Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 28 (2025)

# One-Way Functions and Polynomial Time Dimension

Satyadev Nandakumar[1], Subin Pulari[2], Akhil S[1], and Suronjona Sarma[1]

[1] Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur, Uttar Pradesh, India.
[1]{satyadev,akhis,suronjona}@cse.iitk.ac.in
[2] Université de Bordeaux, CNRS, Bordeaux INP, LaBRI, UMR 5800, F-33400, Talence, France
[2]subin.pulari@labri.fr

**Abstract**

This paper demonstrates a duality between the non-robustness of polynomial time dimension and the existence of one-way functions. Polynomial-time dimension (denoted $\mathrm{cdim_P}$) quantifies the density of information of infinite sequences using polynomial time betting algorithms called $s$-gales. An alternate quantification of the notion of polynomial time density of information is using polynomial-time Kolmogorov complexity rate (denoted $\mathcal{K}_{\mathrm{poly}}$). Hitchcock and Vinodchandran (CCC 2004) showed that $\mathrm{cdim_P}$ is always greater than or equal to $\mathcal{K}_{\mathrm{poly}}$. We first show that if one-way functions exist then there exists a polynomial-time samplable distribution with respect to which $\mathrm{cdim_P}$ and $\mathcal{K}_{\mathrm{poly}}$ are separated by a uniform gap with probability 1. Conversely, we show that if there exists such a polynomial-time samplable distribution, then (infinitely-often) one-way functions exist.

Using our main results, we solve a long standing open problem posed by Hitchcock and Vinodchandran (CCC 2004) and Stull under the assumption that one-way functions exist. We demonstrate that if one-way functions exist, then there are individual sequences $X$ whose poly-time dimension strictly exceeds $\mathcal{K}_{\mathrm{poly}}(X)$, that is $\mathrm{cdim_P}(X) > \mathcal{K}_{\mathrm{poly}}(X)$. The corresponding unbounded notions, namely, the constructive dimension and the asymptotic lower rate of unbounded Kolmogorov complexity are equal for every sequence. Analogous notions are equal even at the polynomial space and finite-state levels. In view of these results, it is reasonable to conjecture that the polynomial-time quantities are identical for every sequence and set of sequences. However, under a plausible assumption which underlies modern cryptography - namely the existence of one-way functions, we *refute* the conjecture thereby giving a negative answer to the open question posed by Hitchcock, Vinodchandran and Stull. Further, we show that the gap between these quantities can be made as large as possible (*i.e.* close to 1). We also establish similar bounds for strong poly-time dimension versus asymptotic upper Kolmogorov complexity rates. Our proof uses several new constructions and arguments involving probabilistic tools such as the Borel-Cantelli Lemma, the Kolmogorov inequality for martingales and the theorem on universal extrapolation by Ilango, Ren, and Santhanam (implicit in Impagliazzo and Levin 1990). This work shows that the question of *non-robustness* of polynomial-time information density notions, which is *prima facie* different, is intimately related to questions which are of current interest in cryptography and *meta-complexity*.



ISSN 1433-8092

# Contents

# 1 Introduction

## 1.1 Context and Motivation

**One-way functions** [DH76, Gol01, Lev03] are functions on finite strings that are easy to compute but are hard to invert, except possibly on a negligible fraction of the input strings of a given length. The concept of a one-way function is central in cryptography, since the existence of such functions are both necessary and sufficient for the existence of essential cryptographic primitives like pseudo-random generators [HILL99], digital signatures [Rom90], private key encryption [HILL99] [GM84], authentication schemes [FS90] and commitment schemes [Nao91]. The question of existence of one-way functions based on average case hardness of NP-complete problems has been one that has been central in cryptography.

Recent advancements in meta-complexity reveal intriguing connections between existence of one-way functions and the computational hardness of problems studied in meta-complexity. Characterisations of existence of one-way functions have been studied based on average case hardness of time bounded Kolmogorov complexity [LP20], average case hardness of McKTP [ACM+21], average-case hardness of approximating Kolmogorov complexity on samplable distributions [IRS22], average case failure of symmetry of information [HIL+23], average-case easiness of approximating pKt complexity [HLO24], and NP-hardness of distributional Kolmogorov complexity under randomized polynomial-time reductions [Hir23].

In this paper, we show that the existence of one-way functions implies the existence of dimension gaps on polynomial time samplable distributions over infinite sequences. Furthermore, we show that existence of such distributions implies existence of infinitely often one way functions. Using this result, we give a surprising conditional negative resolution to the longstanding open question of the robustness of polynomial-time dimension posed by Hitchcock, Vinodchandran, and Stull [HV06, Stu20].

Polynomial-time dimension quantifies the asymptotic rate of information in an infinite sequence of bits. There are several approaches towards defining polynomial time dimension. The first approach analyzes the asymptotic *compressibility* of the finite prefixes of the given infinite sequence. The polynomial-time bounded *Kolmogorov Complexity* of a string $x$ is the length of the shortest program that can output $x$ in at most polynomial number of time steps. In the *compressibility* approach, the polynomial time density of information is defined in terms of the polynomial-time bounded Kolmogorov complexity of the prefixes of the string, denoted $\mathcal{K}_{\text{poly}}$. In contrast, we can also use the *gambling based* approach to quantify polynomial-time density of information. Polynomial-time dimension, denoted $\dim_{\text{P}}$, is defined using polynomial-time betting algorithms known as $s$-gales. These algorithms attempt to achieve profit by placing successive bets on the bits of the sequence. Each bet made by the $s$-gale on a symbol reflects its confidence in the occurrence of that corresponding symbol.

In this work, we initiate a line of investigation into the connection between cryptographic primitives and the *robustness* of complexity notions of infinite sequences. We consider polynomial time samplable distribution $\nu$ over $\Sigma^\infty$. We show that the existence of one-way functions implies dimension gaps between $\dim_{\text{P}}$ and $\mathcal{K}_{\text{poly}}$ over a collection of sequences in $\Sigma^\infty$, such that the collection has probability 1 according to a polynomial time samplable distribution. Futhermore, we show that the existence of such distributions with dimension gaps implies the existence of infinitely-often one-way functions.

Formally establishing the connection between the robustness of these information density notions and one-way functions in the *infinite string* setting requires significant technical effort and new insights, extending beyond the well-known relationships between compressibility and indistin-

guishability [HILL99] [Yao82] [KC00] in the setting of finite strings .

### 1.2 Applications

Considerable research has been devoted to understanding whether fundamental properties of unbounded Kolmogorov complexity survive in the time bounded setting. Recently, it was shown that the symmetry of information of time-bounded Kolmogorov complexity is equivalent to the existence of OWFs [HIL+23]. Along similar lines, we investigate whether the characterization of constructive dimension in terms of Kolmogorov complexity [Lut03a, May02] survives in the time bounded setting. This is the question of *robustness of polynomial-time dimension* was posed by Hitchcock and Vinodchandran [HV04, HV06], and later mentioned in a survey by Stull (see Open Question 3.71 in [Stu20]). As an application of our main result, we provide a surprising negative resolution to this longstanding open question, under the assumption that one-way functions exist.

The unbounded analogue of time-bounded dimension is known to be robust with markedly different approaches to its definition - via predictors, via unbounded time $s$-gales, and via unbounded Kolmogorov complexity rates - all known to be equivalent [May02] [Lut03a]. At the other extreme, *finite-state* analogues of these notions are also known to be robust. Hitchcock and Vinodchandran [HV04] show that the polynomial-dimension of every sequence is at least the asymptotic lower density of the polynomial-time Kolmogorov complexity of its prefixes. Given the robustness at other levels and the fact that the inequality holds in one direction, it is natural to conjecture that the inequality holds in the other direction as well. This would establish the robustness of polynomial time dimension. However, the question of robustness of dimension at the important "intermediate" resource-bounded level of polynomial time dimension, has remained open for a long time.

Using our main theorem, we establish that the existence of one-way functions implies dimension gaps over a *suitable collection* of sequences. Thus, we show that polynomial time dimension of sets is non-robust if one-way functions exist. We then extend this result to show the stronger result that polynomial time dimension of sequences is non-robust if one-way functions exist. Furthermore, we show that the gap between $\mathcal{K}_{\text{poly}}$ and $\dim_{\text{P}}$ can be arbitrarily close to 1. Additionally, we show that *strong* polynomial time-bounded dimension is also non-robust under the same assumption.

The study of *meta-complexity* - the complexity of computing various measure in complexity theory has been shown to have close connections to cryptographic notions. Our work broadens the scope of this connection. Our main results establish that the study of polynomial-time dimension and, more generally, information-theoretic complexity notions of *infinite sequences* is closely connected with the existence of fundamental primitives in complexity and cryptography. In doing so, we also provide an unexpected resolution to a long-standing open problem.

### 1.3 Technical Background

#### s-gales and Kolmogorov Complexity

**$s$-gales** are betting strategies on infinite sequences. The betting game on an infinite binary sequence $X \in \Sigma^\infty$ can be understood as follows. The player starts with an initial capital of $d(\lambda) = 1$ on the empty string. Here $d$ is the betting function (capital) of the $s$-gale. At the $n^{\text{th}}$ stage, having accumulated a capital $d(x_1x_2 \dots x_n)$ on the first $n$ bits of the sequence, the player is allowed to place an amount as a "bet" on the next bit $x_{n+1}$ of the sequence. The rule of the game is that the expected value of capital received by the player after the bet is $2^s$ times the capital they started with, that is $2^s.d(w) = d(w0) + d(w1)$, for any finite string $w \in \Sigma^*$. The player $d$ succeeds on the sequence $X \in \Sigma^\infty$ if they can secure an arbitrary amount of capital over the course of betting on

the infinite sequence, more precisely if $\limsup_{n\to\infty} d(x_1x_2\ldots x_n) = \infty$. More generally, if $d$ satisfies $2^s.d(w) \geq d(w0) + d(w1)$ we refer to $d$ as an *$s$-supergale*.

When $s = 1$, the average capital after the bet on $w0$ or $w1$ is equal to the previous capital $d(w)$ (when $s = 1$, an $s$-gales is referred to as a *martingale*[1]). Therefore, the betting strategy is fair. When $s < 1$, the average capital after the bet of an $s$-gale is strictly less than the previous capital $d(w)$. Therefore, such betting strategies are inherently unfair to the player. When $s = 1$, the player can bet "evenly" on the next bit if they are unsure. But as $s$ decreases, the setting becomes more unfavorable and the player needs to bet more aggressively to keep increasing their capital.

The **Kolmogorov Complexity** of a finite string $x$, denoted by $K(x)$, is the length of the shortest program that produces the string as the output. Any string $x$ can be produced by a program that trivially outputs the string $x$, and therefore the Kolmogorov complexity of a string $x$ is less than or equal to its length, up to an additive constant. However, if the string has lesser amount of information, there may be programs of shorter length that outputs it. For instance, if all the even bits of the string are 0, the program needs to encode only the bits at the odd indices to produce the string. Therefore, its Kolmogorov complexity is at most half its length, up to additive constants.

### Polynomial-time Dimension

**Resource bounded dimension** is defined by placing resource bounds on the computation of the $s$-gale. Analogously, resource bounded Kolmogorov complexity is defined by placing resource bounds on the programs that can print a string.

The **Polynomial time dimension** quantifies the rate of information in an infinite sequence, measured with respect to polynomial time bounded computation. It is formulated using polynomial time $s$-gales. An $s$-gale $d$ wins on an infinite sequence $X$ if $\limsup_{n\to\infty} d(X \upharpoonright n) = \infty$. Let $S^\infty(d)$ denotes the set of sequences on which $d$ succeeds. $d$ is said to be polynomial-time computable if for some $p(n) \in \text{poly}(n)$, $d$ takes at most $p(n)$ time to compute $d(w)$, where $n$ is the length of $w$.

**Definition** (Polynomial-time dimension [Lut03a])**.** *The polynomial-time dimension of $\mathcal{F} \subseteq \Sigma^\infty$ is defined as*

$$\dim_P(\mathcal{F}) = \inf\{s \mid \exists \text{ a polynomial-time } s\text{-gale } d \text{ such that } \mathcal{F} \subseteq S^\infty(d)\}.$$

*For a sequence $X \in \Sigma^\infty$, define* $\dim_P(X) = \dim_P(\{X\})$.

That is $\dim_P(X)$ is the "lowest" $s$ for which there exists a polynomial time $s$-gale $d$ that succeeds on $X$.

### Time bounded Kolmogorov Complexity

On the other hand, we can use *time bounded* Kolmogorov complexity to define a polynomial time analogue of $\mathcal{K}$. For a given time bound $t(n)$, the **$t$-time bounded Kolmogorov complexity** $K_t(x)$ of a string $x$ is the length of the shortest program that generates $x$ in at most $t(|x|)$ time steps (see [LV08]).

For a given time bound $t(n)$, the quantity $\liminf_{n\to\infty} K_t(X \upharpoonright n)/n$ gives the $t$-time bounded rate of information in an infinite string $X$. The polynomial time analogue of $\mathcal{K}$ is the infimum of this quantity over all polynomial time bounds $t$.

[1] When $s = 1$, an $s$-supergale is referred to as a *supermartingale*.

**Definition** ([HV04, HV06]). *For any* $\mathcal{F} \subseteq \Sigma^\infty$,

$$\mathcal{K}_{\text{poly}}(\mathcal{F}) = \inf_{t \in \text{poly}} \sup_{X \in \mathcal{F}} \liminf_{n \to \infty} \frac{K_t(X \upharpoonright n)}{n}.$$

## Robustness of Dimension

### Robustness at other levels

In the classical setting, we use the notion of $\mathcal{K}$ defined using time-unbounded Kolmogorov complexity $K(x)$ and cdim defined using lower semi-computable $s$-gales. Mayordomo [May02] and Lutz [Lut03b] show that the unbounded notions of $\mathcal{K}$ and cdim are equivalent, hence establishing the robustness of *constructive* dimension.

**Theorem 1.1** (Mayordomo [May02] , Lutz [Lut03b]). *For all* $\mathcal{F} \subseteq \Sigma^\infty$, $\text{cdim}(\mathcal{F}) = \sup_{X \in \mathcal{F}} \liminf_{n \to \infty} \frac{K(X \upharpoonright n)}{n}$.

PSPACE analogues of cdim and $\mathcal{K}$ are defined by restricting the $s$-gales in the definition of cdim to be polynomial space computable and by using polynomial space bounded Kolmogorov complexity in the definition of $\mathcal{K}$. Hitchcock [Hit03] showed that these notions of resource bounded dimension coincide in the PSPACE setting, hence establishing the robustness of *polynomial-space* dimension.

**Theorem 1.2** ([Hit03]). *For every* $\mathcal{F} \subseteq \Sigma^\infty$, $\text{cdim}_{\text{PSPACE}}(\mathcal{F}) = \mathcal{K}_{\text{PSPACE}}(\mathcal{F})$.

### Robustness of Polynomial time Dimension

This leads to the following question: *Are the notions of polynomial time dimension formulated using s-gales (*$\dim_{\text{P}}$*) and time bounded Kolmogorov complexity (*$\mathcal{K}_{\text{poly}}$*) equivalent?.*

Hitchcock and Vinodchandran [HV06] showed that $\dim_{\text{P}}$ is always greater than or equal to $\mathcal{K}_{\text{poly}}$[2].

**Theorem 1.3** ([HV04, HV06]). *For every* $\mathcal{F} \subseteq \Sigma^\infty$, $\mathcal{K}_{\text{poly}}(\mathcal{F}) \leq \dim_{\text{P}}(\mathcal{F})$.

The question whether the reverse inequality holds has remained elusive. Hitchcock and Vinodchandran [HV04, HV06] and later Stull in [Stu20] posed the following open question:

**Question 1.1** ([HV04, HV06, Stu20]). *Is it true that, for every sequence* $X \in \Sigma^\infty$

$$\dim_{\text{P}}(X) = \mathcal{K}_{\text{poly}}(X) \ ?$$

### Polynomial-time Strong Dimension

**Polynomial-time strong dimension** is a dual notion of polynomial time dimension ([AHLM07], see also [Stu20]). As in the case of polynomial time dimension, there exist two notions, one defined using $s$-gales and the other defined in terms of time bounded Kolmogorov complexity. An $s$-gale $d$ strongly succeeds on an infinite sequence $X$ if $\liminf_{n \to \infty} d(X_1 X_2 \ldots X_n) = \infty$. Let $S^\infty_{str}(d)$ denotes the set of sequences on which $d$ succeeds strongly.

[2] See Section 11 for alternate proofs of Theorems 1.3 and 1.4.

**Definition** (Polynomial-time strong dimension [AHLM07, Stu20])**.** *The polynomial-time strong dimension of $\mathcal{F} \subseteq \Sigma^\infty$ is defined as*

$$\mathrm{Dim_P}(\mathcal{F}) = \inf\{s \mid \exists \text{ a polynomial-time } s\text{-gale } d \text{ such that } \mathcal{F} \subseteq S^\infty_{str}(d)\}.$$

*For a sequence $X \in \Sigma^\infty$, define* $\mathrm{Dim_P}(X) = \mathrm{Dim_P}(\{X\})$.

The strong dimension analogue of $\mathcal{K}_{\mathrm{poly}}$ is defined by replacing the lim inf in the definition of $\mathcal{K}_{\mathrm{poly}}$ with lim sup.

**Definition** ([HV04, HV06])**.** *For any $\mathcal{F} \subseteq \Sigma^\infty$,*

$$\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\mathcal{F}) = \inf_{t \in \mathrm{poly}} \sup_{X \in \mathcal{F}} \limsup_{n \to \infty} \frac{K_t(X \upharpoonright n)}{n}.$$

Similar to the conclusion of Theorem 1.3, $\mathrm{Dim_P}$ is always greater than or equal to $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}$.

**Theorem 1.4** ([HV04, HV06])**.** *For every $\mathcal{F} \subseteq \Sigma^\infty$, $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\mathcal{F}) \leq \mathrm{Dim_P}(\mathcal{F})$.*

Stull in [Stu20] posed the following question: *Are the notions of polynomial time strong dimension formulated using s-gales ($\mathrm{Dim_P}$) and time bounded Kolmogorov complexity ($\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}$) equivalent?.*

### Polynomial time samplable distributions on infinite sequences

We generalize the notion of polynomial time samplable distributions [IRS22, HIL+23, LP20] to probability distributions on the space of infinite sequences (see Section 2.8 for formal definitions).

Let $\nu$ be a probability measure over $\Sigma^\infty$. For every $n$, let $\nu_n(w) = \nu(X \in \Sigma^\infty : w \sqsubseteq X)$[3] denote the probability distribution induced by $\nu$ on $\Sigma^n$. Now, we define polynomial time samplable distributions on $\Sigma^\infty$.

**Definition 1.1.** *A probability distribution $\nu$ over $\Sigma^\infty$ is polynomial time samplable if there exists a probabilistic polynomial time Turing machine $M$ that uses $q(n)$ random bits, where $q$ is a polynomial, such that for every $n$ and $w \in \Sigma^n$, $\Pr_{r \sim \Sigma^{q(n)}}[M(1^n, r) = w] = \nu_n(w)$*[4].

