Electronic Colloquium on Computational Complexity, Report No. 119 (2025)

Counting Martingales for Measure and Dimension in Complexity Classes

John M. Hitchcock * Adewale Sekoni † Hadi Shafei ‡

Abstract

This paper makes two primary contributions. First, we introduce the concept of *counting martingales* and use it to define *counting measures*, *counting dimensions*, and *counting strong dimensions*. Second, we apply these new tools to strengthen previous *circuit lower bounds*.

Resource-bounded measure and dimension have traditionally focused on deterministic time and space bounds. We use counting complexity classes to develop resource-bounded counting measures and dimensions. Counting martingales are constructed using functions from the #P, SpanP, and GapP complexity classes. We show that counting martingales capture many martingale constructions in complexity theory. The resulting counting measures and dimensions are intermediate in power between the standard time-bounded and space-bounded notions, enabling finer-grained analysis where space-bounded measures are known, but time-bounded measures remain open. For example, we show that BPP has #P-dimension 0 and BQP has GapP-dimension 0, whereas the P-dimensions of these classes remain open.

As our main application, we improve circuit-size lower bounds. Lutz (1992) strengthened Shannon's classic $(1-\epsilon)\frac{2^n}{n}$ lower bound (1949) to PSPACE-measure, showing that almost all problems require circuits of size $\frac{2^n}{n}\left(1+\frac{\alpha \log n}{n}\right)$, for any $\alpha < 1$. We extend this result to SpanP-measure, with a proof that uses a connection through the Minimum Circuit Size Problem (MCSP) to construct a counting martingale. Our results imply that the stronger lower bound holds within the third level of the exponential-time hierarchy, whereas previously, it was only known in ESPACE. Under a derandomization hypothesis, this lower bound holds within the second level of the exponential-time hierarchy, specifically in the class E^{NP}. We study the #P-dimension of classical circuit complexity classes and the GapP-dimension of quantum circuit complexity classes. We also show that if one-way functions exist, then #P-dimension is strictly more powerful than P-dimension.

*Department of Electrical Engineering and Computer Science, University of Wyoming. jhitchco@uwyo.edu. This research was supported in part by NSF grant 2431657.

†Department of Mathematics, Computer Science & Physics, Roanoke College. sekoni@roanoke.edu.

‡School of Computing and Engineering, University of Huddersfield. H.Shafei@hud.ac.uk.

ISSN 1433-8092

Contents

List of Figures

1 Introduction

Resource-bounded measures and dimensions [9, 53–55, 57] are fundamental tools for analyzing complexity classes, offering refined ways to understand the power and limitations of different computational resources [4, 37, 56, 61]. Traditional approaches based on real-valued martingales provide insights into classes like P, NP, PSPACE, and EXP, but they leave gaps when it comes to many intermediate complexity classes. This paper introduces counting martingales, which offer a new perspective on these intermediate classes by utilizing functions from counting complexity classes.

Our main contributions are:

1. Counting Martingales and Counting Measures and Dimensions: We introduce *counting martingales*, which generalize traditional martingales by incorporating functions from counting complexity classes [20, 46, 50, 84], creating intermediate *counting measures and dimensions*. For instance, we define $\#\mathsf{P}$-measure, SpanP-measure, and GapP-measure as intermediate measures between P-measure and PSPACE-measure, allowing finer analysis of complexity classes.

2. Applications to Circuit Complexity: Using these new measures, we provide novel results on nonuniform complexity and the Shannon-Lupanov bound [52, 78]. Shannon's $(1-\epsilon)\frac{2^n}{n}$ lower bound was improved by Lutz [55] who showed that for any $\alpha < 1$, almost all problems require circuits of size $\frac{2^n}{n}\left(1+\frac{\alpha \log n}{n}\right)$. We improve this result further by extending it to SpanP-measure. In our proof, we construct a counting martingale using a connection through the Minimum Circuit Size Problem (MCSP). Moreover, we study classical and quantum circuit complexity classes using $\#\mathsf{P}$-dimension and GapP-dimension, respectively.

