm{T}}^{-1}(B)\ ) = 0.$$

□

Proof of Lemma 5.3.

Let

$$Y = \{A \subseteq \{0,1\}^* \mid \dim^{(-3)}_{\mathrm{pspace}}(\ (\mathrm{P/poly})_{\mathrm{T}}^{-1}(A)\ ) = 0\}.$$

Our goal is to prove $\dim^{(1)}(Y^c \mid \mathrm{ESPACE}) = 0$. The argument is based on the proof of Theorem 4.5 in [14]. We begin by recalling some of the definitions and notations used in that proof, slightly adapting them for use in our argument.

For each $r \in \mathbb{N}$, define the functions

$$a_r, b_r : \mathbb{N} \to \mathbb{N}$$

$$a_r(n) = n^r + r,$$

$$b_r(n) = \sum_{i=0}^{n} a_r(n).$$

Let ADV_r be the class of all advice functions $h : \mathbb{N} \to \{0,1\}^*$ satisfying $|h(n)| = a_r(n)$ for all $n \in \mathbb{N}$. For any $A, B \subseteq \{0,1\}^*$ satisfying $A \leq_{\mathrm{T}}^{\mathrm{P/poly}} B$, there exist $r, k \in \mathbb{N}$ and $h \in \mathrm{ADV}_r$ such that

$$A = L(M_k^B/h),$$

where M_k is the kth polynomial time-bounded oracle Turing machine.

A *partial $a_r(n)$-advice function* is a finite function

$$h' : \{0, 1, \ldots, k-1\} \to \{0,1\}^*$$

for some $k \in \mathbb{N}$ such that for all $0 \leq n < k$, $|h'(n)| = a_r(n)$. For each partial $a_r(n)$-advice function h', the *cylinder generated by h'* is

$$\mathrm{CYL}(h') = \{h \in \mathrm{ADV}_r \mid h \upharpoonright \{0, 1, \ldots, k-1\} = h'\},$$

where $h \upharpoonright \{0,1,\ldots,k-1\}$ denotes h restricted to domain $\{0,1,\ldots,k-1\}$. The *probability* of this cylinder is defined to be

$$\Pr(\mathrm{CYL}(h')) = \prod_{n=0}^{k-1} 2^{-a_r(n)}.$$

For each $r \in \mathbb{N}$, we will use the sample space

$$\Omega_r = \mathrm{ADV}_r \times \mathcal{P}(\{0,1\}^*).$$

Here we use the product probability measure, with the above probability measure on ADV_r and the uniform distribution on $\mathcal{P}(\{0,1\}^*)$.

For each $r,k,j \in \mathbb{N}$, define the event $\mathcal{E}^A_{r,k,j} \subseteq \Omega_r$ by

$$\mathcal{E}^A_{r,k,j} = \{(h,B) \mid (\forall\, 0 \le i < j)\ [\![s_i \in A]\!] = [\![s_i \in L(M_k^B/h)]\!]\}.$$

For each $r,k,j \in \mathbb{N}$ and $A \subseteq \{0,1\}^*$, let

$$N_A(r,k,j) = \left| \left\{ i < j \;\middle|\; \Pr(\mathcal{E}^A_{r,k,i+1}) \le \frac{1}{2}\Pr(\mathcal{E}^A_{r,k,i}) \right\} \right|.$$

Then for all $r,k,j \in \mathbb{N}$ and $A \subseteq \{0,1\}^*$, we have

$$\Pr(\mathcal{E}^A_{r,k,j}) \le 2^{-N_A(r,k,j)}.$$

For each $A \subseteq \{0,1\}^*$ and rational $s,\delta > 0$, define an $s^{(-3)}$-gale $d^A_{s,\delta} : \{0,1\}^* \to [0,\infty)$ by

$$d^A_{s,\delta}(w) = 2^{-g_3(|w|,1-s)} \sum_{r=0}^{\infty} \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} 2^{-(r+k)/4 - j^\delta} \cdot d^A_{r,k,j}(w),$$

where for all $r,k,j \in \mathbb{N}$, $d^A_{r,k,j}$ is the martingale

$$d^A_{r,k,j}(w) = \begin{cases} 2^{|w|}\Pr(\mathrm{ADV}_r \times \mathbf{C}_w \mid \mathcal{E}^A_{r,k,j}) & \text{if } \Pr(\mathcal{E}^A_{r,k,j}) > 0 \\ 1 & \text{if } \Pr(\mathcal{E}^A_{r,k,j}) = 0. \end{cases}$$

It is routine to show that $d^A_{s,\delta}$ is pspace-computable if $A \in \mathrm{ESPACE}$.