One-way functions are secure against inversion by probabilistic polynomial time adversaries. However, polynomial time gales are defined in terms of computation using deterministic machines. In order to bridge this gap, we define martingales and $s$-gales that are approximable using probabilistic polynomial-time machines. Probabilistically approximable martingales were studied in [RS98]. However, for our purposes, we require only a weaker variant of gales that admit fully polynomial-time randomized approximation schemes (FPRAS), as defined in [RS98].

**Definition 1.2.** *Let $d : \Sigma^* \to [0, \infty) \cap \mathbb{Q}$ be an $s$-supergale and $\nu$ be any probability distribution over $\Sigma^\infty$. $d$ is $t(n)$-time $\nu$-approximable if for every constant $k$ there exist a probabilistic $t(n)$-time machine $M$ and constant $c < 1$ such that for every $n$, $\{w \in \Sigma^n : M(w) \notin [c \cdot d(w), d(w)]\} \subseteq \mathrm{supp}(\nu_n)$ and $\nu_n\{w \in \Sigma^n : M(w) \notin [c \cdot d(w), d(w)]\} \leq n^{-k}$.*

In the above, $\mathrm{supp}(\nu_n)$ denotes the support of the distribution $\nu_n$, i.e. $\mathrm{supp}(\nu_n) = \{w \in \Sigma^n : \nu_n(w) > 0\}$. A supergale $d$ is $\nu$-approximable if the set of strings at which the algorithm $M$ makes an error in approximating $d(w)$ up to a constant multiplicative factor lies within the support of $\nu_n$, and the measure of the set of such strings according to $\nu_n$ is bounded by an inverse polynomial function.

[3] $\sqsubseteq$ denotes the prefix operator

[4] An alternate way of defining polynomial time samplable distributions on $\Sigma^\infty$ is the following: $\nu = \{\nu_n\}$ is a *polynomial time samplable distribution on* $\Sigma^\infty$ if $\{\nu_n\}$ is a *polynomial time samplable distribution* (in the sense of [IRS22, HIL+23, LP20]) such that for any $w \in \Sigma^n$, $\nu_n(w) = \nu_{n+1}(w.0) + \nu_{n+1}(w.1)$. The equivalence of these notions follows using routine measure theoretic arguments.

## 1.4 Our Results

### 1.4.1 One way functions and Dimension gaps

Our main result (Theorem 1.5) shows that the existence of one-way functions implies the existence of uniform dimension gaps between $\dim_P$ and $\mathcal{K}_{\text{poly}}$ over a collection of sequences in $\Sigma^\infty$, such that the collection has probability 1 according to a polynomial time samplable distribution. Futhermore we show that such a distribution implies existence of infinitely often one way functions.

**Theorem 1.5.** *In the following, (1) $\implies$ (2) $\implies$ (3):*

1. *One-way functions exist.*
2. *For every $s < \frac{1}{2}$, there exists a polynomial-time samplable distribution $\nu$ over $\Sigma^\infty$ such that:*
   (a) *$\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq s$ for almost every $X \sim \nu$.*
   (b) *For every $s' \in (s, \frac{1}{2})$ and every polynomial-time $\nu$-approximable $s'$-supergale $d$, we have*
   $$\nu(S^\infty(d)) = 0.$$
3. *Infinitely-often one-way functions exist*[5].

The existence of polynomial-time samplable distributions satisfying the condition 1 implies that, with probability 1 according to $\nu$, the polynomial-time Kolmogorov complexity $\mathcal{K}_{\text{poly}}(X)$ of $X \in \Sigma^\infty$ is at most $s$. We later show in the proof of Lemma 1.7 that the polynomial-time constructive dimension $\dim_P(X)$ of almost every such sequence is at least $1/2$. Since $s < 1/2$, this establishes the existence of a dimension gap on a probability 1 set according to $\nu$.

### 1.4.2 Applications

As an application of Theorem 1.5, we show that if one-way functions exist then equality does not hold between $\dim_P$ and $\mathcal{K}_{\text{poly}}$ for sets $\mathcal{F} \subseteq \Sigma^\infty$. To show this, we prove the contrapositive statement that if the equality holds, then one-way functions do not exist.

**Theorem 1.6.** *If for all $\mathcal{F} \subseteq \Sigma^\infty$,*

$$\dim_P(\mathcal{F}) = \mathcal{K}_{\text{poly}}(\mathcal{F}),$$

*then one-way functions do not exist.*

We then show the stronger result that if one-way functions exist then then equality does not hold between $\dim_P$ and $\mathcal{K}_{\text{poly}}$ for sequences $X \in \Sigma^\infty$.

**Theorem 1.7.** *If for all $X \in \Sigma^\infty$,*

$$\dim_P(X) = \mathcal{K}_{\text{poly}}(X),$$

*then one-way functions do not exist.*

[5] See the remarks in section 10 regarding infinitely-often one-way functions and polynomial time dimension and also Lemma 10.1.

Thus, conditioned on the existence of one-way functions, we demonstrate the existence of sequences $X$ such that $\mathcal{K}_{\text{poly}}(X) < \dim_{\text{P}}(X)$.

In the last section of the paper we demonstrate how the proof of Theorem 1.7 can be extended to show that if one-way functions exist, then the distance between these quantities can be arbitrarily close to the maximum possible value of 1.

**Theorem 1.8.** *If one-way functions exist, then for any $\epsilon > 0$, there exists $X \in \Sigma^\infty$ such that,*

$$\dim_{\text{P}}(X) - \mathcal{K}_{\text{poly}}(X) \geq 1 - \epsilon.$$

For polynomial time strong dimension, we show that if one-way functions exist, then there exist sequences for which the gap between $\mathcal{K}^{\text{str}}_{\text{poly}}$ and $\text{Dim}_{\text{P}}$ is arbitrarily close to 1.

**Theorem 1.9.** *If one-way functions exist then for any $\epsilon > 0$, there exists $X \in \Sigma^\infty$ such that,*

$$\text{Dim}_{\text{P}}(X) - \mathcal{K}^{\text{str}}_{\text{poly}}(X) \geq 1 - \epsilon.$$

Therefore, we show that if one-way functions exist, the answers to both parts of Open Question 3.71 from [Stu20] are negative.

### 1.5 Techniques

**Proof of Theorem 1.5**: We use a new construction to extend pseudorandom generators to obtain polynomial-time samplable distributions on infinite sequences for which $\mathcal{K}^{\text{str}}_{\text{poly}} \leq s$ almost everywhere (Section 4, Figure 1.6). We use existing standard $s$-gale manipulation techniques (Lemma 5.1 and Lemma 5.2) to convert winning gales on these distributions to martingales that win *quickly* over certain blocks of bits of the input sequence. Using these we show a new technique to build a distinguisher algorithm (Algorithm 2) that breaks the pseudorandom generators used. To show that the distinguisher succeeds with high probability on pseudorandom outputs, we use a argument involving the Borel-Cantelli lemma (Lemma 5.3) to transform the occurrence of infinitely many events into the occurrence over a large fraction, as required for the distinguisher. We use the Kolmogorov Inequality (Lemma 5.5) to show that the distinguisher succeeds with low probability on uniformly random outputs.

For the converse, we use the theorem on *universal extrapolation* by Ilango, Ren and Santhanam (Theorem 20 from [IRS22], see also [IL89, IL90]) along with a gale construction technique.

**Proof of Theorem 1.7**: Non robustness of polynomial-time dimension for sets (Theorem 1.6) follows as a corollary of Theorem 1.5, along with some compactness arguments. However, to extend the argument to show non-robustness of polynomial-time dimension for sequences (Theorem 1.7) requires additional technical effort. We provide a new gale combination technique (Lemma 8.1) to construct a $t(n).n.\log(n)$ $s$-gale that is universal over all $t(n)$-time $s$-gales. We use this along with a measure-based partitioning trick to construct a polynomial time $s$-gale that is universal over all polynomial time $s$-gales (up to a positive measure subset) to prove Theorem 1.7.

### 1.6 Proof Outline

In this section we give an informal account of the proofs of the main results. The full proofs are given in later sections.

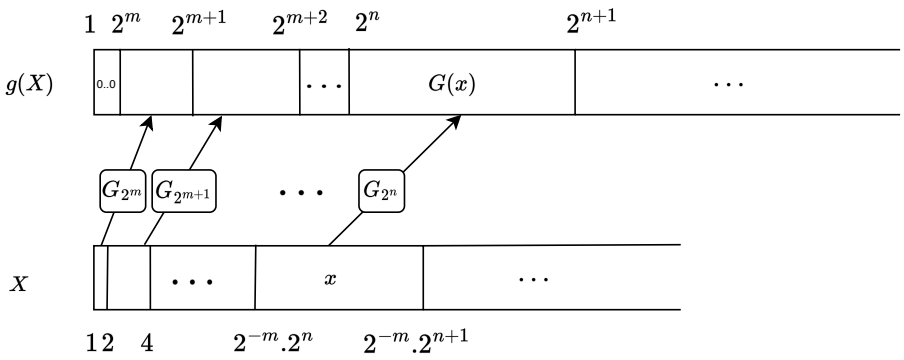


Figure 1: Illustration of the construction of $g(X)$. The first $s = 2^m$ bits of the $g(X)$ are 0. Thereafter, for every for every $n > m$, the block $X[s.2^{n-1}, s.2^n - 1]$ is mapped to $G_{2^{n-1}}(X[s.2^{n-1}, s.2^n - 1])$ in the output string $g(X)$.

**Dimension gaps from one-way Functions**

We first show that one-way functions imply the existence of distributions over which dimension gap exists almost everywhere. Precisely, we show that if one-way functions exist, for any $s < 1/2$, there are polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ samplable using $sn$ bits such that for any $s' \in (s, 1/2)$, any polynomial time $s'$-supergale that is $\nu$-approximable can succeed only on a "small" $\nu$-measure 0 subset of $\Sigma^\infty$. See Section 5 for the formal proof.

**Lemma 1.1.** *If one-way functions exist, then for every $s < 1/2$, there exist a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ such that:*

1. *$\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq s$ for almost every $X \sim \nu$.*
2. *For every $s' \in (s, 1/2)$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.*

**Proof Outline**. We start with the assumption that one-way functions exist. This implies the existence of pseudorandom generators $\{G_n\}_{n\in\mathbb{N}}$ running in time $t(n) \in \text{poly}(n)$ mapping strings of length $sn$ to strings of length $n$ for every $s < 1$ [HILL99]. For the sake of convenience, take any $s$ such that $s = 2^{-m}$ for some $m \in \mathbb{N}$, $m > 1$ (hence $s < 1/4$). We first *extend* the PRG $\{G_n\}_{n\in\mathbb{N}}$ to a mapping between infinite sequences, $g : \Sigma^\infty \to \Sigma^\infty$. We then use $g$ to construct a polynomial time samplable distribution $\nu$ on $\Sigma^\infty$.

The mapping $g$ is constructed as follows. We first define mappings $g_k$ from $\Sigma^k$ to $\Sigma^*$ such that $k = s.2^n$ for some $\in \mathbb{N}$. On an input $w \in \Sigma^k$, where $g_k$ first divides $w$ into blocks $x_n$ of size $s.2^i$ for every $i < n$. Then, for every block $x_i$ in $w$, $g$ applies the appropriate function from $\{G_n\}_{n\in\mathbb{N}}$ to obtain an output block $y_i$ of length $2^i$. Now $g_k(w)$ is defined as the concatenation of blocks $y_i$ for every $i \leq n$. Now, for any $X \in \Sigma^\infty$ we define the function $g$ as the *limit* of the mappings $g_k$, $g(X) = \lim_{k\to\infty} g_k(X \upharpoonright k)$. We abuse the notation and use $g$ instead of $g_k$ when the context is clear. Figure 1.6 gives a detailed illustration of the construction of $g$.

The mapping $g : \Sigma^\infty \to \Sigma^\infty$ naturally generates a polynomial-time samplable distribution $\nu$ over $\Sigma^\infty$. The sampling algorithm $M$ for $\nu$ on input $1^n$, maps a random seed of length $s \cdot 2^{\lceil \log_2(n) \rceil}$ using $g$ to a string of length $2^{\lceil \log_2(n) \rceil}$, and thereafter trims the output to $n$ bits. The number of random bits used by $M$ on input $1^n$ is at most $2s \cdot n$. We show that $\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq 2s$ for almost every $X \sim \nu$.

Towards building a contradiction, let there exist some $s' \in (2s, 1/2)$ and a polynomial-time $\nu$-approximable $s'$-supergale $d'$ such that $\nu(S^{\infty}(d')) > 0$. We show that $d'$ can be used to break the PRG $\{G_n\}_{n\in\mathbb{N}}$, obtaining a contradiction.

Using standard techniques on gales, we convert the polynomial time $\nu$-approximable $s'$-supergale $d'$ to a polynomial-time $\nu$-approximable martingale $\tilde{d}$ that gains a *significant* amount of money over blocks of length $2^n$ for infinitely many $n$. More precisely, for some $\tilde{s} \in (2s', 1)$, for all $Y \in g(\Sigma^{\infty})$, there exist infinitely many $n \in \mathbb{N}$ such that

$$\tilde{d}(Y \upharpoonright 2^{n+1}) > 2^{(1-\tilde{s})2^n}\tilde{d}(Y \upharpoonright 2^n). \tag{1}$$

Let $M$ be the Turing machine that $\nu$-approximates $\tilde{d}$. That is for all $n \in \mathbb{N}$, $\nu_n\{w \in \Sigma^n : M(w) \notin [\mathbf{c} \cdot d(w), d(w)]\} \leq n^{-k}$ where $\mathbf{c} \in \mathbb{Q}, k \in \mathbb{N}$ are constants such that $\mathbf{c} \leq 1$ and $k \geq 1$. We use $M$ to build a distinguisher algorithm $A$ that breaks the PRG $\{G_n\}$. We describe the behavior of $A$ on inputs of length $2^n$. Let $w$ be an input of size $2^n$. The distinguisher randomly chooses $s.2^n$ bits $r$ and takes $w' = g(r)$. Now $A$ outputs 1 if and only if:

$$M(w'w) \geq \mathbf{c} \cdot 2^{(1-\tilde{s})|w|} \cdot M(w').$$

Otherwise $A$ outputs 0. Since $M$ is polynomial time computable, $A$ is a polynomial time algorithm.

To show that $A$ breaks the PRG $\{G_n\}_{n\in\mathbb{N}}$, it suffices to show that for infinitely many $n \in \mathbb{N}$, taking $N = 2^n$, $|\Pr_{x\sim\Sigma^{s.N}}[A(g(x)) = 1] - \Pr_{w\sim\Sigma^N}[A(w) = 1]| > N^{-c}$ for some constant $c$.

We first analyse the behaviour of $A$ on inputs of the PRG $\{G_n\}$. We have shown that $\tilde{d}$ satisfies the condition (1) over $Y \in g(\Sigma^{\infty})$ for infinitely many $n$. But the *fraction* of strings of a particular length $n$ satisfying (1) may in fact be negligible. In order to overcome this difficulty, we use an argument involving the Borel Cantelli Lemma to show that there exist infinitely many $n \in \mathbb{N}$, such that over at least a $1/n^2$ fraction of strings $w \in \Sigma^{s.2^n}$,

$$\tilde{d}(g(w)) > 2^{(1-\tilde{s})2^n}\tilde{d}(g(w) \upharpoonright 2^{n-1})). \tag{2}$$

Let $n+1$ be one of the lengths at which the condition 2 holds. Let $w, w' \in \Sigma^{2^n}$ such that $w = G_{2^n}(x)$ for some $x \in \Sigma^{s.2^n}$ and $w' = g(r)$ for some $r \in \Sigma^{s.2^n}$.

In order for the condition $M(w'w) \geq \mathbf{c} \cdot 2^{(1-\tilde{s})|w|} \cdot M(w')$ to hold, it suffices that $\tilde{d}(w'w) \geq 2^{(1-\tilde{s})|w|} \cdot \tilde{d}(w')$ and $M(w'w) \geq \mathbf{c} \cdot \tilde{d}(w'w)$ and $M(w) \leq \tilde{d}(w)$. From the argument given above, it follows that the first condition holds with probability at least $(n+1)^{-2}$. Since $\tilde{d}$ is $\nu$-approximable, it follows that the second and third conditions hold with probability at least $1 - 2^{-(kn-1)}$ for some constant $k$.

Therefore it follows that for infinitely many n,

$$\Pr_{(x,r)\sim\Sigma^{s\cdot 2^n}\times\Sigma^{s\cdot 2^n}}[A(G_{2^n}(x), r)) = 1] \geq \frac{1}{(n+1)^2} - \frac{1}{2^{kn}}. \tag{3}$$

We now analyze the behaviour of $A$ on uniformly random inputs. We use the Kolmogorov inequality for supermartingales to show that this is inverse exponentially small in input size.

We need an upper bound on the number of strings $w, r \in \Sigma^{2^n}$ such that $A(w, r) = 1$. This happens when $M(w'w) \geq \mathbf{c} \cdot 2^{(1-\tilde{s})|w|} \cdot M(w')$. Using the Kolmogorov inequality for martingales, we show that for a fixed $w'$, the fraction of strings $w \in \Sigma^{2^n}$ such that $\tilde{d}(w'w) \geq \mathbf{c}^2 \cdot 2^{|w|(1-\tilde{s})}.\tilde{d}(w')$ is less than $\mathbf{c}^{-2} \cdot 2^{-|w|(1-\tilde{s})}$. For the remaining set of strings, we have that $\tilde{d}(w'w) < \mathbf{c}^2 \cdot 2^{2^n(1-\tilde{s})}.\tilde{d}(w')$. If we have that $M(w'w) \leq \tilde{d}(w'w)$ and $M(w') \geq \mathbf{c} \cdot \tilde{d}(w')$, it follows that $A(w, r) = 0$. Using the

fact that $\tilde{d}$ is $\nu$-approximable, we show the following that for some constant $k$, for all $n \in \mathbb{N}$, taking $N = 2^n$,

$$\Pr_{w\sim\Sigma^N}\Pr_{r\in\Sigma^{s\cdot N}}[A(w,r)=1] < \frac{1}{\mathbf{c}^2\cdot 2^{N(1-\hat{s})}} + \frac{1}{N^k} + \frac{1}{2^{N(1-s)}}. \tag{4}$$

From Equation 3 and 4, it follows that $A$ breaks the PRG $\{G_n\}$, which is a contradiction.

**Infinitely often one-way functions from dimension gaps**

We now give a proof outline that the existence of distributions over which dimension gap exists almost everywhere implies existence of infinitely often one-way functions. See Section 6 for the formal proof.