The standard definitions of resource-bounded measure use martingales that are real-valued functions computable within deterministic time and space resource bounds [55]. In this paper, we use the counting complexity classes $\#\mathsf{P}$ [84], SpanP [46], and GapP [20, 50] to introduce the concept of *counting martingales* and define *counting measures*, *counting dimensions*, and *counting strong dimensions* that are intermediate in power between the previous time- and space-bounded measures and dimensions. A $\#\mathsf{P}$ function counts the number of accepting paths of a probabilistic Turing machine (PTM), while a SpanP function counts the number of different outputs of a PTM. Every $\#\mathsf{P}$ function is also a SpanP function, and the classes are equal if and only if $\mathsf{UP} = \mathsf{NP}$ [46]. A GapP function counts the difference between the number of accepting paths and the number of rejecting paths of a PTM [20, 50]. For more background on counting complexity, we refer to the surveys [23, 76].

A martingale is a function $d : \{0,1\}^* \to [0,\infty)$ such that

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

for all $w \in \{0,1\}^*$. We view a martingale as acting on Cantor Space $\mathsf{C} = \{0,1\}^\infty$ (the infinite binary tree). The value at any node is the average of the values below it. By induction, the value at any node is also the average of the values at any level of the subtree below the node:

$$d(w) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} d(wx).$$

A martingale starts with a finite amount $d(\lambda)$ at the root. We may assume $d(\lambda) = 1$ without loss of generality.

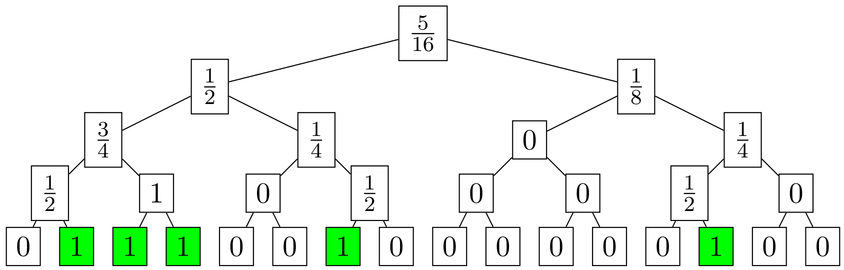

Figure 1.1: Cover Martingale Construction (Construction 4.1)

Intuitively, because the average value of a martingale across $\{0,1\}^n$ is $d(\lambda) = 1$, a martingale is unable to obtain "large" values on "many" sequences. This intuition is formalized into characterizations of Lebesgue measure [49], Hausdorff dimension [30], and packing dimension [9] using martingales. A class $X \subseteq \mathsf{C}$ has measure 0 if and only if there is a martingale that attains unbounded values on all elements of X [86]. A class $X \subseteq \mathsf{C}$ has Hausdorff dimension s if $2^{(1-s)n}$ is the optimal infinitely-often growth rate of martingales on X [57]. A class $X \subseteq \mathsf{C}$ has packing dimension s if $2^{(1-s)n}$ is the optimal almost-everywhere growth rate of martingales on X [9].

Resource-bounded measure and dimension come from restricting these characterizations to martingales computable within some complexity class [9, 55, 57]. The most used resource bounds are polynomial-time (P) and polynomial-space (PSPACE). Generally, it is much easier to construct PSPACE-martingales than it is P-martingales [35, 43]. For more background on resource-bounded measure and dimension we refer to the surveys [4, 37, 56, 58, 61, 67, 68, 81].

1.1 Counting Martingales

Our main conceptual contribution is the introduction of *counting martingales*, which provide intermediate measure and dimension notions between P and PSPACE by using functions from counting complexity classes to define martingales. Many martingale constructions in complexity theory are expressed naturally as counting martingales.