Let $A, B \subseteq \{0,1\}^*$, $k, r \in \mathbb{N}$, and $h \in \mathrm{ADV}_r$ such that $A = L(M_k^B/h)$. There is a polynomial time-bound on M_k and a polynomial length bound on h, so there is a constant $c \in \mathbb{N}$ so that all queries of $(M_k^B/h)(s_i)$ have length strictly bounded by $|s_i|^c$ for all sufficiently large i. Defining $n(i) =$

$\lceil \log(i+2) - 1 \rceil$, we have $|s_i| = n(i)$ for all i. For now, fix $j \in \mathbb{N}$. If we choose

$$l = 2^{(\log(j+1))^c},$$

then all queries of $L(M_k^B/h)(s_i)$ for $0 \leq i < j$ are among $s_0, s_1, \ldots, s_{l-1}$. In other words, $A[0..j-1]$ is determined by $B[0..l-1]$. Note that

$$j + 1 = 2^{(\log l)^{\frac{1}{c}}}.$$

Let $h_j = h \restriction \{0, 1, \ldots, n(j-1)\}$. Then h_j is a restriction of h that provides advice for all the inputs $s_0, \ldots, s_{j-1}$. It follows that $\mathrm{CYL}(h_j) \times \mathbf{C}_{B[0..l-1]} \subseteq \mathcal{E}^A_{r,k,j}$, so we can argue as in [14] that

$$\Pr(\mathcal{E}^A_{r,k,j} \mid \mathrm{ADV}_r \times \mathbf{C}_{B[0..l-1]}) \geq 2^{-b_r(n(j))},$$

and then obtain

$$d^A_{r,k,j}(B[0..l-1]) \geq 2^{N_A(r,k,j) - b_r(n(j))}.$$

Let $\epsilon > \delta > 0$ and define

$$X_\epsilon = \{A \subseteq \{0,1\}^* \mid (\forall k)(\forall r)(\forall^\infty j) N_A(r,k,j) > j^\epsilon\}.$$

We claim that $X_\epsilon \cap \mathrm{ESPACE} \subseteq Y$, i.e., that

$$\dim^{(-3)}_{\mathrm{pspace}}(\ (\mathrm{P/poly})^{-1}_{\mathrm{T}}(A)\ ) = 0 \tag{2}$$

for every $A \in X_\epsilon \cap \mathrm{ESPACE}$. For this, let $A \in X_\epsilon \cap \mathrm{ESPACE}$ and let $B \in (\mathrm{P/poly})^{-1}_{\mathrm{T}}(A)$. Then there exist $k, r \in \mathbb{N}$ and $h \in \mathrm{ADV}_r$ such that $A = L(M_k^B/h)$. Let j be sufficiently large to ensure $N_A(r,k,j) > j^\epsilon$. Then, defining c and l as above, we have

$$\begin{aligned}
\log d^A_{s,\delta}(B[0..l-1]) &\geq \log d^A_{r,k,j}(B[0..l-1]) - g_3(l, 1-s) - (r+k)/4 - j^\delta \\
&\geq j^\epsilon - b_r(n(j)) - g_3(l, 1-s) - (r+k)/4 - j^\delta
\end{aligned}$$

$$= \left(2^{(\log l)^{1/c}} - 1\right)^\epsilon - b_r(n(j)) - 2^{2^{(\log\log l)^{(1-s)}}} - (r+k)/4 - \left(2^{(\log l)^{1/c}} - 1\right)^\delta.$$

Since r and k are constants here, it follows that $B \in S^\infty[d^A_{s,\delta}]$. Therefore $(\mathrm{P/poly})^{-1}_{\mathrm{T}}(A) \subseteq S^\infty[d^A_{s,\delta}]$. Since $A \in \mathrm{ESPACE}$, $d^A_{s,\delta}$ is pspace-computable, so $\dim^{(-3)}_{\mathrm{pspace}}((\mathrm{P/poly})^{-1}_{\mathrm{T}}(A)) \leq s$. This holds for all $s > 0$, so we obtain (2).

Now we show that for every $\epsilon > 0$,

$$\dim^{(1)}_{\mathrm{pspace}}(X^c_\epsilon) \leq \epsilon. \tag{3}$$

Let $A \in X_\epsilon^c$. Then there exist $r, k \in \mathbb{N}$ such that $N_A(r,k,j) \le j^\epsilon$ for infinitely many $j \in \mathbb{N}$. Notice that $N_A(r,k,j)$ is determined by $A[0..j-1]$. For each $j \in \mathbb{N}$, let

$$Z_{r,k,j} = \{B[0..j-1] \mid N_B(r,k,j) \le j^\epsilon\} \subseteq \{0,1\}^j.$$