**Lemma 1.2.** *If there exist an $s < 1$ and a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ such that:*

1. *$\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq s$ for almost every $X \sim \nu$.*
2. *There exist some $\hat{s} \in (s, 1]$ such that for every $s' \in (s, \hat{s})$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.*

*Then, infinitely-often one-way functions exist.*

**Proof Outline**. We start with the hypothesis that for some $s < 1$ there exist a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ such that $\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq s$ for almost every $X \sim \nu$ and there exists $\hat{s} \in (s, 1]$ such that for every $s' \in (s, \hat{s})$ and polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$. Assume that there exist no infinitely often one-way functions.

Fix arbitrary $s'$ and $s'''$ such that $s < s' < s'''' < \hat{s}$, $2^{s'} \in \mathbb{Q}$ and $2^{s'''} \in \mathbb{Q}$. Consider the function $d : \Sigma^* \to [0, \infty)$ defined as $d(w) = 2^{s''''|w|}\nu(w)$. We show that $d$ is an $s'''$-supergale that satisfies,

$$\nu\left\{X \in \Sigma^\infty : \limsup_{n\to\infty} d(X \upharpoonright n) = \infty\right\} > 0.$$

We now show that if infinitely-often one-way functions do not exist, there exists a randomized polynomial time algorithm $M$ that $\nu$-approximates $d$. Using a theorem on *universal extrapolation* by Ilango, Ren and Santhanam (Theorem 20 from [IRS22], implicit in [IL89, IL90]), it follows that for any $q \geq 1$, there exists a probabilistic polynomial time algorithm $\mathcal{A}$ and constant $c < 1$ such that for all $n$,

$$\Pr_{w\sim\nu_n}[c\cdot\nu_n(w) \leq \mathcal{A}(w) \leq \nu_n(w)] \geq 1 - O\left(\frac{1}{n^q}\right).$$

Furthermore, since there infinitely-often one-way functions do not exist (and therefore weak infinitely-often one-way functions do not exist), there is an algorithm $\mathcal{I}$ which *inverts* the function $f : \Sigma^* \to \Sigma^*$ defined as

$$f(x) = M(1^{|x|^{1/c'}}, x)$$

on all but finitely many input lengths $n$. We combine the algorithms $\mathcal{A}$ and $\mathcal{I}$ to give an algorithm $M$ satisfying the following properties: for every $n$, $\{w : M(w) \notin [c\cdot d(w), d(w)]\} \subseteq \text{supp}(\nu_n)$ and

$$\Pr_{x\sim\nu_n}[c\cdot d(x) \leq M(x) \leq d(x)] \geq 1 - O\left(\frac{1}{n^q}\right).$$

Using the fact that $\mathcal{A}$ and $\mathcal{I}$ are randomized polynomial time algorithms and $q$ is arbitrary we show that $M$ approximates $\nu$ in polynomial time. Since this contradicts our hypothesis, it must be the case that there exist infinitely-often one-way functions.

**Dimension gaps over sequences from one-way functions**

We use Lemma 1.1 to show that if one-way functions exist then there exists sequences $X$ for which $\mathcal{K}_{\text{poly}}(X)$ and $\dim_{\text{P}}(X)$ are separated by a gap of $1/2$. Thereafter we refine our proof to increase the gap to any value arbitrarily close to 1. The corresponding theorems for sets is trivially implied by considering the set $\mathcal{F} = \{X\}$.

**Theorem 1.7.** *If for all $X \in \Sigma^\infty$,*

$$\dim_{\text{P}}(X) = \mathcal{K}_{\text{poly}}(X),$$

*then one-way functions do not exist.*

**Proof Outline.** We start with the assumption that one-way functions exist. From Lemma 1.1, for every $s < 1/2$ there exist a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ and polynomial $t$ such that:

1. The number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$.
2. For every $s' \in (s, 1/2)$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.

Consider the following set $\mathcal{F} = \bigcap_{n \geq 1} \bigcup_{w \in \text{supp}(\nu_n)} C_w$. Using an argument involving the compactness of $\Sigma^\infty$ as a topological space, we demonstrate that $\mathcal{F}$ is a non-empty set such that $\nu(\mathcal{F}) = 1$. Since the number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$, $\mathcal{K}_{\text{poly}}(X) \leq s$ for every $X \in \mathcal{F}$. For the sake of contradiction, assume that there exist $s' \in (s, 1/2)$ such that $\dim_{\text{P}}(X) < s'$ for every $X \in \mathcal{F}$. So, every $X \in \mathcal{F}$ there exists an exact computable $s'$-gale $d'_X$ that runs in time $t_{d'_X}(n) \in \text{poly}(n)$, such that $d'_X$ succeeds on $X$.

We now use a partitioning trick to build a set $\mathcal{S} \subseteq \Sigma^\infty$ such that $\nu(\mathcal{S}) > 0$. Thereafter we use a new gale combination technique to construct a $n^{k+c}$-time computable $s'$-gale $d'$ that succeeds on all sequences in $\mathcal{S}$. Since $d$ is polynomial-time computable, $d$ is trivially a polynomial-time $\nu$-approximable $s'$-supergale. Now, since we know that $\nu(S^\infty(d)) \geq \nu(\mathcal{S}) > 0$, we obtain a contradiction. Hence, it must be the case that there exist a sequence $X \in \mathcal{F}$ with $\dim_{\text{P}}(X) > s'$. Since $s'$ was arbitrary, the theorem follows.

**Theorem 1.8.** *If one-way functions exist, then for any $\epsilon > 0$, there exists $X \in \Sigma^\infty$ such that,*

$$\dim_{\text{P}}(X) - \mathcal{K}_{\text{poly}}(X) \geq 1 - \epsilon.$$

**Proof Outline.** In order to demonstrate that for every $\epsilon$, there exist sequences $X$ for which the gap between $\dim_{\text{P}}$ and $\mathcal{K}_{\text{poly}}$ is greater than $1 - \epsilon$, we combine the proof techniques in the proofs of Lemma 1.1 and the proof of existence of sequences with gaps close to $1/2$ sketched above. Also, we require an important modification in the construction of the martingale $\tilde{d}$ in the proof of Lemma 1.1. While constructing the martingale $\tilde{d}$ in the proof of Lemma 1.1, we used the assumption that $s' < 1/2$. This is important because in order to obtain the condition $\tilde{d}(Y \upharpoonright 2^{n+1}) > 2^{(1-\tilde{s})2^n} \tilde{d}(Y \upharpoonright 2^n)$ for infinitely many $n$ over any $Y \in g(\Sigma^\infty)$, we require $\tilde{s} > 2s'$. For $\tilde{s}$ to be less than 1, we require $s' < 1/2$. The major tool we need to overcome this hurdle is a generalization of the construction of martingale $\tilde{d}$ to every $s' < 1$ (see Lemma 5.2). We transform $d'$ into a polynomial time martingale $\tilde{d}$ satisfying the following property: let $\tilde{s}$ and $s''$ be such that $\tilde{s} > s'' > s'$. Then for any $Y \in g(\Sigma^\infty)$ there exist infinitely many $n$ satisfying either of the following conditions:

1. $\tilde{d}(Y \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}}\tilde{d}(Y \upharpoonright 2^{n-1})$.
2. There exists $\ell$ satisfying $((\tilde{s} - s'')/s'') \cdot 2^{n-1} \leq \ell \leq 2^{n-1}$ such that $\tilde{d}(Y \upharpoonright 2^{n-1} + \ell) > 2^{(1-s'')(2^{n-1}+\ell)}$.

We need the second condition above to handle the case when $s'$ may be between $1/2$ and 1. Finally, we modify Algorithm A from the proof of Lemma 1.1 to incorporate the second condition above. We adapt the analysis of the algorithm and the arguments involving the Borel Cantelli lemma appropriately to show that the modified algorithm $A$ is a distinguisher for the PRG $\{G_n\}_{n\in\mathbb{N}}$.

### 1.7 Related Work

In [LP20], Liu and Pass proved that one-way functions exist if and only if the *t-time bounded Kolmogorov complexity problem* $\mathrm{MK}^t\mathrm{P}$, is *mildly* hard on average. In a follow-up work [LP21] they define a problem that is NP-complete under randomized reductions whose mild average case hardness is equivalent to existence of one-way functions. Allender, Cheraghchi, Myrisiotis, Tirumala and Volkovich [ACM+21] showed similar results in the setting of KT complexity, basing the existence of one-way functions on the average case hardness of McKTP (an analogue of $\mathrm{McK}^t\mathrm{P}$ for KT-complexity). Hirahara [Hir23] gave the first characterization of a one-way function by worst-case hardness assumptions. He showed that one-way function exists if and only if it is NP-hard to approximate the distributional Kolmogorov complexity under randomized polynomial-time reductions, assuming NP is hard in the worst case. Hirahara, Lu and Oliveira [HLO24] showed the relationship between One-way functions and pKt complexity. Ilango, Ren, and Santhanam [IRS22] characterize the existence of OWFs by the average-case hardness of approximating Kolmogorov complexity on samplable distributions. Hirahara, Ilango, Lu, Nanashima and Oliveira [HIL+23] gave a complete characterization of one-way functions in terms of the average case failure of symmetry of information (and related properties like the conditional coding theorem) for $\mathrm{pK}^t$.

Considerable research has been devoted to understanding whether fundamental properties of unbounded Kolmogorov complexity survive in the time bounded setting. One of the important properties that was studied in this context is the symmetry of information of Kolmogorov complexity [LV08, SUV22, DH10, Nie09]. Longpré and Mocas [LM93] (also Longpré and Watanabe [LW92]) showed that if one-way functions exist then symmetry of information does not hold for time bounded Kolmogorov complexity. In [Hir22] and [GK22], symmetry of information for polynomial time bounded probabilistic Kolmogorov complexity $\mathrm{pK}^t$ (see [GKLO22, LO22]) was derived from the stronger assumption DistNP $\subseteq$ AvgBPP.

This work explores whether the characterization of constructive dimension in terms of Kolmogorov complexity [Lut03a, May02] extends to the time-bounded setting. Our results establish a duality between the separation of $\dim_{\mathrm{P}}$ and $\mathcal{K}_{\mathrm{poly}}$ as notions of polynomial-time dimension over a *sufficiently large collection* of sequences and the existence of one-way functions.

As an application of our main result, we show that if one-way functions exist then polynomial time bounded Kolmogorov complexity does not yield a characterization of polynomial time dimension of infinite sequences, thereby refuting an open question posed by Hitchcock and Vinodchandran in [HV04] and by Stull in [Stu20].

### 1.8 Open Problems

Our findings suggest several promising directions for future research. A key open question is whether weaker hardness assumptions, such as P $\neq$ NP, DistNP $\not\subseteq$ AvgP or DistNP $\not\subseteq$ AvgBPP

can be characterized in terms of the separation of polynomial-time dimension, as defined using time-bounded $s$-gales and time-bounded Kolmogorov complexity in appropriate settings. Specifically, *can these hardness assumptions be equivalently expressed through if-and-only-if statements involving polynomial-time dimension?*.

Our results reveal a duality between the non-robustness of polynomial-time dimension and the existence of one-way functions. An interesting open question is whether notions of polynomial-time randomness-defined via betting algorithms and Kolmogorov incompressibility of prefixes (see [Stu20] for more details) capture equivalent concepts of randomness. Polynomial-time betting algorithms that succeed on specific sequences do not necessarily provide guarantees on the rate of capital accumulation in general. Consequently, investigating the robustness of polynomial-time randomness and its potential connections to cryptographic and complexity-theoretic primitives may require fundamentally new approaches.

# 2 Preliminaries

In this section, we introduce the basic notation and formally define the necessary concepts from the theory of pseudorandomness and constructive dimension.

## 2.1 Notation

Let $\Sigma$ denote the binary alphabet $\{0,1\}$. $\Sigma^n$ denotes the set of $n$-length strings and $\Sigma^*$ denotes the set of all finite strings over $\Sigma$. For a finite string $w \in \Sigma^*$, $|w|$ denotes the length of $w$. $1^*$ denotes the set of all finite strings in the unary alphabet $\{1\}$. $\Sigma^\infty$ denotes the *Cantor space*, or the set of all infinite strings over $\Sigma$. We use small letters $w$, $x$ to represent finite strings and capital letters $X$, $Y$ to represent infinite strings over $\Sigma$. For an infinite string $X \in \Sigma^\infty$, $X[i]$ denotes the $i^{\text{th}}$ bit of $X$ and $X \upharpoonright n$ denotes the first n bits of $X$. For infinite string $X = X_1X_2X_3X_4\ldots$ and $m \geq n$, $X[n:m]$ denotes the the substring $X_nX_{n+1}X_{n+2}\ldots X_m$. For a finite string $w \in \Sigma^*$, $w[i]$, $w \upharpoonright n$ and $w[n:m]$ are defined similarly. $\lambda$ denotes the empty string. $\mathbb{N}$ denotes the set of natural numbers and $\mathbb{Q}$ denotes the set of rationals. All the logarithms in the paper are taken to base 2 unless specified otherwise. For any function $f : \Sigma^\infty \to \Sigma^\infty$ and $\mathcal{S} \subseteq \Sigma^\infty$ let $f(\mathcal{S})$ denote $\{f(X) : X \in \mathcal{S}\}$.

For $w \in \Sigma^*$, $C_w$ denotes the *cylinder set* of $w$, that is the set of all infinite sequences in $\Sigma^\infty$ that begin with $w$. Let $\mathcal{B}(\Sigma^\infty)$ denote the Borel $\sigma$-algebra over $\Sigma^\infty$ generated by the set of all cylinder sets $\{C_w : w \in \Sigma^*\}$. For two finite strings $x, y \in \Sigma^*$, $x.y$ denotes the concatenation of the strings $x$ and $y$.

We use poly$(n)$ to denote the set of polynomial (time) functions $\bigcup_{c\in\mathbb{N}}\{n^c\}$. When the context is clear, we also use poly to denote poly$(n)$. We use $U_n$ to denote the uniform probability distribution over $\Sigma^n$.

## 2.2 Time Bounded Kolmogorov complexity

We define time bounded Kolmogorov complexity.

**Definition 2.1** ($t$-time bounded Kolmogorov complexity [Kol65, LV08])**.** *Let $t$ be a time-constructible function, and $x \in \Sigma^*$ be a finite binary string. The $t$-time bounded Kolmogorov complexity of $x$ is*

$$K_t(x) = \min\{|\Pi| \text{ such that } \Pi \in \Sigma^* \text{ and } \mathcal{U}(\Pi) = x \text{ in } t(|x|) \text{ steps}\}.$$

*where $\mathcal{U}$ is any fixed universal Turing machine.*

Since in the study of resource dimension we divide $K_t(x)$ by $|x|$, our results are unaffected by the choice between prefix-free Kolmogorov complexity and plain Kolmogorov complexity. We use plain Kolmogorov complexity in the rest of the paper.

### 2.3 Polynomial-time dimension

We first give the formal definition of polynomial time dimension using polynomial time $s$-gales. Towards this end, we first define the concepts of $s$-gales, supergales, martingales and supermartingales.

**Definition 2.2** ([Lut03a, Lut03b]). *For $s \in [0, \infty)$,*

1. *An $s$-supergale is a function $d : \Sigma^* \to [0, \infty)$ such that $d(\lambda) < \infty$ and for every finite string $w \in \Sigma^*$,*
$$d(w) \geq \frac{d(w0) + d(w1)}{2^s}.$$
2. *A supermartingale is a 1-supergale.*
3. *An $s$-gale is a function $d : \Sigma^* \to [0, \infty)$ with $d(\lambda) < \infty$ for every finite string $w \in \Sigma^*$,*
$$d(w) = \frac{d(w0) + d(w1)}{2^s}.$$
4. *A martingale is a 1-gale.*

Unless specified otherwise, for every $s$-supergale $d$, we assume that the initial capital $d(\lambda) = 1$.

**Definition 2.3** ([Lut03a, Lut03b]). *The* success set *of an $s$-supergale $d$ is*
$$S^\infty(d) = \left\{ X \in \mathbb{N}^\infty \mid \limsup_{n\to\infty} d(X \upharpoonright n) = \infty \right\}.$$

**Definition 2.4** ([AHLM07]). *The* strong success set *of an $s$-supergale $d$ is*
$$S^\infty_{\mathrm{str}}(d) = \left\{ X \in \mathbb{N}^\infty \mid \liminf_{n\to\infty} d(X \upharpoonright n) = \infty \right\}.$$

Now, we define time bounded supergales. We first define $t(n)$-time computable $s$-gales.

**Definition 2.5** ($t(n)$-time computability [Lut03a]). *An $s$-supergale $d : \Sigma^* \to [0, \infty) \cap \mathbb{Q}$ is $t(n)$-time computable if there exist a $t(n)$-time computable function $f : \Sigma^* \times 1^* \to \mathbb{Q}$ such that $|d(w) - f(w, 1^n)| \leq 2^{-n}$ for every $w \in \Sigma^*$ and $n \in \mathbb{N}$.*

Another notion of time bounded computability is that of exact $t(n)$-time computability.

**Definition 2.6** (Exact $t(n)$-time computability [Lut03a]). *An $s$-supergale $d : \Sigma^* \to [0, \infty) \cap \mathbb{Q}$ is exact $t(n)$-time computable if there exist a $t(n)$-time computable function $f : \Sigma^* \to \mathbb{Q}$ such that $d(w) = f(w)$ for every $w \in \Sigma^*$.*

Now, we define polynomial-time dimension and strong dimension.

**Definition 2.7** (Polynomial-time dimension [Lut03a]). *The polynomial-time dimension of $\mathcal{F} \subseteq \Sigma^\infty$ is defined as*
$$\dim_{\mathrm{P}}(\mathcal{F}) = \inf\{s \mid (\exists k) \text{ there is an exact } n^k\text{-time computable } s\text{-gale } d \text{ such that } \mathcal{F} \subseteq S^\infty(d)\}.$$
*For a sequence $X \in \Sigma^\infty$, define $\dim_{\mathrm{P}}(X) = \dim_{\mathrm{P}}(\{X\})$.*

**Definition 2.8** (Polynomial-time strong dimension [AHLM07, Stu20]). *The polynomial-time strong dimension of $\mathcal{F} \subseteq \Sigma^\infty$ is defined as*

$$\mathrm{Dim}_{\mathrm{P}}(\mathcal{F}) = \inf\{s \mid (\exists k) \text{ there is an exact } n^k\text{-time computable } s\text{-gale } d \text{ such that } \mathcal{F} \subseteq S^\infty_{\mathrm{str}}(d)\}.$$

*For a sequence $X \in \Sigma^\infty$, define $\mathrm{Dim}_{\mathrm{P}}(X) = \mathrm{Dim}_{\mathrm{P}}(\{X\})$.*

We now make an important remark. Polynomial time dimension and strong dimension are often defined in terms of $n^k$-time computable $s$-gales that need not be exact computable. But these definitions are in fact equivalent. This is a direct consequence of the following lemma from [Lut03a] which is also useful in proving the main results in this paper.