For example, a standard technique for constructing a martingale is betting on a cover (see Figure 1.1) [4, 56]. Given a set $A \subseteq \{0,1\}^*$ and a length $n \geq 0$, we choose $x \in \{0,1\}^n$ uniformly at random and define a martingale d_A by

$$d_A(w) = \Pr_{x \in \{0,1\}^n}[x \in A \mid w \sqsubseteq x] = \frac{|\{x \in A \cap \{0,1\}^n \mid w \sqsubseteq x\}|}{2^{n-|w|}}$$

for all $w \in \{0,1\}^{\leq n}$. Strings of longer length have the value of their length-n prefix. If we can construct an infinite family of such martingales that cover a class and the sum of their initial values converges, the Borel-Cantelli lemma applies to show the class has measure 0 [19].

A key difference between space-bounded measure and time-bounded measure is that a space-bounded martingale can enumerate a covering, whereas a time-bounded martingale does not have time to do this. The complexity of computing d_A depends on the complexity of A and the enumeration bottleneck. Suppose that $A \in \mathsf{P}$. Naively computing d_A would involve an enumeration of A, requiring polynomial space. Computing d_A in polynomial time would only be possible if we have some special structure in A. For example, if A is P-rankable [3], then d_A is polynomial-time computable [40]. It is also possible to approximately compute d_A using an oracle from the polynomial-time hierarchy [40, 66, 80].

The numerator in the definition of d_A is in general a #P function if $A \in \mathsf{P}$. This is because we can use a PTM (Probabilistic Turing Machine) to count how many extensions of a string are in the cover. We call this a #P-*martingale*. In general, a martingale is a #P-martingale if it can be approximated by the ratio of a #P function and a polynomial-time function.

The case when the cover $A \in \mathsf{NP}$ is also interesting, for example when A is the Minimum Circuit Size Problem (MCSP). Then the numerator is a SpanP function. A martingale of this form is a SpanP-*martingale*.

When we use a GapP function for the numerator of a martingale, we call it a GapP-*martingale*. We will show that GapP-martingales are capable of measuring quantum complexity classes. Until now, quantum complexity has not been addressed by resource-bounded measure and dimension.

We call #P-martingales, SpanP-martingales, and GapP-martingales *counting martingales*. Definition 3.1 contains the formal definitions of counting martingales.

1.2 Counting Measures and Counting Dimensions

A class X has #P-measure 0, written $\mu_{\#\mathsf{P}}(X) = 0$, if there is a #P-martingale that succeeds on X. Analogously, a class X has SpanP-measure 0, written $\mu_{\mathsf{SpanP}}(X) = 0$, if there is a SpanP-martingale that succeeds on X. Furthermore, a class X has GapP-measure 0, written $\mu_{\mathsf{GapP}}(X) = 0$, if there is a GapP-martingale that succeeds on X. These *counting measures* are intermediate between P-measure and PSPACE-measure [55]: for every class $X \subseteq \mathsf{C}$,

$$\begin{array}{ccccc} \mu_{\mathsf{P}}(X)=0 & \Rightarrow & \mu_{\#\mathsf{P}}(X)=0 & \Rightarrow & \mu_{\mathsf{GapP}}(X)=0 \\ & & \Downarrow & & \Downarrow \\ & & \mu_{\mathsf{SpanP}}(X)=0 & \Rightarrow & \mu_{\mathsf{PSPACE}}(X)=0. \end{array}$$

We do not know of any relationship between μ_{SpanP} and μ_{GapP}. An individual problem B is Δ-*random* if no Δ-martingale succeeds on B. We show that UE problems are not #P-random and NE problems are not SpanP-random, where UE and NE are the exponential-time versions of UP and NP. When we have a proposition that is known in PSPACE-measure, but open in P-measure, we can investigate it in #P-measure, SpanP-measure, or GapP-measure.