We can bound the size of $Z_{r,k,j}$ as

$$|Z_{r,k,j}| \le j^\epsilon \binom{j}{j^\epsilon} 2^{j^\epsilon} \le j^\epsilon \cdot 2^{\mathcal{H}(j^{\epsilon-1})j + j^\epsilon}$$

because we can specify an element of the set by first identifying the at most j^ϵ positions i on which $\mathcal{E}^A_{r,k,i+1} \le \frac{1}{2}\mathcal{E}^A_{r,k,i}$ and then using j^ϵ bits to specify which of the two possibilities to use for the i^{th} bit in case $\mathcal{E}^A_{r,k,i+1} = \frac{1}{2}\mathcal{E}^A_{r,k,i}$. Therefore

$$\mathcal{H}(j^{\epsilon-1})j + j^\epsilon + \log j$$

bits are enough to identify each string in $Z_{r,k,j}$. From this description along with encodings of r, k, and j we can compute the string using polynomial space: for some polynomial p we have

$$KS^p(w) \le \mathcal{H}(j^{\epsilon-1})j + j^\epsilon + 2\log j + \log r + \log k$$

for all $w \in Z_{r,k,j}$. We have a single polynomial p that works for every r, k and for every $j \ge j_0(r,k)$ for some $j_0(r,k)$.

Notice that

$$\begin{aligned}
\mathcal{H}(j^{\epsilon-1})j &= \left(j^{\epsilon-1}\log j^{1-\epsilon} + (1-j^{\epsilon-1})\log\frac{1}{1-j^{\epsilon-1}}\right)j \\
&= j^\epsilon(1-\epsilon)\log j + j(1-j^{\epsilon-1})\log\left(1+\frac{j^{\epsilon-1}}{1-j^{\epsilon-1}}\right) \\
&\le j^\epsilon(1-\epsilon)\log j + j(1-j^{\epsilon-1})\frac{j^{\epsilon-1}}{1-j^{\epsilon-1}}\log e \\
&= j^\epsilon[(1-\epsilon)\log j + \log e].
\end{aligned}$$

It follows from the above that $\mathcal{KS}^p_{(1)}(A) \le \epsilon$ because A satisfies $A[0..j-1] \in Z_{r,k,j}$ infinitely often. Since $A \in X_\epsilon$ is arbitrary and the polynomial p does not depend on A, we have $\mathcal{KS}^{\text{pspace}}_{(1)}(X_\epsilon) \le \epsilon$. Appealing to Theorem 4.2, we establish (3).

We proved that $X_\epsilon \cap \text{ESPACE} \subseteq Y$ for all $\epsilon \in (0,1)$. This implies $Y^c \cap \text{ESPACE} \subseteq X_\epsilon^c$, so

$$\dim^{(1)}(Y^c \mid \text{ESPACE}) = \dim^{(1)}_{\text{pspace}}(Y^c \cap \text{ESPACE}) \le \dim^{(1)}_{\text{pspace}}(X_\epsilon^c) \le \epsilon$$

for all $\epsilon \in (0,1)$. Therefore $\dim^{(1)}(Y^c \mid \mathrm{ESPACE}) = 0$, so the lemma holds.

□

Theorem 5.2 generalizes Theorem 5.1 because $\dim^{(-3)}(X) < 1$ implies $\mu_{\mathrm{pspace}}(X) = 0$. Hitchcock shows in in [8] that $(-2)^{\mathrm{nd}}$-scaled Small Span Theorems are not possible, since for A a $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language for ESPACE, $\dim_{\mathrm{pspace}}^{(-2)}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = 1$. Therefore we can't substitute -3 by a bigger scale in the statement of Theorem 5.2.

Because of the connections we have obtained between scaled dimension and Kolmogorov complexity we can conclude the following.

Theorem 5.4 *For every* $A \in \mathrm{ESPACE}$, *if*

$$\dim^{(1)}((\mathrm{P/poly})_{\mathrm{T}}(A)|\mathrm{ESPACE}) > 0$$

then

$$\mathcal{KS}_{\mathrm{pspace}}^{(-3)}((\mathrm{P/poly})_{\mathrm{T}}^{-1}(A)) = 0$$

Proof. The theorem follows from Theorem 5.2 and Lemma 4.4.

□

In particular for hard languages we have the following corollary.

Corollary 5.5 *Let* $\mathcal{H}$ *be the class of languages that are* $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$*-hard for* ESPACE. *Then*

$$\mathcal{KS}_{\mathrm{pspace}}^{(-3)}(\mathcal{H}) = 0,$$

that is, for each $\epsilon > 0$ *there is a* c *such that for every* $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$*-hard* H

$$\mathcal{KS}^{2^{cn}}(H_{\leq n}) < 2^{n+1} - 2^{2^{(\log n)^{1-\epsilon}}} \quad i.o.\ n$$

This corollary tells us that $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard languages are unusually simple, since for most languages the opposite holds, even when allowing any resource bound on the Kolmogorov complexity.