**Lemma 2.1** (Exact Computation Lemma [Lut03a]). *If there is a polynomial time computable $s$-gale $d$ such that $2^s \in \mathbb{Q}$, then there exists an exact polynomial time computable $s$-gale $\tilde{d}$ such that $S^\infty(d) \subseteq S^\infty(\tilde{d})$.*

We will often use the terminology polynomial-time computable gales to refer to exact $t(n)$-time computable $s$-gales where $t(n) \in \mathrm{poly}(n)$. Similar comment applies in the case of exact polynomial-time computability and other notions related to gales such as martingales and supergales.

Now, we define the asymptotic polynomial-time density of information of a subset $\mathcal{F} \subseteq \Sigma^\infty$.

**Definition 2.9** ($\mathcal{K}_{\mathrm{poly}}$ and $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}$ [HV06, Stu20, Hit03]). *For any $\mathcal{F} \subseteq \Sigma^\infty$, define*

$$\mathcal{K}_{\mathrm{poly}}(\mathcal{F}) = \inf_{t \in poly} \sup_{X \in \mathcal{F}} \liminf_{n\to\infty} \frac{K_t(X \upharpoonright n)}{n}.$$

$$\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\mathcal{F}) = \inf_{t \in poly} \sup_{X \in \mathcal{F}} \limsup_{n\to\infty} \frac{K_t(X \upharpoonright n)}{n}.$$

For individual sequences, we define $\mathcal{K}_{\mathrm{poly}}(X) = \mathcal{K}_{\mathrm{poly}}(\{X\})$ and $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) = \mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\{X\})$. Note that $\mathcal{K}_{\mathrm{poly}}$ and $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}$ are equivalently defined in the following way.

**Definition 2.10** ($\mathcal{K}_{\mathrm{poly}}$ and $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}$ [HV06, Stu20, Hit03]). *For any $X \in \Sigma^\infty$, define*

$$\mathcal{K}_{\mathrm{poly}}(X) = \inf_{t \in poly} \liminf_{n\to\infty} \frac{K_t(X \upharpoonright n)}{n} \text{ and } \mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) = \inf_{t \in poly} \limsup_{n\to\infty} \frac{K_t(X \upharpoonright n)}{n}.$$

From the results we prove in the following sections, it is implied that if one-way functions exist, then $\mathcal{K}_{\mathrm{poly}}$ and $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}$ and not equivalent to $\mathrm{dim}_{\mathrm{P}}$ and $\mathrm{Dim}_{\mathrm{P}}$.

## 2.4 Measure over the Cantor Space

**Definition 2.11** ( [Roy88]). *A function $\mu : \mathcal{M} \to [0, \infty]$, where $\mathcal{M} \subseteq P(\Sigma^\infty)$, is called a measure over $(\Sigma^\infty, \mathcal{M})$ if $\mu(\emptyset) = 0$ and $\mu$ is countably additive. That is, for any countable disjoint collection $\{E_k\}_{k=1}^\infty$ of measurable sets,*

$$\mu\left(\bigcup_{k=1}^{\infty} E_k\right) = \sum_{k=1}^{\infty} \mu(E_k).$$

*We take $\mathcal{M}$ as the set of Borel Measurable sets. Note that $\mathcal{B} \subseteq \mathcal{M}$, where $\mathcal{B}$ is the Borel sigma algebra over $\Sigma^\infty$, we omit $\mathcal{M}$ and say that $\mu$ is a measure over $\Sigma^\infty$.*

Note that $\mathcal{B}$ contains all open sets, and therefore all cylinder sets $C_w$ for all $w \in \Sigma^*$.

**Definition 2.12.** *Let $\nu$ be a measure over $\Sigma^\infty$. We say that $\nu$ is a probability distribution over $\Sigma^\infty$ if it holds that $\nu(\Sigma^\infty) = 1$.*

**Definition 2.13.** *Let $\nu$ be a probability distribution over $\Sigma^\infty$. For every $n$, let $\nu_n$ denote the probability distribution induced by $\nu$ on $\Sigma^n$ defined as $\nu_n(w) = \nu(C_w)$ for every $w \in \Sigma^\infty$.*

Now we define the uniform (Lebesgue) measure over the Cantor space.

**Definition 2.14** (Uniform measure over the Cantor Space [DH10, Nie09])**.** *Let $\Sigma^\infty$ be the Cantor space. The uniform measure of a cylinder set $C_w$ determined by a finite string $w$ is defined as:*

$$\mu(C_w) = 2^{-|w|}.$$

Using routine measure theoretic arguments, $\mu$ uniquely extends to a probability measure over $(\Sigma^\infty, \mathcal{B}(\Sigma^\infty))$ (see [Bil95]).

## 2.5 One-way functions

The following is the definition of one-way functions secure against uniform probabilistic polynomial time adversaries.

**Definition 2.15** (One-way functions [Gol08, Vad12, Gol01])**.** *A function $f_n : \Sigma^* \to \Sigma^*$ is a one-way function (OWF) if:*

1. *There is a constant $b$ such that $f_n$ is computable in time $n^b$ for sufficiently large $n$.*
2. *For every probabilistic polynomial time algorithm $A$ and every constant $c > 0$:*

$$\Pr[A(f_n(U_n)) \in f_n^{-1}(f_n(U_n))] \leq \frac{1}{n^c}$$

*for all sufficiently large $n$, where the probability is taken over the choice of $U_n$ and the internal randomness of algorithm $A$.*

## 2.6 Pseudorandom generators

In order to define pseudorandom generators, we first define computational indisitinguishability.

**Definition 2.16** (Computational Indistinguishability [Gol08, Vad12])**.** *The ensembles of random variables $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are computationally indistinguishable if for every probabilistic polynomial time algorithm $T$ and every constant $c > 0$,*

$$|\Pr[T(X_n) = 1] - \Pr[T(Y_n) = 1]| \leq \frac{1}{n^c}$$

*where the probabilities are taken over the distributions of either $X_n$ or $Y_n$ and the internal randomness of the algorithm $T$.*

**Definition 2.17** (Pseudorandom generators [Gol08, Vad12, Gol01])**.** *A sequence of functions $G_m : \Sigma^{d(m)} \to \Sigma^m$ is a pseudorandom generator (PRG) if:*

1. *$d(m) < m$*
2. *There exist an uniform and deterministic polynomial time algorithm $M$ such that $M(m, x) = G_m(x)$.*
3. *$\{G(U_{d(n)})\}_{n\in\mathbb{N}}$ and $\{U_n\}_{n\in\mathbb{N}}$ are computationally indistinguishable.*

### 2.7 One-way functions and Pseudorandom generators

The equivalence theorem stated below demonstrates that one-way functions and pseudorandom generators are fundamentally equivalent.

**Theorem 2.1** (Equivalence of One-way Functions and PRGs [HILL99, Gol08, Gol01])**.** *The following are equivalent:*

1. *One-way functions exist.*
2. *There exist a pseudorandom generator with seed length $d(m) = m - 1$.*
3. *For every polynomial-time computable constant $\epsilon \in (0, 1)$, there exists a pseudorandom generator with seed length $d(m) = \epsilon.m$.*

### 2.8 Polynomial time samplable distributions on $\Sigma^\infty$

Now we define polynomial time samplable distributions on $\Sigma^\infty$.

**Definition 1.1.** *A probability distribution $\nu$ over $\Sigma^\infty$ is polynomial time samplable if there exists a probabilistic polynomial time Turing machine $M$ that uses $q(n)$ random bits, where $q$ is a polynomial, such that for every $n$ and $w \in \Sigma^n$, $\Pr_{r\sim\Sigma^{q(n)}}[M(1^n, r) = w] = \nu_n(w)$*[6]*.*

One-way functions are secure against inversion by probabilistic polynomial time adversaries. However, polynomial time gales are defined in terms of computation using deterministic machines. In order to bridge this gap, we define martingales and $s$-gales that are approximable using probabilistic polynomial-time machines.

The support of a distribution is the set of points at which the distribution does not vanish. That is $\mathrm{supp}(\nu_n) = \{w \in \Sigma^n : \nu_n(w) > 0\}$.

**Definition 1.2.** *Let $d : \Sigma^* \to [0, \infty) \cap \mathbb{Q}$ be an $s$-supergale and $\nu$ be any probability distribution over $\Sigma^\infty$. $d$ is $t(n)$-time $\nu$-approximable if for every constant $k$ there exist a probabilistic $t(n)$-time machine $M$ and constant $c < 1$ such that for every $n$, $\{w \in \Sigma^n : M(w) \notin [c{\cdot}d(w), d(w)]\} \subseteq \mathrm{supp}(\nu_n)$ and $\nu_n\{w \in \Sigma^n : M(w) \notin [c \cdot d(w), d(w)]\} \leq n^{-k}$.*

In other words, the set of strings at which the algorithm $M$ makes an error in approximating $d(w)$ outside $[c.d(w), d(w)]$ lies within the support of $\nu_n$, and the measure of the set of such strings according to $\nu_n$ is inverse polynomial.

## 3 One-way functions and polynomial time samplable distributions

We show that the existence of dimension gaps almost everywhere with respect to certain polynomial time samplable distributions over $\Sigma^\infty$ is equivalent to the existence of one-way functions. Towards this end, we consider polynomial time samplable distributions $\nu$ such that for almost every $X$ according to $\nu$, we have that $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$.

In this work, we define the notion of a "significant" gap between Kolmogorov complexity ($\mathcal{K}_{\mathrm{poly}}$) and gale based ($\dim_{\mathrm{P}}$) formulations of polynomial-time dimension for polynomial time samplable

[6] An alternate way of defining polynomial time samplable distributions on $\Sigma^\infty$ is the following: $\nu = \{\nu_n\}$ is a *polynomial time samplable distribution on* $\Sigma^\infty$ if $\{\nu_n\}$ is a *polynomial time samplable distribution* (in the sense of [IRS22, HIL+23, LP20]) such that for any $w \in \Sigma^n$, $\nu_n(w) = \nu_{n+1}(w.0) + \nu_{n+1}(w.1)$. The equivalence of these notions follows using routine measure theoretic arguments.

distributions. The gap is said to be significant if $\dim_{\mathrm{P}}$ and $\mathcal{K}_{\mathrm{poly}}$ differ for a large collection of the sequences in the range of the distribution. We say that there is no "significant" dimension gap induced by $\nu$ if for any $s' < s$, an $s'$-gale $d$ would win on a significant fraction of the sequences in $\mathcal{F}$, ensuring that $\nu(S^{\infty}(d)) > 0$.

We first show that one-way functions imply the existence of distributions over which dimension gap exists almost everywhere.

**Lemma 1.1.** *If one-way functions exist, then for every $s < 1/2$, there exist a polynomial time samplable distribution $\nu$ over $\Sigma^{\infty}$ such that:*

1. *$\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ for almost every $X \sim \nu$.*
2. *For every $s' \in (s, 1/2)$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^{\infty}(d)) = 0$.*

We then show the result in the converse direction that the existence of distributions over which dimension gap exists almost everywhere implies the existence of infinitely often one-way functions.

**Lemma 1.2.** *If there exist an $s < 1$ and a polynomial time samplable distribution $\nu$ over $\Sigma^{\infty}$ such that:*

1. *$\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ for almost every $X \sim \nu$.*
2. *There exist some $\hat{s} \in (s, 1]$ such that for every $s' \in (s, \hat{s})$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^{\infty}(d)) = 0$.*

*Then, infinitely-often one-way functions exist.*

Together we obtain the following theorem between dimension gaps and existence of one-way functions.

**Theorem 1.5.** *In the following, (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3):*

1. *One-way functions exist.*
2. *For every $s < \frac{1}{2}$, there exists a polynomial-time samplable distribution $\nu$ over $\Sigma^{\infty}$ such that:*
   (a) *$\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ for almost every $X \sim \nu$.*
   (b) *For every $s' \in (s, \frac{1}{2})$ and every polynomial-time $\nu$-approximable $s'$-supergale $d$, we have*
   $$\nu(S^{\infty}(d)) = 0.$$
3. *Infinitely-often one-way functions exist*[7].

*Proof.* (1) $\Longrightarrow$ (2) follows from Lemma 1.1. Choosing $s < 1/2$ and setting $\hat{s} = 1/2$, the hypothesis of Lemma 1.2 follows from (2). And therefore we get (2) $\Longrightarrow$ (3) from Lemma 1.2. □

# 4 A mapping between infinite sequences using PRGs

One of the major constructions we require in proving our results is an extension of pseudorandom generators with constant stretch to a mapping between infinite strings.

[7] See the remarks in section 10 regarding infinitely-often one-way functions and polynomial time dimension and also Lemma 10.1.

## 4.1 Definition of $g$

Given a PRG $G_n : \Sigma^{sn} \to \Sigma^n$ where $s = 2^{-m}$ for some $m \in \mathbb{N}$, we construct a mapping $g$ from the Cantor set to itself, by using the family $\{G_n\}_{n\in\mathbb{N}}$ to map blocks within the input string to *longer* blocks within the output string. Given an input $X \in \Sigma^\infty$, $g(X)$ is constructed by applying $G_n$ to successive block $x$ of size $s.2^n$ from $X$ for all $n \in \mathbb{N}$. We first define a sequence of mappings $g_k$ from $\Sigma^k$ to $\Sigma^*$. These mappings preserves the prefix ordering among finite strings and hence we define $g(X)$ for $X \in \Sigma^\infty$ as the limit of $g_k(X \upharpoonright k)$.

**Definition 4.1.** *Let $G_n : \Sigma^{sn} \to \Sigma^n$ where $s = 2^{-m}$ for some $m \in \mathbb{N}$ and let $k \in \mathbb{N}$. For $w \in \Sigma^k$, define $g_k(w)$ as follows. For any $n$ satisfying any $m < n \leq \lfloor \log(k/s) \rfloor$ and $i \in \{2^{n-1}+1, 2^{n-1}+2, \ldots 2^n\}$, let*

$$g_k(w)[i] = G_{2^{n-1}}(x)[i - 2^{n-1}]$$

*where $x = w[s \cdot 2^{n-1}, s \cdot 2^n - 1]$. For $i \in \{1, 2, \ldots, 2^m\}$, we set $g_k(w)[i] = 0$.*

Note that $g_k(w)[2^{n-1}+1, 2^n] = G_{2^{n-1}}(w[s.2^{n-1}, s.2^n - 1])$. For $k \leq 2^m$, $g_k$ maps any $w \in \Sigma^k$ to $0^{2^m}$. Observe that the sequence of mappings $\langle g_k \rangle_{k\in\mathbb{N}}$ preserves the prefix order between strings. That is, If $w' \sqsubseteq w$, then $g_{|w'|}(w') \sqsubseteq g_{|w|}(w)$. Therefore, we define $g$ as the limit of the mappings $g_k$ as $k \to \infty$.

**Definition 4.2.** *For every $X \in \Sigma^*$ let $g(X) = \cap_{n=1}^\infty C_{g(X\upharpoonright n)}$.*

Notice that for any $X \in \Sigma^\infty$ and $k \in \mathbb{N}$, $g_k(X \upharpoonright k) \sqsubseteq g(X)$. For convenience, we abuse the notation and use $g$ to denote the mapping between infinite strings defined above or a mapping between finite strings defined as follows: $g(w) = g_{|w|}(w)$ for any $w \in \Sigma^*$. The intended meaning is clear from the context.

## 4.2 Analysis of $K_t(g(X) \upharpoonright 2^n)$

Now, we prove the following lemma that the polynomial time bounded Kolmogorov complexity of prefixes of sequences in the image set of $g$ is low.

**Lemma 4.1.** *For $s = 2^{-m}$ for some $m > 1$, let $g : \Sigma^\infty \to \Sigma^\infty$ be constructed from a PRG $G_n : \Sigma^{sn} \to \Sigma^n$ that runs in time $t_G(n)$ as in Definition 4.1. There exists a constant $c \in \mathbb{N}$ such that for all $X \in \Sigma^*$ and for all $n \in \mathbb{N}$,*

$$K_{t_g}(g(X) \upharpoonright 2^n) \leq s.2^n + c$$

*where $t_g(n) = t_G(n)n$.*

*Proof.* Consider the algorithm $M$ which implements the mapping in Definition 4.1 as follows.

**Algorithm 1** Algorithm M

```
Input: A string w.
if w = λ then
    Output λ
else
    Output 0^{2^m}
end if
for i = m to ⌊log(|w|2^m)⌋ − 1 do
    Output G_{2^i}(w[2^{−m} · 2^i, 2^{−m} · 2^{i+1} − 1])
end for
```

Since $G_n$ runs in $t_G(n)$ time, it follows that $M$ runs in $t_g(n) = t_G(n) \cdot n$ time. Also, for any $X \in \Sigma^\infty$ and $n \geq m$, $M$ outputs the string $g(X) \upharpoonright 2^n$ on input $X \upharpoonright 2^{-m} \cdot 2^n = X \upharpoonright s \cdot 2^n$. Therefore, it follows that $K_{t_g}(g(X) \upharpoonright 2^n) \leq s \cdot 2^n + c$ where the constant $c$ depends only on the length of any representation of $M$ in the prefix language of the fixed universal Turing machine. □

**Corollary 4.1.** *For $s = 2^{-m}$ for some $m > 1$, let $g : \Sigma^\infty \to \Sigma^\infty$ be constructed from a PRG $G_n : \Sigma^{sn} \to \Sigma^n$ that runs in time $t_G(n)$ as in Definition 4.1. There exists a constant $c \in \mathbb{N}$ such that for all $X \in \Sigma^*$ and for all $i \in \mathbb{N}$,*

$$K_{t_g}(g(X) \upharpoonright i) \leq 2s \cdot i + 2\log(i) + c'$$

*where $t_g(n) = t_G(n)n$.*

*Proof.* From Lemma 4.1, we know that

$$K_{t_g}(g(X) \upharpoonright 2^{\lceil log(i) \rceil}) \leq s \cdot 2^{\lceil log(i) \rceil} + c'.$$

By providing $K_n(i)$ extra information specifying the value of the index $i$ at which $g(X) \upharpoonright 2^{\lceil log(i) \rceil}$ needs to be trimmed, we obtain a program that outputs $g(X) \upharpoonright i$ in $t_g(n)$-time. There is a trivial prefix free program which given $2\log(i)$ bits of information, runs in linear time and prints $i$. Therefore, the value of $K_n(i)$ is at most $2\log(i)$ up to an additive constant. Since $2^{\lceil log(i) \rceil} \leq 2i$, there exists $c' > 0$ such that

$$K_{t_g}(g(X) \upharpoonright i) \leq 2s \cdot i + K_n(i) + c \leq 2s \cdot i + 2\log(i) + c'.$$

□

## 5 Dimension Gap from one-way functions

In this section, we prove Lemma 1.1 by showing that if one-way functions exists, there exists a short polynomial time samplable distribution $\nu$ with a dimension gap, that is for any $s' > s$, and any polytime $\nu$-approximable gale $d$, $\nu(S^\infty(d)) = 0$.