We also introduce *counting dimensions*, #P-dimension, SpanP-dimension, and GapP-dimension, written $\dim_{\#\mathsf{P}}(X)$, $\dim_{\mathsf{SpanP}}(X)$, and $\dim_{\mathsf{GapP}}(X)$, respectively. These dimensions analogously fall between P-dimension and PSPACE-dimension [57]. For all $X \subseteq \mathsf{C}$,

$$\begin{array}{ccccccc} 0 & \le & \dim_{\mathsf{PSPACE}}(X) & \le & \dim_{\mathsf{GapP}}(X) & & \\ & & \rotatebox{90}{$\ge$} & & \rotatebox{90}{$\ge$} & & \\ & & \dim_{\mathsf{SpanP}}(X) & \le & \dim_{\#\mathsf{P}}(X) & \le & \dim_{\mathsf{P}}(X) \le 1. \end{array}$$

We do not know of any relationship between $\dim_{\mathsf{SpanP}}$ and $\dim_{\mathsf{GapP}}$. We also develop *counting strong dimensions*, written $\mathrm{Dim}_{\#\mathsf{P}}(X)$, $\mathrm{Dim}_{\mathsf{SpanP}}(X)$, and $\mathrm{Dim}_{\mathsf{GapP}}(X)$, respectively. These dimensions similarly fall between P-strong dimension and PSPACE-strong dimension [9]. For all $X \subseteq \mathsf{C}$,

$$\begin{array}{ccccccc} 0 & \le & \mathrm{Dim}_{\mathsf{PSPACE}}(X) & \le & \mathrm{Dim}_{\mathsf{GapP}}(X) & & \\ & & \rotatebox{90}{$\ge$} & & \rotatebox{90}{$\ge$} & & \\ & & \mathrm{Dim}_{\mathsf{SpanP}}(X) & \le & \mathrm{Dim}_{\#\mathsf{P}}(X) & \le & \mathrm{Dim}_{\mathsf{P}}(X) \le 1. \end{array}$$

Strong dimension is a more stringent criterion, requiring success to hold for almost all input lengths, rather than just for infinitely many. We work out the definitions and basic properties of counting measures and dimensions in Section 3.

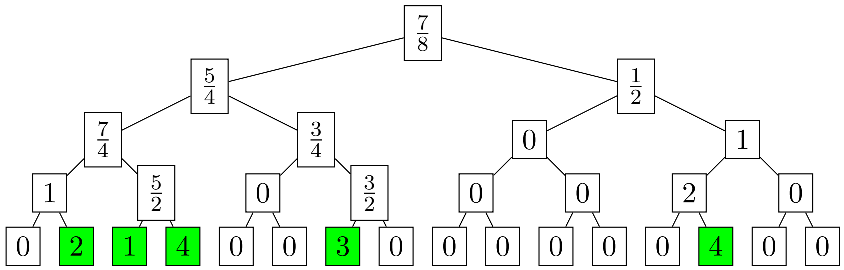

Figure 1.2: Conditional Expectation Martingale Construction (Construction 4.3)

1.3 Our Techniques

Many martingale constructions in complexity theory are expressed naturally as counting martingales. These and other martingale constructions in this paper follow similar patterns. In Section 4 we present five martingale constructions in a unified framework.

1. **Cover Martingale.** The Cover Martingale construction utilizes a cover set A and defines the martingale based on the conditional probability that an extension of the current string belongs to A. If $A \in \mathsf{UP}$, this construction produces a $\#\mathsf{P}$-martingale; if $A \in \mathsf{NP}$, it results in a SpanP-martingale. If A is in the counting complexity class SPP, then this generates a GapP-martingale. The class SPP consists of all languages L for which there exists a GapP function f such that if $x \in L$ then $f(x) = 1$, and $f(x) = 0$ otherwise [20]. This approach is effective for capturing known martingale constructions in the literature, particularly in scenarios where membership within a subset can be determined with unique or nondeterministic witnesses. For further details, refer to Figure 1.1 and Construction 4.1.