Theorem 5.6 *For very resource bound* t, *the class of all sets* A *such that for any* ϵ

$$KS^{t(2^n)}(A_{\leq n}) < 2^{n+1} - 2^{2^{(\log n)^{1-\epsilon}}} \quad i.o.\ n$$

has $(-3)^{rd}$ comp-*dimension 0.*

Proof. The result follows from our characterization in Theorem 4.2.

□

Theorem 5.6 implies that most decidable languages (in a very strong sense) don't have the upper bound on Kolmogorov complexity that $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard languages have.

Notice that the best known lower bound on the Kolmogorov complexity of $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard sets is Theorem 4.1. in [14], stating that for each $\leq_{\mathrm{T}}^{\mathrm{P/poly}}$-hard H there is an $\epsilon > 0$ such that

$$KS^{2^{n^\epsilon}}(H_{\leq n}) > 2^{n^\epsilon} \text{ a.e. } n$$

6 Conclusion

We have obtained a Kolmogorov complexity characterization of scaled dimension for the cases where such a characterization is possible. We expect that the combination of fractal and information theory techniques will produce interesting results on the problem of uniform vs nonuniform complexity.

Acknowledgement

We thank Jack Lutz for very helpful discussions on reference [14].

References

[1] K. Ambos-Spies, W. Merkle, J. Reimann, and F. Stephan. Hausdorff dimension in exponential time. In *Proceedings of the 16th IEEE Conference on Computational Complexity*, pages 210–217, 2001.

[2] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn. Genericity and measure for exponential time. *Theoretical Computer Science*, 168(1):3–19, 1996.

[3] K. B. Athreya, J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. Effective strong dimension in algorithmic information and computational complexity. In *Proceedings of the Twenty–First Symposium on Theoretical Aspects of Computer Science*, volume 2996 of *Lecture Notes in Computer Science*, pages 632–643. Springer-Verlag, 2004.

[4] J. L. Balcázar and R. V. Book. Sets with small generalized Kolmogorov complexity. *Acta Informatica*, 23:679–688, 1986.

[5] H. Buhrman and D. van Melkebeek. Hard sets are hard to find. *Journal of Computer and System Sciences*, 59(2):327–345, 1999.

[6] J. Hartmanis. Generalized Kolmogorov complexity and the structure of feasible computations. In *Proceedings of the 24th IEEE Symposium on the Foundations of Computer Science*, pages 439–445, 1983.

[7] J. M. Hitchcock. *Effective Fractal Dimension: Foundations and Applications*. PhD thesis, Iowa State University, 2003.

[8] J. M. Hitchcock. Small spans in scaled dimension. In *Proceedings of the 19th IEEE Conference on Computational Complexity*, 2004. To appear.

[9] J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. Scaled dimension and nonuniform complexity. *Journal of Computer and System Sciences*. To appear. Preliminary version appeared in *Proceedings of the 30th International Colloquium on Automata, Languages, and Programming*, pages 278–290, 2003.

[10] J. M. Hitchcock and N. V. Vinodchandran. Dimension, entropy rates, and compression. In *Proceedings of the 19th IEEE Conference on Computational Complexity*, 2004. To appear.

[11] J.M. Hitchcock and E. Mayordomo. Base invariance of feasible dimension. Manuscript, 2003.

[12] D. T. Huynh. Resource-bounded Kolmogorov complexity of hard languages. In *Structure in Complexity Theory*, pages 184–195, Berlin, 1986. Springer-Verlag.

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

[14] D. W. Juedes and J. H. Lutz. Completeness and weak completeness under polynomial-size circuits. *Information and Computation*, 125(1):13–31, 1996.

[15] A. N. Kolmogorov. Three approaches to the quantitative definition of 'information'. *Problems of Information Transmission*, 1:1–7, 1965.

[16] L. A. Levin. Randomness conservation inequalities; information and independence in mathematical theories. *Information and Control*, 61:15–37, 1984.

[17] M. Li and P. M. B. Vitányi. *An Introduction to Kolmogorov Complexity and its Applications*. Springer-Verlag, Berlin, 1997. Second Edition.

[18] W. Lindner. On the polynomial time bounded measure of one-truth-table degrees and p-selectivity, 1993. Diplomarbeit, Technische Universität Berlin.

[19] L. Longpré. *Resource Bounded Kolmogorov Complexity, a Link Between Computational Complexity and Information Theory*. PhD thesis, Cornell University, 1986. Technical Report TR-86-776.

[20] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44(2):220–258, 1992.

[21] J. H. Lutz. Dimension in complexity classes. *SIAM Journal on Computing*, 32:1236–1259, 2003.

[22] M. Sipser. A complexity-theoretic approach to randomness. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 330–335, 1983.

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'