We start with the assumption that one-way functions exist. From Theorem 2.1, we have that for $s = 2^{-m}$ with $m \geq 2$, pseudorandom generators $\{G_n : \Sigma^{sn} \to \Sigma^n\}$ exist. Note that the mapping $g : \Sigma^\infty \to \Sigma^\infty$ constructed using the ensemble $\{G_n\}$ naturally generates a polynomial-time samplable distribution $\nu$ over $\Sigma^\infty$. The sampling algorithm $M$ for $\nu$ on input $1^n$, maps a random seed of length $s \cdot 2^{\lceil \log_2(n) \rceil}$ using $g$ to a string of length $2^{\lceil \log_2(n) \rceil}$, and thereafter trims the output to $n$ bits. The number of random bits used by $M$ on input $1^n$ is at most $2s \cdot n$. We show that the distribution $\nu$ defined by $g$ satisfies the required properties. It follows from Corollary 4.1 that $\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq 2s$ for almost every $X \sim \nu$.

Towards building a contradiction, let there exist some $s' \in (2s, 1/2)$ with $2^{s'} \in \mathbb{Q}$ and a polynomial-time $\nu$-approximable $s'$-supergale $d'$ such that $\nu(S^\infty(d')) > 0$. We now convert the polynomial time $\nu$-approximable $s'$-supergale $d'$ to a polynomial-time $\nu$-approximable martingale $\tilde{d}$ with a guarantee that its capital grows *significantly* between blocks of length $2^n$ for infinitely many $n$ and $\nu(S^\infty(\tilde{d})) > 0$.

**Lemma 5.1.** *For $s' \in [0, \infty)$ if $d' : \Sigma^\infty \to [0, \infty)$ is a $t(n)$-time computable $\nu$-approximable $s'$-gale, then for any $s''$ satisfying $s' \leq s'' \leq 1$ and $2^{s''} \in \mathbb{Q}$, there exists an exact $t(n)poly(n)$-time $\nu$-approximable supermartingale $\tilde{d} : \Sigma^\infty \to [0, \infty)$ such that for any $X \in S^\infty(d')$,*

$$\limsup_{n \to \infty} \frac{\tilde{d}(X \upharpoonright n)}{2^{(1-s'')n}} = \infty.$$

*Proof.* Let $s'' \geq s'$ such that $2^{s''} \in \mathbb{Q}$. We know that $d'$ is an exact $t(n)$-time $s''$-supergale that succeeds on $X$ (see Observation 4.4 from [Lut03a]). Let $\bar{d}$ be defined as $\bar{d}(w) = d'(w)2^{(1-s'')|w|}$. Note that as $d'$ is $\nu$-approximable, it follows that $\bar{d}$ is $\nu$-approximable.

From Observation 3.2 in [Lut03b], it follows that $\bar{d}$ is a supermartingale such that,

$$\limsup_{n\to\infty} \frac{\bar{d}(X \upharpoonright n)}{2^{(1-s'')n}} = \infty.$$

Since $2^{s''}$ is rational, so is $2^{(1-s'')}$. Hence, $\bar{d}$ is an exact $t(n)poly(n)$-time computable supermartingale. □

**Lemma 5.2.** *For $s' < 1/2$, let $d' : \Sigma^\infty \to [0,\infty)$ be an $t(n)$-time $\nu$-approximable $s'$-gale. Let $\tilde{s}$ be such that $\tilde{s} > s'$, $2^{\tilde{s}} \in \mathbb{Q}$. Then, there exists an $t(n)poly(n)$-time $\nu$-approximable martingale $\tilde{d} : \Sigma^\infty \to [0,\infty)$ such that for any $X \in S^\infty(d')$, there exists infinitely many $n \in \mathbb{N}$ such that*

$$\tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1}) \tag{5}$$

*Proof.* Choose $s'' \in (s', 1/2)$ such that $s' < 2s' < 2s'' < \tilde{s}$ and $2^{s''} \in \mathbb{Q}$. Let $\tilde{d}$ be the exact $t(n)poly(n)$-time computable martingale from Lemma 5.1 such that,

$$\limsup_{n\to\infty} \frac{\tilde{d}(X \upharpoonright n)}{2^{(1-s'')n}} = \infty.$$

We show that $\tilde{d}$ satisfies the required property. On the contrary, assume that there exists $m > 0$ such that for every $n > m$,

$$\tilde{d}(X \upharpoonright 2^n) \leq 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1}).$$

Consider any $n > m$. Let $\ell \leq 2^n$. We get that,

$$\begin{aligned}\tilde{d}(X \upharpoonright 2^n + \ell) &\leq 2^\ell 2^{(1-\tilde{s})\sum_{i=m}^{n-1} 2^i} \tilde{d}(X \upharpoonright 2^m) \\ &= 2^\ell 2^{(1-\tilde{s})(2^n - 2^m)} \tilde{d}(X \upharpoonright 2^m).\end{aligned}$$

If $\tilde{d}(X \upharpoonright 2^n + \ell) \geq 2^{(2^n+\ell)(1-s'')}$, then

$$2^{\ell s''} \geq \frac{2^{(1-\tilde{s})2^m}}{\tilde{d}(X \upharpoonright 2^m)} 2^{2^n(\tilde{s}-s'')}.$$

Since $\ell \leq 2^n$, we obtain

$$2^{2^n(\tilde{s}-2s'')} \leq \frac{\tilde{d}(X \upharpoonright 2^m)}{2^{(1-\tilde{s})2^m}}. \tag{6}$$

If there exist infinitely many $k$ such that $\tilde{d}(X \upharpoonright k) \geq 2^{(1-s'')k}$ then there exist infinitely many $n$ satisfying 6. But, since $\tilde{s} > 2s''$, 6 cannot be true for large enough $n$ and therefore we obtain a contradiction. Hence, it must be the case that for infinitely many $n$,

$$\tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1})$$

which is the required conclusion. □

## 5.1 A Distinguisher Algorithm for PRGs

Let $\tilde{d}$ be the $t(n).poly(n)$-time $\nu$-approximable martingale obtained from Lemma 5.2. Let $M$ be the Turing machine that $\nu$-approximates $d$. That is for all $n \in \mathbb{N}$, $\nu_n\{w \in \Sigma^n : M(w) \notin [\mathbf{c} \cdot d(w), d(w)]\} \leq n^{-k}$ where $\mathbf{c} \in \mathbb{Q}, k \in \mathbb{N}$ are constants such that $\mathbf{c} \leq 1$ and $k \geq 1$. We use $M$ to build a distinguisher algorithm $A$ that breaks the PRG $\{G_n\}$.

**Algorithm 2** Algorithm A

**Input:** A string $w$ where $|w| = 2^n$
$r \leftarrow \text{random}(s \cdot 2^n)$ ▷ Generate a random seed of length $s \cdot 2^n$
**for** $i = m$ to $n - 1$ **do**
    $v_i \leftarrow G_{2^i}(r[s \cdot 2^i, s \cdot 2^{i+1} - 1])$ ▷ Use $r$ and $G_{2^i}$ to get a PRG output of length $2^i$
**end for**
$w' \leftarrow 0^{2^m} v_1 \dots v_n$ ▷ Concatenate all $v_i$
**return** 1 **if** $M(w'w) \geq \mathbf{c} \cdot 2^{(1-\tilde{s})|w|} \cdot M(w')$.

## 5.2 Analysis of the Distinguisher Algorithm

### 5.2.1 Performance of the algorithm on outputs of PRGs

Now, we define the function $f$.

**Lemma 5.3.** *Let $f : \Sigma^\infty \times \mathbb{N} \to \{0,1\}$ and $\mathcal{S} \subseteq \Sigma^\infty$ such that $\nu(\mathcal{S}) > 0$. If for every $X \in \mathcal{S}$, there exist infinitely many $n \in \mathbb{N}$ such that $f(X,n) = 1$. Then for any $c > 1$, there exist infinitely many $n \in \mathbb{N}$, such that $\nu(\{X : f(X,n) = 1\}) > n^{-c}$.*

*Proof.* Let $A_n = \{X \in \Sigma^\infty : f(X,n) = 1\}$. We know that,

$$\mathcal{S} \subseteq \limsup_{n\to\infty} A_n = \bigcap_{i=0}^{\infty} \bigcup_{n=i}^{\infty} A_n.$$

Therefore, $\nu(\limsup_{n\to\infty} A_n) \geq \nu(\mathcal{S}) > 0$. Since for $c > 1$, the series $\sum n^{-c}$ is convergent, using the Borel-Cantelli Lemma (see [Bil95]), we obtain that $\nu(A_n) > n^{-c}$ for infinitely many $n$, which is the required conclusion. □

**Definition 5.1.** *Let $f : \Sigma^\infty \times \mathbb{N} \to \{0,1\}$ be defined as follows,*

$$f(X,n) = \begin{cases} 1 & \text{if } \tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^n} \tilde{d}(X \upharpoonright 2^{n-1}) \\ 0 & \text{otherwise.} \end{cases}$$

**Lemma 5.4.** *Given $\tilde{d} : \Sigma^\infty \to [0,\infty)$, if for all sequences $X \in \mathcal{S}$ where $\nu(\mathcal{S}) > 0$, there exists infinitely many $n \in \mathbb{N}$ such that*

$$\tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1})$$

*Then it holds that for infinitely many $n$,*

$$\Pr_{x \sim \Sigma^{s.2^n}}[\tilde{d}(g(x)) > 2^{(1-\tilde{s})2^n} \tilde{d}(g(x \upharpoonright s.2^{n-1}))] \geq \frac{1}{n^2}. \tag{7}$$

*Proof.* We have that for all $Y \in \mathcal{S}$ where $\nu(\mathcal{S}) > 0$, there exists infinitely many $n \in \mathbb{N}$ such that $\tilde{d}(Y \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}}\tilde{d}(Y \upharpoonright 2^{n-1})$. From the definition of the function $f$ (Definition 5.1), we have that for all $X \in \mathcal{S}$, there exist infinitely many $n \in \mathbb{N}$ such that $f(X, n) = 1$.

Since $\nu(\mathcal{S}) > 0$, using Lemma 5.3, we obtain that for any $c > 1$ there exist infinitely many $n \in \mathbb{N}$ such that $\nu(\{X : f(X, n) = 1\}) > n^{-c}$. Then, from the definition of $f$, we have

$$\nu(\{X : \tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^n}\tilde{d}(X \upharpoonright 2^{n-1})\} > n^{-c}.$$

Since $\nu$ is defined in terms of $g$, it follows that

$$\Pr_{x\sim\Sigma^{s.2^n}}[\tilde{d}(g(x)) > 2^{(1-\tilde{s})2^n}\tilde{d}(g(x \upharpoonright s.2^{n-1}))] > n^{-c}.$$

Putting $c = 2$ , we have

$$\Pr_{x\sim\Sigma^{s.2^n}}[\tilde{d}(g(x)) > 2^{(1-\tilde{s})2^n}\tilde{d}(g(x \upharpoonright s.2^{n-1}))] > n^{-2}.$$

□

Let $n + 1$ be one of the lengths at which the condition in Lemma 5.4 holds. Let $w, w' \in \Sigma^{2^n}$ such that $w = G_{2^n}(x)$ for some $x \in \Sigma^{2^{sn}}$ and $w' = g(r)$ for some $r \in \Sigma^{2^{sn}}$.

In order for the condition $M(w'w) \geq \mathbf{c} \cdot 2^{(1-\tilde{s})|w|} \cdot M(w')$ to hold, it suffices that $\tilde{d}(w'w) \geq 2^{(1-\tilde{s})|w|} \cdot \tilde{d}(w')$ and $M(w'w) \geq \mathbf{c} \cdot \tilde{d}(w'w)$ and $M(w) \leq \tilde{d}(w)$.

From Lemma 5.4, it follows that the first condition holds with probability at least $(n + 1)^{-2}$ among $x, r$ selected uniformly at random from $\Sigma^{s\cdot 2^n} \times \Sigma^{s\cdot 2^n}$ and taking $w = g(x), w' = g(r)$. Since $\tilde{d}$ is $\nu$-approximable, for some $k \in \mathbb{N}$, on input $w \in \Sigma^{2^n}$, the computations of all $M(w)$ in Algorithm 2 outputs a value in $[\mathbf{c} \cdot \tilde{d}(w), \tilde{d}(w)]$ with probability at least $1 - 2^{-(kn-1)}$ according to the distribution $\nu_{2^n}$. Note that the distribution according to $\nu_{2^n}$ corresponds to $g$ applied to the uniform distribution on $2^{sn}$.

Therefore it follows that for infinitely many n,

$$\Pr_{(x,r)\sim\Sigma^{s\cdot 2^n}\times\Sigma^{s\cdot 2^n}}[A(G_{2^n}(x), r)) = 1] \geq \frac{1}{(n+1)^2} - \frac{1}{2^{kn}}.$$

Hence, taking $N = 2^n$, for infinitely many $n$,

$$\Pr_{x\sim\Sigma^{s\cdot N}}[A(G_N(x)) = 1] \geq \frac{1}{(\log N + 1)^2} - \frac{1}{N^k}. \tag{8}$$

### 5.2.2 Performance of the algorithm on uniformly random inputs

We now analyze $\Pr_{x\in\Sigma^{2^n}}[A(x) = 1]$. We use the Kolmogorov inequality for supermartingales to show that this is inverse exponentially small in input size.

**Lemma 5.5** (Kolmogorov Inequality [Lut03a])**.** *Let $d : \Sigma^\infty \to [0, \infty)$ be a supermartingale. For any $w' \in \Sigma^*$ and $n, c \in \mathbb{N}$, the number of strings $w \in \Sigma^n$ such that $d(w'y) \geq c.d(w')$ for some $y \sqsubseteq w$ is less than or equal to $2^n/c$.*

*Proof.* Define,

$$\mathcal{E} = \{x : (\exists w \in \Sigma^n(x \sqsubseteq w)) \wedge (d(w'x) \geq c \cdot d(w')) \wedge (\forall y \sqsubset x(d(w'y) < c \cdot d(w')))\}$$

Observe that $\mathcal{E}$ is a prefix free set such that for every $w \in \Sigma^n$ satisfying $d(w'y) \geq c.d(w')$ for some $y \sqsubseteq w$, there exists an $x \in \mathcal{E}$ such that $x \sqsubseteq y$. Since $d$ is a supermartingale, using an induction argument, it follows that

$$d(w') \geq \sum_{x \in \mathcal{E}} \frac{1}{2^{|x|}} \cdot d(w'x) = \sum_{x \in \mathcal{E}} \frac{2^{n-|x|}}{2^n} \cdot d(w'x) \geq \frac{1}{2^n} \sum_{x \in \mathcal{E}} 2^{n-|x|} d(w'x).$$

If $d(w') = 0$, then the lemma follows trivially. Assume that $d(w') > 0$. Let $M$ be the number of strings $w \in \Sigma^n$ such that $d(w'y) \geq c.d(w')$ for some $y \sqsubseteq w$. It follows that,

$$d(w') \geq \frac{1}{2^n} \cdot M \cdot c \cdot d(w').$$

Therefore, we obtain that $M \leq 2^n/c$, which is the required conclusion. □

We need an upper bound on the number of strings $w \in \Sigma^{2^n}$ and $r \in \Sigma^{2^{sn}}$ such that $A(w, r) = 1$. This happens when $M(w'w) \geq \mathbf{c} \cdot 2^{(1-\tilde{s})|w|} \cdot M(w')$.

For any $n \in \mathbb{N}$, take any $r \in \Sigma^{s.2^n}$, and let $w' = g(r)$. Using the Kolmogorov Inequality for Martingales (Lemma 5.5), the number of strings $w \in \Sigma^{2^n}$ such that $\tilde{d}(w'w) \geq \mathbf{c}^2 \cdot 2^{|w|(1-\tilde{s})} \tilde{d}(w')$ is less than $2^{|w|}/(\mathbf{c}^2 \cdot 2^{|w|(1-\tilde{s})})$.

For the remaining set of strings, we have that $\tilde{d}(w'w) < \mathbf{c}^2 \cdot 2^{|w|(1-\tilde{s})} \tilde{d}(w')$. If we have that $M(w'w) \leq \tilde{d}(w'w)$ and $M(w') \geq \mathbf{c} \cdot \tilde{d}(w')$, it follows that $A(w, r) = 0$.

We know that, $\nu\{w \in \Sigma^{2^n} : M(w) \notin [\mathbf{c} \cdot \tilde{d}(w), \tilde{d}(w)]\} \leq 2^{-nk}$ for some $k \in \mathbb{N}$. From this, it follows that $\Pr_{r \in \Sigma^{s.N}}[M(w') < \mathbf{c} \cdot \tilde{d}(w')] \leq 2^{-nk}$.

Notice that $\{w \in \Sigma^j : M(w) \notin [\mathbf{c} \cdot \tilde{d}(w), \tilde{d}(w)]\} \subseteq \text{supp}(\nu_j)$ for every $j$. From the block-wise definition of the mapping $g$, for any fixed $w' \in g(\Sigma^{2^n})$, we obtain that there are at most $2^{s \cdot 2^n}$ strings in the set $\{w'w\}_{w \in \Sigma^{2^n}}$ contained in $\text{supp}(\nu_{2^{n+1}})$. Therefore, for any fixed $w'$, the number of strings $w \in \Sigma^{2^n}$ such that $M(w'w) \notin [\mathbf{c} \cdot \tilde{d}(w'w), \tilde{d}(w'w)]$ is at most $2^{s \cdot 2^n}$.

Therefore, we have that

$$\Pr_{x \sim \Sigma^N} \Pr_{r \in \Sigma^{s.N}}[A(x, r) = 1] < \mathbf{c}^{-2} \cdot 2^{-N(1-\tilde{s})} + N^{-k} + 2^{-(1-s)N}.$$

Therefore, it follows that for any $n \in \mathbb{N}$,

$$\Pr_{x \sim \Sigma^N}[A(x) = 1] < \frac{1}{\mathbf{c}^2 \cdot 2^{N(1-\tilde{s})}} + \frac{1}{N^k} + \frac{1}{2^{N(1-s)}}. \tag{9}$$

### 5.3 Proof of Lemma 1.1

Now, we conclude the proof of Lemma 1.1.

*Proof of Lemma 1.1.* If one-way functions exist then there exists PRG $G_n : \Sigma^{sn} \to \Sigma^n$ running in time $t_G(n) \in \text{poly}(n)$ [Theorem 2.1]. For all $s = 2^{-m}$ with $m \geq 2$, using $\{G_n\}$, we construct a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ such that the number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$.