2. **Conditional Expectation Martingale.** This martingale generalizes the Cover Martingale by using a counting function $f(x)$ as a random variable and taking its conditional expectation given the current prefix w. This construction is adaptable to functions within $\#\mathsf{P}$, SpanP and GapP, making it effective for applications that require combining information from extensions of a given string. The Conditional Expectation Martingale averages the values of f over all extensions, providing a flexible tool. See Figure 1.2 and Construction 4.3 for an example and technical details.

3. **Subset Martingale.** This martingale is designed to succeed on all infinite subsets of a language B. If $B \in \mathsf{UP}$, it produces a $\#\mathsf{P}$-martingale, and if $B \in \mathsf{NP}$, it yields a SpanP-martingale. If $B \in \mathsf{SPP}$, then this is a GapP-martingale. Unlike deterministic martingales that can focus directly on a language, the Subset Martingale is unique in its ability to succeed across all subsets of a language. This property allows us to conclude that $\#\mathsf{P}$-random languages are not in UE, SpanP-random languages are not in NE, and GapP-random languages are not in SPE (the exponential version of SPP). See Figure 4.1 for an example and Construction 4.5 for a formal definition.

4. **Acceptance Probability Martingale.** We also show that betting according to the acceptance probabilities of a PTM or QTM (quantum Turing machine) yields a counting martingale. Using this, we show that BPP has $\#\mathsf{P}$-dimension 0 and BQP has GapP-dimension 0. See Figure 4.2 for an example and Construction 4.9 for a formal definition.

5. **Bi-Immunity Martingale.** Mayordomo [65] showed P-random languages are E-bi-immune and PSPACE-random languages are ESPACE-bi-immune using a construction that we call a bi-immunity martingale. This construction is designed to succeed on all supersets of an infinite language. We show that this construction works as counting martingales to show $\#\mathsf{P}$-random languages are $\mathsf{UE}\cap\mathsf{coUE}$-bi-immune, SpanP-random languages are $\mathsf{NE}\cap\mathsf{coNE}$-bi-immune, and GapP-random languages are SPE-bi-immune. See Figure 4.3 for an example and Construction 4.16 for a formal definition.

Entropy Rates. Hitchcock and Vinodchandran [40] showed a covering notion called the NP-entropy rate is an upper bound for Δ_3^{P}-dimension, where $\Delta_3^{\mathsf{P}} = \mathsf{P}^{\Sigma_2^{\mathsf{P}}}$. In Section 5.1, we extend this by showing that SpanP-dimension lies between Δ_3^{P}-dimension and the NP-entropy rate. Informally, for a complexity class $\mathcal{C}$ and $X \subseteq \mathsf{C}$, the $\mathcal{C}$-entropy rate of X is the infimum s for which all elements of X can be covered infinitely often by a language $A \in \mathcal{C}$ that has $\frac{\log|A_{=n}|}{n} \leq s$ for all sufficiently large n. Intuitively, this corresponds to the compression rate when using A as an implicit code, where it takes $\log|A_{=n}|$ bits to specify a member of $A_{=n}$.

Kolmogorov Complexity. In Section 5.2, we connect $\#\mathsf{P}$-measure and $\#\mathsf{P}$-dimension to Kolmogorov complexity. For a time bound $t(n)$, $K^t(x)$ is the length of the shortest program that prints x in $t(|x|)$ time on a universal Turing machine. In particular, we extend a result from Lutz [55] and show that $\{S \mid (\exists^\infty n)K^p(S \restriction n) < n - f(n)\}$ has $\#\mathsf{P}$-measure 0, where p is a polynomial, and $\sum_{n=0}^{\infty} 2^{-f(n)}$ is a P-convergent series. In other words, we prove that if S is $\#\mathsf{P}$-random, then $K^p(S \restriction n) \geq n - f(n)$ almost everywhere. We also show that $\#\mathsf{P}$-dimension is at most the polynomial-time Kolmogorov rate [31, 40]. We build on recent work of Nandakumar, Pulari, Akhil S, and Sarma [72] on Kolmogorov complexity rates and polynomial-time dimension to show that if one-way functions exist, then $\#\mathsf{P}$-dimension is distinct from P-dimension.