We further show that if we assume to the contrary that for some $s' \in (s, 1/2)$ and some polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) > 0$, then there exists a distinguisher algorithm $A$ that runs in time $t_A(n) \in \text{poly}(n)$, such that for infinitely many $N \in \mathbb{N}$, for all $k \in \mathbb{N}$,

$$\Pr_{x \in \Sigma^{s.N}}[A(G_N(x)) = 1] - \Pr_{x \in \Sigma^N}[A(x) = 1] > \frac{1}{(\log N + 1)^2} - \frac{2}{N^k} - \frac{1}{\mathbf{c}^2 \cdot 2^{N(1-\tilde{s})}} - \frac{1}{2^{N(1-s)}}.$$

Let $c$ be any constant such that $t_A(n) \leq n^c$ and for all large enough $N$,

$$\frac{1}{(\log N+1)^2} - \frac{2}{N^k} - \frac{1}{\mathbf{c}^2 \cdot 2^{N(1-\tilde{s})}} - \frac{1}{2^{N(1-s)}} \geq \frac{1}{N^c}$$

It follows that $G_N$ is not a $(N^c, 1/N^c)$ PRG for infinitely many $N$. Therefore the family $\{G_n\}_{n\in\mathbb{N}}$ is not a PRG. Hence we have shown that PRG's $G_n : \Sigma^{sn} \to \Sigma^n$ do not exist for $s = 2^{-m}$ where $m \geq 2$, which contradicts the assumption that One-way functions exist. This completes the proof of the lemma.

□

# 6 Infinitely-often one-way functions from dimension gaps

Now, we prove Lemma 1.2.

**Lemma 1.2.** *If there exist an $s < 1$ and a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ such that:*

1. *$\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ for almost every $X \sim \nu$.*
2. *There exist some $\hat{s} \in (s, 1]$ such that for every $s' \in (s, \hat{s})$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.*

*Then, infinitely-often one-way functions exist.*

Assume there exists some $s < 1$, a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ such $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ for almost every $X \sim \nu$ and a constant $\hat{s} \in (s, 1]$ such that for every $s' \in (s, \hat{s})$ and polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.

Fix arbitrary $s', s''$ and $s'''$ such that $s < s' < s'' < s''' < \hat{s}$ and $2^{s'''} \in \mathbb{Q}$. Consider the function $d : \Sigma^* \to [0, \infty)$ defined as $d(w) = 2^{s'''|w|}\nu(w)$. It is easy to verify that $d$ is an $s'''$-supergale.

**Claim 6.1.** $\nu\{X \in \Sigma^\infty : \exists^\infty n \text{ such that } \nu_n(X \upharpoonright n) \geq 2^{-n\cdot s''}\} > 0$.

*Proof.* Assume that the set of $X$ satisfying the property has probability 0. Then, for any $\epsilon > 0$, there exist a large enough $N$ such that

$$\nu\{X \in \Sigma^\infty : \forall n \geq N,\ 0 < \nu_n(X \upharpoonright n) < 2^{-n\cdot s''}\} \geq 1 - \epsilon.$$

Since $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ for almost every $X \sim \mu$, there exist a large enough constant $c$ such that for $t(n) = n^c$,

$$\nu\{X \in \Sigma^\infty : \limsup_{n\to\infty} K_t(X \upharpoonright n)/n \leq s\} \geq 1 - \epsilon.$$

Without loss of generality we assume that $N$ is large enough so that

$$\nu\{X \in \Sigma^\infty : \forall n \geq N,\ K_t(X \upharpoonright n) \leq n \cdot s'\} \geq 1 - 2\epsilon.$$

Using a union bound, for any $n \geq N$,

$$\nu\{w \in \Sigma^n : 0 < \nu_n(w) < 2^{-n\cdot s''} \text{ and } K_t(X \upharpoonright n) \leq n \cdot s'\} \geq 1 - 3\epsilon.$$

Let $\mathcal{S}_n = \{w \in \Sigma^n : 0 < \nu_n(w) < 2^{-n\cdot s''}$ and $K_t(X \upharpoonright n) \leq n \cdot s'\}$. The above inequality gives $\nu(\Sigma^n \cap \mathcal{S}_n^{\mathsf{c}}) \leq 3\epsilon$. Since there are at most $2^{n\cdot s'}$ strings with $K_t(X \upharpoonright n) \leq n \cdot s'$, we obtain

$$\nu(\mathcal{S}_n) \leq \frac{2^{n\cdot s'}}{2^{n\cdot s''}} = 2^{-n\cdot(s''-s')}.$$

Recall that $s'' > s'$. By choosing $n$ large enough so that $2^{-n\cdot(s''-s')} \leq \epsilon$ and summing the probabilities of all $w \in \Sigma^n$ we get

$$1 = \sum_{w\in\Sigma^n} \nu_n(w) = \sum_{w\in\Sigma^n\cap\mathcal{S}_n} \nu_n(w) + \sum_{w\in\Sigma^n\cap\mathcal{S}_n^{\mathsf{c}}} \nu_n(w) \leq 2^{-n\cdot(s''-s')} + 3\epsilon \leq 4\epsilon.$$

By choosing $\epsilon < 1/4$ we arrive at a contradiction. Therefore, the measure of the set of $X$ satisfying $\nu_n(X \upharpoonright n) \geq 2^{-n\cdot s''}$ for infinitely many $n$ must be positive. □

Notice that if $\nu_n(w) \geq 2^{-n\cdot s''}$ then $d(w) \geq 2^{n(s'''-s'')}$. Therefore from Claim 6.1 we obtain that

$$\nu\left\{X \in \Sigma^\infty : \limsup_{n\to\infty} d(X \upharpoonright n) = \infty\right\} > 0.$$

We now show that if infinitely-often one-way functions do not exist, there exists an algorithm $M$ that $\nu$-approximates $d$. Hence, we obtain a contradiction to our assumption that for every $s' \in (s, \hat{s})$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$. Therefore, it must be the case that infinitely-often one-way functions exist. We require the following result by Ilango, Ren and Santhanam (see Theorem 20 from [IRS22]) which is implicit in [IL89, IL90].

**Theorem 6.1** ([IRS22, IL89, IL90])**.** *Assume that no infinitely-often one-way functions exist. Let $\mathcal{D} = \{\mathcal{D}_n\}$ be a polynomial time samplable distribution and $q \geq 1$ be an arbitrary constant. Then, there exists a probabilistic polynomial time algorithm $\mathcal{A}$ and constant $c < 1$ such that for all $n$,*

$$\Pr_{x\sim\mathcal{D}_n}[c \cdot \mathcal{D}_n(x) \leq \mathcal{A}(x) \leq \mathcal{D}_n(x)] \geq 1 - O\left(\frac{1}{n^q}\right).$$

The following claim completes the proof of the Lemma 1.2.

**Claim 6.2.** *$d$ is polynomial time $\nu$-approximable.*

*Proof.* Let $S$ be the machine that samples the distribution $\nu$ such that for every $n$, $\Pr_r[S(1^n, r) = w] = \nu_n(w)$ for every $w \in \Sigma^n$. Let $c'$ be the constant such that $M$ uses $n^{c'}$ random bits to sample a string of length $n$.

Assume that no infinitely-often one-way functions exist. Then, the function $f : \Sigma^* \to \Sigma^*$ defined as

$$f(x) = M(1^{|x|^{1/c'}}, x)$$

is not an infinitely-often weak one-way function. Hence for any $q \geq 1$ there exist an algorithm $\mathcal{I}$ such that for all $n$,

$$\Pr_{r\sim\Sigma^{n^{c'}}}[f(\mathcal{I}(f(r))) = f(r)] = \Pr_{w\sim\nu_n}[f(\mathcal{I}(w)) = w] \geq 1 - O\left(\frac{1}{n^q}\right). \tag{10}$$

From our assumption that infinitely-often one-way functions do not exist and Theorem 6.1, we obtain that for any $q \geq 1$, there exists a probabilistic polynomial time algorithm $\mathcal{A}$ and constant $c < 1$ such that for all $n$,

$$\Pr_{w\sim\nu_n}[c \cdot \nu_n(w) \leq \mathcal{A}(w) \leq \nu_n(w)] \geq 1 - O\left(\frac{1}{n^q}\right). \tag{11}$$

Finally, we give the algorithm $M$ that $\nu$-approximates $d$. $M$ on input $w \in \Sigma^n$ runs $\mathcal{I}$ on $w$. If $f(\mathcal{I}(w)) \neq w$, $M$ outputs 0. Else, $M$ runs $\mathcal{A}$ on $w$ and outputs $2^{s'''|w|}\mathcal{A}(w)$. Since $2^{s'''} \in \mathbb{Q}$, $M$ runs in polynomial time. For any $w$ such that $\nu(w) = 0$ (i.e. $w \notin \mathrm{supp}(\nu_n)$), $\mathcal{I}$ will never succeed in finding a pre-image $r$ such that $f(r) = w$ and hence $M$ always outputs 0. Therefore for every $n$, $\{w : M(w) \notin [c \cdot d(w), d(w)]\} \subseteq \mathrm{supp}(\nu_n)$.

Now, from (10) and (11) we obtain that,

$$\Pr_{x\sim\nu_n}[c \cdot d(x) \leq M(x) \leq d(x)] \geq 1 - O\left(\frac{1}{n^q}\right) - O\left(\frac{1}{n^q}\right) \geq 1 - O\left(\frac{1}{n^q}\right).$$

Therefore for every $n$, $\nu\{w : M(w) \notin [c \cdot d(w), d(w)]\} \leq O\left(n^{-q}\right)$. Since $\mathcal{A}$ runs in randomized polynomial time and $q$ is arbitrary, $M$ witness the fact that $d$ is a polynomial time $\nu$-approximable $s'''$-gale. □

# 7 One-way functions and polynomial-time dimension of sets

We prove the following.

**Theorem 1.6.** *If for all $\mathcal{F} \subseteq \Sigma^\infty$,*

$$\dim_{\mathrm{P}}(\mathcal{F}) = \mathcal{K}_{\mathrm{poly}}(\mathcal{F}),$$

*then one-way functions do not exist.*

In fact, we prove the following stronger assertion.

**Theorem 7.1.** *If one-way functions exist, then for every $s < 1/2$, there exist $\mathcal{F} \subseteq \Sigma^\infty$ such that $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\mathcal{F}) \leq s$ and $\dim_{\mathrm{P}}(\mathcal{F}) \geq 1/2$.*

*Proof.* Assume that one-way functions exist. From Lemma 1.1, for every $s < 1/2$ there exist a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ and polynomial $t$ such that:

1. The number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$.
2. For every $s' \in (s, 1/2)$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.

Consider the following set,

$$\mathcal{F}' = \bigcap_{n\geq 1} \bigcup_{w\in\mathrm{supp}(\nu_n)} C_w.$$

Observe that $\cup_{w\in\mathrm{supp}(\nu_n)} C_w$ is a finite union of cylinder sets in $\Sigma^\infty$ and hence is a closed set. Since $\nu$ is a polynomial time samplable probability distribution on $\Sigma^\infty$, $\cup_{w\in\mathrm{supp}(\nu_n)} C_w$ is a superset of $\cup_{w\in\mathrm{supp}(\nu_{n+1})} C_w$ for every $n$. Since $\mathcal{F}'$ is an intersection of a decreasing sequence of non-empty closed sets in the compact space $\Sigma^\infty$, $\mathcal{F}'$ is non-empty (see [S+63]). Since $\nu(\cup_{w\in\mathrm{supp}(\nu_n)} C_w) = 1$ for every $n$, using the continuity of probability measures from above [Bil95], we get $\nu(\mathcal{F}') = 1$. Since the number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$, $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\mathcal{F}') \leq s$. Since the number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$, $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\mathcal{F}) \leq s$. For the sake of contradiction, assume that $\dim_{\mathrm{P}}(\mathcal{F}) < 1/2$. Therefore, for some $s' \in (\dim_{\mathrm{P}}(\mathcal{F}), 1/2)$, there exist a polynomial-time $s'$-supergale $d$ such that $\mathcal{F} \subseteq S^\infty(d)$. Since $d$ is polynomial-time computable, $d$ is trivially a polynomial-time $\nu$-approximable $s'$-supergale. Now, since we know that $\nu(S^\infty(d)) \geq \nu(\mathcal{F}) = 1$, we obtain a contradiction. Hence, it must be the case $\dim_{\mathrm{P}}(\mathcal{F}) \geq 1/2$. □

## 8 One-way functions and polynomial-time dimension of sequences

**Theorem 1.7.** *If for all $X \in \Sigma^\infty$,*

$$\dim_{\mathrm{P}}(X) = \mathcal{K}_{\mathrm{poly}}(X),$$

*then one-way functions do not exist.*

In order to prove the above theorem, it is enough to show the following.

**Theorem 8.1.** *If one-way functions exist, then for every $s < 1/2$, there exist $X \in \Sigma^\infty$ such that $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ and $\dim_{\mathrm{P}}(X) \geq 1/2$.*

We require the following construction.

**Lemma 8.1.** *For any time $t(n) \in \mathrm{poly}(n)$, and $s > 0$ with $2^s \in \mathbb{Q}$, there exists an exact $t(n) \cdot n \cdot \log(n)$-time computable $s$-gale $\tilde{d}$ such that for all exact $t(n)$-time computable $s$-gales $d$, there exist a constant $c$ such that for all $X \in \Sigma^\infty$ and $n \in \mathbb{N}$, $\tilde{d}(X \upharpoonright n) \geq c \cdot d(X \upharpoonright n)$.*

*Proof.* Let $\{M_i\}$ be a standard computable enumeration of all Turing machines. The idea of the proof is that we consider the $t(n)$-time martingales among the first $\log n$ machines to place bets on strings of length $n$. The remaining martingales are assumed to bet evenly on all strings of length $n$.

We will therefore define the martingale, conditioned on the length of the input string $x$. When the length of the input string $x$ satisfies $2^n \leq |x| < 2^{n+1}$, we consider the machines $M_1 \dots M_n$ to decide $\tilde{d}(x)$.

The remaining machines $M_i$ for $i \geq n+1$ are assumed to bet *evenly* on $x$. So, for $i \geq n+1$, we force the capital placed by $M_i$ on $x$ to be $2^{|x|\cdot(s-1)}$.

Therefore, given $x \in \Sigma^*$, such that $2^n \leq |x| < 2^{n+1}$, we define

$$\begin{aligned}\tilde{d}(x) &= \sum_{i=1}^{n} 2^{-i} \cdot M'_i(x) + \sum_{i=n+1}^{\infty} 2^{-i} \cdot 2^{|x|\cdot(s-1)} \\ &= 2^{-n+|x|\cdot(s-1)} + \sum_{i=1}^{n} 2^{-i} \cdot M'_i(x).\end{aligned}$$

We now define $M'_i(x)$. For $n \in N$, let $\mathcal{D}_n(x)$ be the set of machines in $\{M_1, \dots M_n\}$ such that for each $j \leq |x|$, $M(x \upharpoonright j)$ runs in time $t(j)$ and $M(\lambda) = 1$ and $2^s \cdot M(x \upharpoonright j) = M((x \upharpoonright j).0) + M((x \upharpoonright j).1)$.

**Case 1:** $M_i \in \mathcal{D}_n(x)$. The actual bets placed by martingale $M_i$ is taken into consideration for strings of length more than $2^i$. In that case, we need to ensure that the capital of $M_i$ at $x \upharpoonright 2^i$ is forced to be $2^{2^i\cdot(s-1)}$.

In this case, when $M_i(x \upharpoonright 2^i) > 0$, we define $M'_i(x) = 2^{2^i\cdot(s-1)}(M_i(x)/M_i(x \upharpoonright 2^i))$. If $M_i(x \upharpoonright 2^i) = 0$, then it holds that $M_i(x) = 0$, so we just take $M'_i(x) = 0$.

**Case 2:** $M_i \notin \mathcal{D}_n(x)$. In this case, let $j < |x|$ be the least number such that $M_i(x \upharpoonright j)$ takes more than $t(j)$ time to run, or the $s$-gale condition gets violated, that is $2^s \cdot M_i(x \upharpoonright j) \neq M_i((x \upharpoonright j)0) + M_i((x \upharpoonright j)1)$. In this case, we freeze $M'_i s$ capital at index $j$, and $M_i$ is forced to bet evenly after that. Note that we have to force $M_i$ to bet evenly up to $x \upharpoonright 2^i$. Therefore if $j < 2^i$, we take $M'_i(x) = 2^{|x|\cdot(s-1)}$. Otherwise, $j \geq 2^i$ and $M'_i(x) = M'_i(x \upharpoonright j) \cdot 2^{(|x|-j)\cdot(s-1)}$. Note that from the previous case, we have $M'_i(x \upharpoonright j) = 2^{2^i\cdot(s-1)}(M_i(x \upharpoonright j)/M_i(x \upharpoonright 2^i))$.

Consider any exact $t$-time computable martingale $d$. Let $M_k$ be any $t$-time machine such that $d(w) = M_k(w)$ for every $w \in \Sigma^*$. Then, it follows from the construction of $\tilde{d}$ that for all $w$ with $|w| > 2^k$,

$$\tilde{d}(w) \geq \frac{2^{-k} \cdot 2^{-2^k(1-s)}}{d(w \upharpoonright 2^k)} \cdot d(w).$$

Let $c$ be the constant on the right hand side. Note that the membership of any machine from $\{M_1, M_2, \dots M_n\}$ in $\mathcal{D}_n(w)$ is decidable in time $t(|w|) \cdot n \cdot |w|$. Since $n \leq \log(|w|)$, and $2^s \in \mathbb{Q}$, it follows that, $d$ is an exact $t(n) \cdot n \cdot \log(n)$-time computable $s$-gale.

□

Now, we prove Theorem 8.1.

*Proof of Theorem 8.1.* Assume that one-way functions exist. From the proof of Lemma 1.1, we obtain that for every $s < 1/2$ there exist a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ and polynomial $t$ such that:

1. The number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$.
2. For every $s' \in (s, 1/2)$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.

Consider the following set,

$$\mathcal{F} = \bigcap_{n \geq 1} \bigcup_{w \in \text{supp}(\nu_n)} C_w.$$

Observe that $\cup_{w \in \text{supp}(\nu_n)} C_w$ is a finite union of cylinder sets in $\Sigma^\infty$ and hence is a closed set. Since $\nu$ is a polynomial time samplable probability distribution on $\Sigma^\infty$, $\cup_{w \in \text{supp}(\nu_n)} C_w$ is a superset of $\cup_{w \in \text{supp}(\nu_{n+1})} C_w$ for every $n$. Since $\mathcal{F}$ is an intersection of a decreasing sequence of non-empty closed sets in the compact space $\Sigma^\infty$, $\mathcal{F}$ is non-empty (see [S+63]). Since $\nu(\cup_{w \in \text{supp}(\nu_n)} C_w) = 1$ for every $n$, using the continuity of probability measures from above [Bil95], we get $\nu(\mathcal{F}) = 1$. Since the number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$, $\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq s$ for every $X \in \mathcal{F}$. For the sake of contradiction, assume that there exist $s' \in (s, 1/2)$ such that $\dim_{\text{P}}(X) < s'$ for every $X \in \mathcal{F}$. So, every $X \in \mathcal{F}$ there exists an exact computable $s'$-gale $d'_X$ that runs in time $t_{d'_X}(n) \in \text{poly}(n)$, such that $d'_X$ succeeds on $X$.

We first partition the set $\mathcal{F}$, based on the running time of the $s'$-gales that succeeds on it. Define

$$R_i = \{X \in \mathcal{F} : \text{ there exists an } n^i\text{-time } s'\text{-gale } d \text{ such that } X \in S^\infty(d)\}$$

and let $S_i = R_i \setminus R_{i-1}$. Note that $\{S_i\}_{i \in \mathbb{N}}$ is a partition of $\mathcal{F}$ into countably many disjoint subsets. As $\sum_{i=1}^{\infty} \nu(S_i) = 1$, there exists an $k \in \mathbb{N}$ such that $\sum_{i=1}^{k} \nu(S_i) > 0$. Define $\mathcal{S} = \bigcup_{i=1}^{k} S_i$. Using Lemma 8.1, there exists an exact $n^{k+c}$-time computable $s'$-gale $d'$ that succeeds on all sequences in $\mathcal{S}$. Since $d$ is polynomial-time computable, $d$ is trivially a polynomial-time $\nu$-approximable $s'$-supergale. Now, since we know that $\nu(S^\infty(d)) \geq \nu(\mathcal{S}) > 0$, we obtain a contradiction. Hence, it must be the case that there exist a sequence $X \in \mathcal{F}$ with $\dim_{\text{P}}(X) > s'$. Since $s'$ was arbitrary, the theorem follows. □

We also note the following lemma which follows using the same ideas in the proof of Theorem 8.1.

**Lemma 8.2.** *If for some $s < 1/2$, $\nu$ is a polynomial time samplable distribution over $\Sigma^\infty$ such that:*

1. *The number of random bits used by the sampler for $\nu$ on input $1^n$ is at most $sn$.*
2. *For every $s' \in (s, 1/2)$ and any polynomial-time $\nu$-approximable $s'$-supergale $d$, $\nu(S^\infty(d)) = 0$.*

*Then,*

$$\nu\{X \in \Sigma^\infty : \mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq s \text{ and } \dim_{\text{P}}(X) \geq 1/2 > s\} = 1.$$

*Proof.* Consider the set $\mathcal{F}$ in the proof of Theorem 8.1. It is enough to show that, $\nu\{X \in \Sigma^\infty : \mathcal{K}^{\text{str}}_{\text{poly}}(X) > s \text{ or } \dim_{\text{P}}(X) < 1/2\} = 0$. It follows directly from the argument in the proof of Theorem 8.1 that $\mathcal{K}^{\text{str}}_{\text{poly}}(X) \leq s$ for every $X \in \mathcal{F}$. Consider the set $\mathcal{H} = \{X \in \mathcal{F} : \dim_{\text{P}}(X) < 1/2\}$. If $\mu(\mathcal{H}) > 0$ then there exist some $\hat{s} < 1/2$ such that $\mu(\hat{\mathcal{H}}) > 0$ where $\hat{\mathcal{H}} = \{X \in \mathcal{F} : \dim_{\text{P}}(X) < \hat{s}\}$. By using the partitioning argument along with the gale combination technique in the in the proof of Theorem 8.1 over the set $\hat{\mathcal{H}}$ instead of $\mathcal{F}$, we obtain a contradiction to the second statement in the hypothesis of the lemma. Therefore, it must be the case that $\mu(\mathcal{H}) = 0$ which completes the proof of the lemma. □

# 9 Sets and sequences with maximal gap between $\mathcal{K}^{\text{str}}_{\text{poly}}$ and $\dim_{\text{P}}$

In this section we prove that if one-way functions exist, the gap between $\dim_{\text{P}}$ and $\mathcal{K}^{\text{str}}_{\text{poly}}$ can be arbitrarily close to 1.

**Theorem 9.1.** *If one-way functions exist, then for every $\epsilon > 0$ there exist set $\mathcal{F}$ and sequence $X$ such that $\dim_{\text{P}}(\mathcal{F}) - \mathcal{K}^{\text{str}}_{\text{poly}}(\mathcal{F}) \geq 1 - \epsilon$ and $\dim_{\text{P}}(X) - \mathcal{K}^{\text{str}}_{\text{poly}}(X) \geq 1 - \epsilon$ respectively.*

We prove the existence of a sequence $X$ such that $\dim_{\text{P}}(X) - \mathcal{K}^{\text{str}}_{\text{poly}}(X) \geq 1 - \epsilon$. The assertion for sets follows trivially from this claim. Let $s = 2^{-m}$ for some $m > 1$. We have $s < 1/2$ and therefore $2s < 1$. Consider the set $\mathcal{F}'_{2s} = \{X \in \Sigma^\infty : \limsup_{n\to\infty} \frac{K_{t_g}(X\restriction n)}{n} \leq 2s\}$. For any $X \in \mathcal{F}'_{2s}$,

$$\mathcal{K}^{\text{str}}_{\text{poly}}(X) = \inf_{t \in poly} \limsup_{n\to\infty} \frac{K_t(X \restriction n)}{n} \leq 2s.$$

We argue that there does exist any $s' < 1$ satisfying $2s < s' < 1$ and $2^{s'} \in \mathbb{Q}$ such that $\dim_{\text{P}}(X) < s'$ for every $X \in \mathcal{F}'_{2s}$. Assume that for some such $s'$ and every $X \in \mathcal{F}'_{2s}$ there exists an exact computable $s'$-gale $d'_X$ that runs in time $t_{d'_X}(n) \in \text{poly}(n)$, such that $d'_X$ succeeds on $X$.

As in the proof of Theorem 1.6, we construct the mapping $g : \Sigma^\infty \to \Sigma^\infty$ as in Definition 4.1. For any $X \in \Sigma^\infty$, from Corollary 4.1, it follows that $g(X) \in \mathcal{F}_{2s'}$. Therefore, $g(\Sigma^\infty) \subseteq \mathcal{F}_{2s'}$.

So, every $X \in \Sigma^\infty$ there exists an exact computable $s'$-gale $d'_X$ that runs in time $t_{d'_X}(n) \in \text{poly}(n)$, such that $d'_X$ succeeds on $g(X)$. Similar to the proof of Theorem 1.7, using a gale combination technique, we construct a set $\mathcal{S} \subseteq \Sigma^\infty$ such that $\mu(\mathcal{S}) > 0$ and a single $s$-gale $d'$ that succeeds on $g(X)$ for all $X \in \mathcal{S}$.

We first partition sequences in the input space of $g$ into sets, based on the running time of the $s'$-gales that succeeds on it. Define

$$R_i = \{X \in \Sigma^\infty : \text{ there exists an } n^i\text{-time } s'\text{-gale } d \text{ such that } g(X) \in S^\infty(d)\}$$

and let $S_i = R_i \setminus R_{i-1}$. Note that $\{S_i\}_{i\in\mathbb{N}}$ is a partition of $\Sigma^\infty$ into countably many disjoint subsets. As $\sum_{i=1}^\infty \mu(S_i) = 1$, there exists an $k \in \mathbb{N}$ such that $\sum_{i=1}^k \mu(S_i) > 0$. Define $\mathcal{S} = \bigcup_{i=1}^k S_i$.

Now, using Lemma 8.1, there exists an exact $t(n)$-time computable $s'$-gale $d'$ that succeeds on all sequences in $g(\mathcal{S})$ for some polynomial $t(n)$.

Now, using Lemma 8.1, there exists an exact $t(n)$-time computable $s'$-gale $d'$ that succeeds on all sequences in $g(\mathcal{S})$ for some polynomial $t(n)$. The major tool we require is the following generalization of Lemma 5.2 to any $s' < 1$.

**Lemma 9.1.** *For $s' < 1$, let $d' : \Sigma^\infty \to [0, \infty)$ be an exact $t(n)$-time computable $s'$-gale. Let $\tilde{s}$ and $s''$ be such that $\tilde{s} > s'' > s'$, $2^{\tilde{s}} \in \mathbb{Q}$ and $2^{s''} \in \mathbb{Q}$. Then, there exists an exact $t(n)poly(n)$-time computable martingale $\tilde{d} : \Sigma^\infty \to [0, \infty)$ such that for any $X \in S^\infty(d')$, there exists infinitely many $n \in \mathbb{N}$ satisfying at least one of the following:*

1. *$\tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1})$.*
2. *There exists $\ell$ satisfying $((\tilde{s} - s'')/s'') \cdot 2^{n-1} \leq \ell \leq 2^{n-1}$ such that $\tilde{d}(X \upharpoonright 2^{n-1} + \ell) > 2^{(1-s'')(2^{n-1}+\ell)}$.*

*Proof.* Let $\tilde{d}$ be the exact $t(n)poly(n)$-time computable martingale from Lemma 5.1 such that,

$$\limsup_{n\to\infty} \frac{\tilde{d}(X \upharpoonright n)}{2^{(1-s'')n}} = \infty.$$

We show that $\tilde{d}$ satisfies the required property. On the contrary, assume that there exists $m > 0$ such that for every $n > m$, $\tilde{d}(X \upharpoonright 2^n) \leq 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1})$ and $\tilde{d}(X \upharpoonright 2^n + \ell) \leq 2^{(1-s'')(2^{n-1}+\ell)}$ for every $\ell$ such that $((\tilde{s} - s'')/s'') \cdot 2^{n-1} \leq \ell \leq 2^{n-1}$. Since, there exist infinitely many $k$ such that $\tilde{d}(X \upharpoonright k) \geq 2^{(1-s'')k}$, we obtain that infinitely many $n$ and $\ell \leq ((\tilde{s} - s'')/s'') \cdot 2^{n-1}$ should satisfy,

$$\tilde{d}(X \upharpoonright 2^{n-1} + \ell) > 2^{(1-s'')(2^{n-1}+\ell)}. \tag{12}$$

But for any large enough $n$ and $\ell$ satisfying $\ell \leq ((\tilde{s} - s'')/s'') \cdot 2^{n-1}$, we have

$$\begin{aligned}\tilde{d}(X \upharpoonright 2^{n-1} + \ell) &\leq 2^\ell 2^{(1-\tilde{s})\sum_{i=m}^{n-2} 2^i} \tilde{d}(X \upharpoonright 2^m) \\ &= 2^\ell 2^{(1-\tilde{s})(2^{n-1}-2^m)} \tilde{d}(X \upharpoonright 2^m).\end{aligned}$$

From 12, we obtain

$$2^{\ell s''} \geq \frac{2^{(1-\tilde{s})2^m}}{\tilde{d}(X \upharpoonright 2^m)} 2^{2^{n-1}(\tilde{s}-s'')}.$$

Since $\ell \leq ((\tilde{s} - s'')/s'') \cdot 2^n$,

$$2^{2^{n-1}(\tilde{s}-s'')} \leq \frac{\tilde{d}(X \upharpoonright 2^m)}{2^{(1-\tilde{s})2^m}}. \tag{13}$$

Since $\tilde{s} > s''$, the above cannot be true for large enough $n$. So, we obtain a contradiction. Therefore, it must be the case that there exist infinitely many $n$ satisfying conditions 1 or 2. □

**Definition 9.1.** *Let $f' : \Sigma^\infty \times \mathbb{N} \to \{0, 1\}$ be defined as follows. $f'(X, n) = 1$ if either of the following are true:*

1. *$\tilde{d}(g(X) \upharpoonright 2^n) > 2^{(1-\tilde{s})2^n} \tilde{d}(g(X) \upharpoonright 2^{n-1})$.*
2. *There exists $\ell$ satisfying $((\tilde{s} - s'')/s'') \cdot 2^{n-1} \leq \ell \leq 2^{n-1}$ such that $\tilde{d}(g(X) \upharpoonright 2^{n-1} + \ell) > 2^{(1-s'')(2^{n-1}+\ell)}$.*

*Otherwise we define* $f'(X, n) = 0$.

Now, we prove an analogue of Lemma 5.4 for the new function $f'$. The proof is identical to that of Lemma 5.4 and uses the Borel-Cantelli lemma.

**Lemma 9.2.** *Given* $\tilde{d} : \Sigma^\infty \to [0, \infty)$*, if for all sequences* $Y \in g(\mathcal{S})$ *where* $\mu(\mathcal{S}) > 0$*, there exists infinitely many* $n \in \mathbb{N}$ *satisfying at least one of the following:*

1. $\tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1})$.
2. *There exists* $\ell$ *satisfying* $((\tilde{s} - s'')/s'') \cdot 2^{n-1} \leq \ell \leq 2^{n-1}$ *such that* $\tilde{d}(X \upharpoonright 2^{n-1} + \ell) > 2^{(1-s'')(2^{n-1}+\ell)}$.

*For any* $n > 0$*, let* $\mathcal{H}_n$ *be the set of strings in* $\Sigma^{s.2^n}$ *such that* $\tilde{d}(g(x)) > 2^{(1-\tilde{s})2^n} \tilde{d}(g(x \upharpoonright s.2^{n-1}))$ *or there exists* $\ell$ *satisfying* $((\tilde{s} - s'')/s'') \cdot 2^{n-1} \leq \ell \leq 2^{n-1}$ *such that* $\tilde{d}(x \upharpoonright 2^{n-1} + \ell) > 2^{(1-s'')(2^{n-1}+\ell)}$*. Then it holds that for infinitely many* $n$*,*

$$\Pr_{x \in \Sigma^{s.2^n}} [x \in \mathcal{H}_n] \geq \frac{1}{n^2}.$$

Let $q$ be a rational number such that

$$0 < \frac{(\tilde{s} - s'')}{2s''} \leq q \leq \frac{(\tilde{s} - s'')}{s''}.$$

Now we modify Algorithm A (see Algorithm 2) such that the last step is,

**return** $\tilde{d}(w'w) \geq 2^{(1-\tilde{s})|w|} \cdot \tilde{d}(w')$ **or** $\tilde{d}(w'w) \geq 2^{(1-\tilde{s})(2^n+\ell)}$ for some $\ell$ such that $q \cdot 2^n \leq \ell \leq 2^n$.

The analysis to prove that for $N = 2^n$,

$$\Pr_{(x,r) \in \Sigma^{s \cdot N} \times \Sigma^{s \cdot N}} [A(G_N(x)) = 1] \geq \frac{1}{N^2}.$$

is quite similar to the one in the proof of Lemma 1.1. The only difference is that instead of Lemma 5.4, we use Lemma 9.2.

Now, for any $n \in \mathbb{N}$, take any $r \in \Sigma^{s.2^n}$, and let $w' = g(r)$. Using Lemma 5.5, for any $w' \in \Sigma^{2^n}$, the number of strings $w \in \Sigma^{2^n}$ such that $d(w'w) \geq 2^{2^n \cdot (1-\tilde{s})} d(w')$ is less than $2^{2^n}/2^{2^n(1-\tilde{s})}$. Again, using Lemma 5.5, the number of strings $w'w \in \Sigma^{2^{n+1}}$ such that $\tilde{d}(w'w) \geq 2^{(1-\tilde{s})(2^n+\ell)}$ for some $\ell$ such that $q \cdot 2^n \leq \ell \leq 2^n$ is at most $2^{2^{n+1}}/2^{(1-\tilde{s})(2^n+q2^n)}$. Let $N = 2^n$. Now, using the union bound it follows that,

$$\Pr_{(x,r) \in \Sigma^N \times \Sigma^N} [A(x) = 1] < \frac{1}{2^{N(1-\tilde{s})}} + \frac{1}{2^{(1-\tilde{s})(1+q)N}}.$$

Notice that $q$ is a constant which depends only on $\tilde{s}$ and $s''$.

It follows that if one-way functions exist, for every $s' < 1$ with $2^{s'} \in \mathbb{Q}$ there exist $X \in g(\Sigma^\infty)$ such that $\dim_P(X) \geq s'$. Since $\mathrm{Dim}_P(X) \geq \dim_P(X)$, for every $s' \in (2s, 1)$ with $2^{s'} \in \mathbb{Q}$ there exist $X \in g(\mathcal{S})$ such that $\mathrm{Dim}_P(X) \geq s'$. Now, Theorem 9.1 follows from the observation that by taking $m$ large enough and choosing an appropriate $s'$, the quantity $s' - 2s = s' - 2^{-m-1}$ can be made arbitrarily close to 1.

We obtain the following corollary of Theorem 9.1. These results provide a strong negative answer to the open question posed by Stull in [Stu20] under the assumption that one-way functions exist.

**Corollary 9.1.** *If one-way functions exist then for every $\epsilon < 1/2$ there exists $\mathcal{F} \subseteq \Sigma^\infty$ such that,*

$$\mathcal{K}_{\text{poly}}(\mathcal{F}) \leq \mathcal{K}^{\text{str}}_{\text{poly}}(\mathcal{F}) < \epsilon < 1 - \epsilon < \dim_{\text{P}}(\mathcal{F}) \leq \text{Dim}_{\text{P}}(\mathcal{F})$$

**Corollary 9.2.** *If one-way functions exist then for every $\epsilon < 1/2$ there exists $X \in \Sigma^\infty$ such that,*

$$\mathcal{K}_{\text{poly}}(X) \leq \mathcal{K}^{\text{str}}_{\text{poly}}(X) < \epsilon < 1 - \epsilon < \dim_{\text{P}}(X) \leq \text{Dim}_{\text{P}}(X).$$

# 10 Remarks on dimension gaps and infinitely-often one-way functions

Our main theorem (Theorem 1.5) shows that one-way functions implies the existence of polynomial time samplable distributions with respect to which dimension gaps exist on a probability 1 set. This assertion in turn implies the existence of infinitely-often one-way functions. In this section we remark on the possibility of proving that either one-way functions or infinitely-often one-way functions are equivalent to the existence of polynomial time samplable distributions with respect to which dimension gaps exist on a probability 1 set.

Consider the statement of Lemma 1.1. It is unlikely that the weaker hypothesis of existence of infinitely-often one-way functions yields the conclusion of Lemma 1.1 using the methods in the proof of the main theorem. In order to prove the conclusion of the lemma from the existence of infinitely-often one-way functions we need to break the PRG $\{G_n\}$ at all but finitely many lengths $n$. In our proof method, this requires that the following condition from Lemma 5.4,

$$\Pr_{x \sim \Sigma^{s.2^n}}[\tilde{d}(g(x)) > 2^{(1-\tilde{s})2^n} \tilde{d}(g(x \upharpoonright s.2^{n-1}))] \geq \frac{1}{n^2}$$

is true for all but finitely many $n$. This in turn requires that the following condition from Lemma 5.2,

$$\tilde{d}(X \upharpoonright 2^n) > 2^{(1-\tilde{s})2^{n-1}} \tilde{d}(X \upharpoonright 2^{n-1})$$

is true for all but finitely many $n$ whenever there exist an $s'$-gale $d'$ that wins on $X$. However, the existence of an $s'$-gale $d'$ that wins on $X$ need not imply that there exists a martingale that roughly doubles it capital on half of the bits of $X$ from index $2^{n-1}$ to $2^n$ for all but finitely many $n$. If this happens, then by transforming the martingale $\tilde{d}$ to an $s'$-gale $d'$ (using the inverse of the transformation in Lemma 5.1), we obtain that

$$d'(X \upharpoonright 2^n) > \frac{1}{2^{(\tilde{s}-s')2^{n-1}}} \cdot d'(X \upharpoonright 2^{n-1})$$

for all but finitely many $n$. However, an $s'$-gale $d'$ winning on $X$ need not respect this bound for all but finitely many $n$. $d'$ may violate this inequality infinitely many times and still manage to gain sufficient capital infinitely often to win on $X$.

Now, consider the statement of Lemma 1.2. The main technical hurdle in obtaining a one-way function in the conclusion of Lemma 1.2 is that assuming the non-existence of one-way functions, the approximation algorithm $\mathcal{A}$ from Theorem 6.1 may only succeed in approximating $\mathcal{D}_n$ for infinitely many values of $n$. Therefore, the $s'$-supergale $d$ in the proof of Lemma 1.2 can only be approximated on infinitely many input string lengths $n$.

However using the same techniques as in the proof of Lemma 1.2, we can obtain the following lemma which shows that if dimension gaps exists between $\dim_{\text{P}}$ defined using gales which are only approximable on infinitely many lengths and $\mathcal{K}^{\text{str}}_{\text{poly}}$, then one-way functions exist.

**Lemma 10.1.** *If for some $s < 1$ there exist a polynomial time samplable distribution $\nu$ over $\Sigma^\infty$ such that:*

1. $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(X) \leq s$ *for almost every* $X \sim \nu$.
2. *There exist some* $\hat{s} \in (s, 1]$ *such that for every* $s' \in (s, \hat{s})$ *and any polynomial-time* $s'$*-supergale* $d$ *that is* $\nu$***-approximable on infinitely many input lengths****, we have* $\nu(S^\infty(d)) = 0$.

*Then,* ***one-way functions*** *exist.*

The proof is essentially identical to that of Lemma 1.2 except that we use the universal extrapolation result Theorem 19 instead of Theorem 20 from [IRS22].

# 11 Additional Proofs

Below we give an alternative proof of the fact that $\dim_{\mathrm{P}}$ dominates $\mathcal{K}_{\mathrm{poly}}$ from [HV06, HV04]. We also prove the analogous inequality for polynomial time strong dimension.

**Theorem 11.1** ([HV04, HV06])**.** *For every* $\mathcal{F} \subseteq \Sigma^\infty$, $\mathcal{K}_{\mathrm{poly}}(\mathcal{F}) \leq \dim_{\mathrm{P}}(\mathcal{F})$ *and* $\mathcal{K}^{\mathrm{str}}_{\mathrm{poly}}(\mathcal{F}) \leq \mathrm{Dim}_{\mathrm{P}}(\mathcal{F})$.

We need the following lemma to prove the above theorem.

**Lemma 11.1.** *Let* $[a, b]$ *be a sub-interval of* $[0, 1]$. *Then, there exist* $m \leq \lfloor \log(1/(b-a)) \rfloor$ *and* $j < 2^{m+2}$ *such that,*

$$\left[\frac{j}{2^{m+2}}, \frac{j+1}{2^{m+2}}\right] \subseteq [a, b].$$

*Proof.* Let $m = \lfloor -\log(b-a) \rfloor$. Among the set of all intervals of the form $[k/2^m, k + 1/2^m]$, let $I_m$ be the interval which maximizes the length of $I_m \cap [a, b]$ (if there are two such intervals, choose any of them). Consider the following sub-intervals of $I_m$,

$$\left[\frac{4k}{2^{m+2}}, \frac{4k+1}{2^{m+2}}\right], \left[\frac{4k+1}{2^{m+2}}, \frac{4k+2}{2^{m+2}}\right], \left[\frac{4k+2}{2^{m+2}}, \frac{4k+3}{2^{m+2}}\right] \text{ and } \left[\frac{4k+3}{2^{m+2}}, \frac{4k+4}{2^{m+2}}\right].$$

If none of the above are completely contained in $[a, b]$, then the length of $I_m \cap [a, b]$ is at most $1/2^{m+2}$. From the choice of $I_m$, it follows that then length of $[a, b]$ is at most $1/2^{m+1}$. Therefore, $m = \lfloor -\log(b-a) \rfloor \geq m + 1$ which is a contradiction. Therefore, one of the above sub-intervals of $I_m$ satisfies the required condition. □

Now, we prove Theorem 1.3.

*Proof of Theorem 1.3.* Let $d : \Sigma^\infty \to \mathbb{Q}$ be an exact $s$-gale that runs in time $t$ such that $d$ succeeds on all $X \in \mathcal{F}$. We show that for all $X \in \mathcal{F}$, $\liminf_{n\to\infty} \frac{K_{t'}(X\upharpoonright n)}{n} \leq s$, where $t'(n) = \mathrm{poly}(t(n))$.

Given $n \in \mathbb{N}$, let $S_n = \{x \in \Sigma^n : d(x) > 1\}$. From the Lemma 5.5, it follows that $|S_n| < 2^{sn}$. For $x \in S_n$, we now define an encoding $\mathcal{E}(x)$ that takes at most $sn + O(1)$ bits.

**Encoding**: For any $n \in \mathbb{N}$ and $x \in \Sigma^n$, letting $p(x) = d(x).2^{-sn}$ we obtain a probability distribution over $\Sigma^n$. For every $n$, define the cumulative probability $c_n(x) = \sum_{y\in\Sigma^n,\, y<x} p(y)$, where $y < x$ means that $y$ is less than $x$ in the lexicographic ordering. If $d(x) > 1$, then $p(x) > 2^{-sn}$. Hence $c_n(x+1) - c_n(x) > 2^{-sn}$. Here $x+1$ is the $n$-length successor of $x$ in the lexicographic order. Also, we assume that $c_n(1^n + 1) = 1$.

From Lemma 11.1, there exist a dyadic interval $[j/2^{m+2}, (j+1)/2^{m+2}]$ that is totally contained in $[c_n(x), c_n(x+1)]$. Define $\mathcal{E}(x)$ to be the binary encoding of this dyadic interval. From Lemma 11.1, we have

$$|\mathcal{E}(x)| \leq m+2 \leq \left\lfloor \log \frac{1}{c_n(x+1) - c_n(x)} \right\rfloor + 2 \leq \lfloor \log 2^{sn} \rfloor + 2 = sn + O(1).$$

Hence, it follows that $\mathcal{E}$ defines a one to one encoding from $S_n \to \Sigma^*$ such that $|\mathcal{E}(x)| < sn + O(1)$. for every $x \in S_n$.

**Decoding**: We will now give a $\text{poly}(t(n))$ procedure that uses $d$ to generate an $x \in \Sigma^n$, given $\mathcal{E}(x)$ as input. The idea is that we perform a binary search over $\Sigma^n$ using the exact polynomial time computable $s$-gale $d$ and the input encoding $\mathcal{E}(x)$.

Given $\mathcal{E}(x) \in \Sigma^{sn}$, observe that the dyadic interval $[j/2^{m+2}, (j+1)/2^{m+2}]$ encoded by $\mathcal{E}(x)$ is totally contained in $[c_n(x), c_n(x+1)]$ for some $x \in \Sigma^n$.

**Algorithm 3** Decoding Algorithm. Input $w$

```
Set x_0 = λ, c_0(x_0) = 0
Compute the dyadic interval I such that w is an encoding of I
for i = 0 to n − 1 do
    if I ⊆ [c_i(x_i), c_i(x_i) + p(x_i.0)] then
        Set x_{i+1} = x_i.0
        Set c_{i+1}(x_{i+1}) = c_{i+1}(x_i)
    else
        Set x_{i+1} = x_i.1
        Set c_{i+1}(x_{i+1}) = c_{i+1}(x_i) + p(x_i.0)
    end if
end for
```

**Running time of the algorithm:** Since $d$ is exact computable $2^{-s}$ is rational and hence $p(y) = d(y)2^{-s|y|}$ can be computed in time polynomial in $t(|w|)$ for any $y$ with length less than or equal to that of $w$. Every other step in the algorithm can be performed in polynomial time. Therefore on input $w$, the algorithm terminates in $\text{poly}(t(n))$ steps.

**Correctness:** At each step in the main loop of the algorithm, we keep track of the cumulative probability $c_i(x_i)$ for the current node as a running sum. On input $\mathcal{E}(x)$ for some $x \in \Sigma^n$, we are guaranteed that the interval $I$ encoded by $\mathcal{E}(x)$ satisfies $I \subseteq [c_n(x), c_n(x+1)]$. At step 0, either $I \subseteq [0, p(0)]$ or $I \subseteq [p(0), p(1)]$. A simple inductive argument shows that at every step $i$, either $I \subseteq [c_i(x_i), c_i(x_i) + p(x_i.0)]$ or $I \subseteq [c_i(x_i) + p(x_i.0), c_i(x_i) + p(x_i.0) + p(x_i.1)]$.

The above conclusion implies that at the end of step $i$, $I \subseteq [c_{i+1}(y), c_{i+1}(y+1)]$ for some $y \in \Sigma^{i+1}$. therefore, at the end of the loop $I \subseteq [c_n(y), c_n(y+1)]$ for some $y \in \Sigma^n$. From the definition of the encoding $\mathcal{E}$, it follows that the algorithm on input $\mathcal{E}(x)$ for $x \in \Sigma^n$ terminates with $x_n = x$.

**Conclusion:** Given $\mathcal{F} \subseteq \Sigma^\infty$ and $s > \dim_P(\mathcal{F})$ such that $2^s \in \mathbb{Q}$. There exists an $s$-gale $d$ that succeeds on all $X \in \mathcal{F}$, we have that for every $X \in \mathcal{F}$, for infinitely many $n \in \mathbb{N}$, $d(X \upharpoonright n) \geq 1$. From the above algorithm it follows that, $\liminf_{n\to\infty} K_{\text{poly}(t(n))}/n \leq s$ and so $\mathcal{K}_{\text{poly}}(\mathcal{F}) \leq s$. Hence we conclude that for every $\mathcal{F} \subseteq \Sigma^\infty$, $\mathcal{K}_{\text{poly}}(\mathcal{F}) \leq \dim_P(\mathcal{F})$. This proves the first inequality.

Similarly, let $s > \text{Dim}_P(\mathcal{F})$. then there exists an $s$-gale $d$ such that $d$ strongly succeeds on all $X \in \mathcal{F}$. It follows that for every $X \in \mathcal{F}$, for all but finitely many $n \in \mathbb{N}$, $d(X \upharpoonright n) \geq 1$. Therefore using the above algorithm we obtain, $\limsup_{n\to\infty} K_{\text{poly}(t(n))}/n \leq s$ and so $\mathcal{K}^{\text{str}}_{\text{poly}}(\mathcal{F}) \leq s$. Hence we conclude that for every $\mathcal{F} \subseteq \Sigma^\infty$, $\mathcal{K}^{\text{str}}_{\text{poly}}(\mathcal{F}) \leq \text{Dim}_P(\mathcal{F})$. □

## Acknowledgments

The authors would like to thank CS Bhargav, Laurent Bienvenu, John Hitchcock, Jaikumar Radhakrishnan, Mahesh Sreekumar Rajasree and Marius Zimand for helpful comments and discussions.

## References

[ACM+21] Eric Allender, Mahdi Cheraghchi, Dimitrios Myrisiotis, Harsha Tirumala, and Ilya Volkovoch. One-way functions and a conditional variant of mktp. In *41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2021)*, volume 213, pages 7–1. Schloss Dagstuhl–Leibniz-Zentrum fur Informatik, 2021.

[AHLM07] Krishna B Athreya, John M Hitchcock, Jack H Lutz, and Elvira Mayordomo. Effective strong dimension in algorithmic information and computational complexity. *SIAM journal on computing*, 37(3):671–705, 2007.

[Bil95] Patrick Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons, Inc., New York, third edition, 1995. A Wiley-Interscience Publication.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi:10.1109/TIT.1976.1055638.

[DH10] Rodney G. Downey and Denis R. Hirschfeldt. *Algorithmic randomness and complexity*. Theory and Applications of Computability. Springer, New York, 2010. doi:10.1007/978-0-387-68441-3.

[FS90] Uriel Feige and Adi Shamir. Witness indistinguishable and witness hiding protocols. In Harriet Ortiz, editor, *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 416–426. ACM, 1990. doi:10.1145/100216.100272.

[GK22] Halley Goldberg and Valentine Kabanets. A simpler proof of the worst-case to average-case reduction for polynomial hierarchy via symmetry of information. *Electron. Colloquium Comput. Complex.*, TR22, 2022. URL: https://api.semanticscholar.org/CorpusID:246653509.

[GKLO22] Halley Goldberg, Valentine Kabanets, Zhenjian Lu, and Igor C. Oliveira. Probabilistic Kolmogorov Complexity with Applications to Average-Case Complexity. In Shachar Lovett, editor, *37th Computational Complexity Conference (CCC 2022)*, volume 234 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:60, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2022.16, doi:10.4230/LIPIcs.CCC.2022.16.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984. URL: https://www.sciencedirect.com/science/article/pii/0022000084900709, doi:https://doi.org/10.1016/0022-0000(84)90070-9.

[Gol01] Oded Goldreich. *Foundations of Cryptography*. Cambridge University Press, 2001.

[Gol08] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 2008.

[HIL+23] Shuichi Hirahara, Rahul Ilango, Zhenjian Lu, Mikito Nanashima, and Igor C Oliveira. A duality between one-way functions and average-case symmetry of information. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1039–1050, 2023.

[HILL99] Johan HÅstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999. arXiv:https://doi.org/10.1137/S0097539793244708, doi:10.1137/S0097539793244708.

[Hir22] Shuichi Hirahara. Symmetry of Information from Meta-Complexity. In Shachar Lovett, editor, *37th Computational Complexity Conference (CCC 2022)*, volume 234 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 26:1–26:41, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2022.26, doi:10.4230/LIPIcs.CCC.2022.26.

[Hir23] Shuichi Hirahara. Capturing one-way functions via NP-hardness of meta-complexity. In *STOC'23—Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1027–1038. ACM, New York, [2023] ©2023. doi:10.1145/3564246.3585130.

[Hit03] John M Hitchcock. *Effective fractal dimension: foundations and applications*. Iowa State University, 2003.

[HLO24] Shuichi Hirahara, Zhenjian Lu, and Igor C. Oliveira. One-way functions and pKt complexity. Cryptology ePrint Archive, Paper 2024/1388, 2024. URL: https://eprint.iacr.org/2024/1388.

[HV04] J.M. Hitchcock and N.V. Vinodchandran. Dimension, entropy rates, and compression. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, pages 174–183, 2004. doi:10.1109/CCC.2004.1313835.

[HV06] John M. Hitchcock and N.V. Vinodchandran. Dimension, entropy rates, and compression. *Journal of Computer and System Sciences*, 72(4):760–782, 2006. URL: https://www.sciencedirect.com/science/article/pii/S0022000005001248, doi:https://doi.org/10.1016/j.jcss.2005.10.002.

[IL89] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *30th Annual Symposium on Foundations of Computer Science*, pages 230–235, 1989. doi:10.1109/SFCS.1989.63483.

[IL90] R. Impagliazzo and L.A Levin. No better ways to generate hard np instances than picking uniformly at random. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 812–821 vol.2, 1990. doi:10.1109/FSCS.1990.89604.

[IRS22] Rahul Ilango, Hanlin Ren, and Rahul Santhanam. Robustness of average-case meta-complexity via pseudorandomness. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1575–1583, 2022.

[KC00] Valentine Kabanets and Jin-Yi Cai. Circuit minimization problem. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, STOC '00, page 73–79, New York, NY, USA, 2000. Association for Computing Machinery. doi:10.1145/335305.335314.

[Kol65] Andrei N Kolmogorov. Three approaches to the quantitative definition ofinformation'. *Problems of information transmission*, 1(1):1–7, 1965.

[Lev03] L. A. Levin. The tale of one-way functions. *Probl. Inf. Transm.*, 39(1):92–103, January 2003. doi:10.1023/A:1023634616182.

[LM93] Luc Longpré and Sarah Mocas. Symmetry of information and one-way functions. *Information Processing Letters*, 46(2):95–100, 1993. URL: https://www.sciencedirect.com/science/article/pii/002001909390204M, doi:https://doi.org/10.1016/0020-0190(93)90204-M.

[LO22] Zhenjian Lu and Igor C Oliveira. Theory and applications of probabilistic kolmogorov complexity. *Bulletin of EATCS*, 137, 2022.

[LP20] Yanyi Liu and Rafael Pass. On one-way functions and kolmogorov complexity. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1243–1254. IEEE, 2020.

[LP21] Yanyi Liu and Rafael Pass. On one-way functions from np-complete problems. *Cryptology ePrint Archive*, 2021.

[Lut03a] Jack H. Lutz. Dimension in complexity classes. *SIAM J. Comput.*, 32(5):1236–1259, 2003. doi:10.1137/S0097539701417723.

[Lut03b] Jack H. Lutz. The dimensions of individual strings and sequences. *Information and Computation*, 187(1):49–79, 2003. URL: https://www.sciencedirect.com/science/article/pii/S0890540103001871, doi:https://doi.org/10.1016/S0890-5401(03)00187-1.

[LV08] Ming Li and Paul Vitányi. *An introduction to Kolmogorov complexity and its applications*, volume 3. Springer, 2008.

[LW92] Luc Longpré and Osamu Watanabe. On symmetry of information and polynomial time invertibility. In Toshihide Ibaraki, Yasuyoshi Inagaki, Kazuo Iwama, Takao Nishizeki, and Masafumi Yamashita, editors, *Algorithms and Computation*, pages 410–419, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

[May02] Elvira Mayordomo. A Kolmogorov complexity characterization of constructive Hausdorff dimension. *Inform. Process. Lett.*, 84(1):1–3, 2002. doi:10.1016/S0020-0190(02)00343-5.

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *J. Cryptol.*, 4(2):151–158, January 1991. doi:10.1007/BF00196774.

[Nie09] Andre Nies. *Computability and Randomness*. Oxford University Press, Inc., USA, 2009.

[Rom90] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *Symposium on the Theory of Computing*, 1990. URL: https://api.semanticscholar.org/CorpusID:10858937.

[Roy88] H. L. Royden. *Real Analysis*. Prentice Hall, 1988.

[RS98] K.W. Regan and D. Sivakumar. Probabilistic martingales and bptime classes. In *Proceedings. Thirteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat. No.98CB36247)*, pages 186–200, 1998. doi:10.1109/CCC.1998.694604.

[S+63] George F Simmons et al. Introduction to topology and modern analysis. 1963.

[Stu20] Donald M. Stull. *Resource bounded randomness and its applications*, page 301–348. Lecture Notes in Logic. Cambridge University Press, 2020.

[SUV22] A. Shen, V.A. Uspensky, and N. Vereshchagin. *Kolmogorov Complexity and Algorithmic Randomness*. Mathematical Surveys and Monographs. American Mathematical Society, 2022. URL: https://books.google.fr/books?id=WhZuEAAAQBAJ.

[Vad12] Salil P. Vadhan. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012. URL: http://dx.doi.org/10.1561/0400000010, doi:10.1561/0400000010.

[Yao82] Andrew C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 160–164, 1982. doi:10.1109/SFCS.1982.38.



ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il