1.4 Our Results

In Section 6 we study the measure and dimension of classical and quantum circuit complexity classes. Shannon [78] showed that almost all Boolean functions on n input bits require $(1-\epsilon)\frac{2^n}{n}$-size circuits. Lutz [55] strengthened this in two ways, showing that the larger circuit complexity class

$$X_\alpha = \mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1 + \frac{\alpha \log n}{n}\right)\right)$$

has PSPACE-measure 0 for all $\alpha < 1$. Frandsen and Miltersen [26] strengthened the original upper bound of Lupanov [52] to show that Lutz's bound is nearly tight: X_α contains all problems when $\alpha > 3$.

We improve Lutz's result to show that $\mu_{\mathsf{SpanP}}(X_\alpha) = 0$ for all $\alpha < 1$. Lutz's proof extensively reuses polynomial space to consider only *novel* circuits, that compute a different function than any previously considered circuit. This proof does not adapt easily to our setting. In Section 5, we introduce a measure notion called $\mathcal{M}_{\mathsf{NP}}$ that bridges the gap between μ_{PSPACE} and μ_{SpanP} by utilizing the Minimum Circuit Size Problem (MCSP) [44], allowing the construction of a counting martingale. As a corollary, we conclude that X_α has measure 0 in the third level $\Delta_3^{\mathsf{E}} = \mathsf{E}^{\Sigma_2^{\mathsf{P}}}$ of the exponential-time hierarchy. While it was previously known how to construct a problem in Δ_3^{E} with maximum circuit-size complexity [70], our result says most problems in Δ_3^{E} have nearly maximal circuit-size complexity.

Li [51], building on work of Korten [47] and Chen, Hirahara, and Ren [16], showed the first exponential-size circuit lower bound within the second level of the exponential-time hierarchy, that

$\mathsf{SIZE}^{\mathrm{i.o.}}\left(\frac{2^n}{n}\left(1+\frac{\alpha \log n}{n}\right)\right)$	$\mathcal{M}_{\mathsf{NP}}$-measure 0	Theorem 6.1
$\mathsf{SIZE}^{\mathrm{i.o.}}\left(\frac{2^n}{n}\left(1+\frac{\alpha \log n}{n}\right)\right)$	SpanP-measure 0	Corollary 6.2
$\mathsf{SIZE}^{\mathrm{i.o.}}\left(\frac{2^n}{n}\left(1+\frac{\alpha \log n}{n}\right)\right)$	Δ_3^{P}-measure 0	Corollary 6.3
$\mathsf{SIZE}\left(\alpha\frac{2^n}{n}\right)$	#P-strong dimension α	Theorem 6.5
P/poly	#P-strong dimension 0	Corollary 6.6
$\mathsf{SIZE}^{\mathrm{i.o.}}\left(\alpha\frac{2^n}{n}\right)$	#P-dimension $\frac{1+\alpha}{2}$	Theorem 6.7
$\mathsf{BQSIZE}\left(o\left(\frac{2^n}{n}\right)\right)$	GapP-strong dimension 0	Theorem 6.10
BQP/poly	GapP-strong dimension 0	Corollary 6.11
$(\mathsf{P/poly})_{\mathsf{T}}(\mathsf{DENSE}^c)$	#P-dimension 0	Theorem 6.13

Figure 1.3: Summary of Measure, Dimension, and Strong Dimension Results

the symmetric alternation class $S_2^{\mathsf{E}} \not\subseteq \mathsf{SIZE}^{\mathrm{i.o.}}(\frac{2^n}{n})$. We note that Li's proof extends to show $S_2^{\mathsf{E}} \not\subseteq X_\alpha$ for all $\alpha < 1$. Under suitable derandomization assumptions (see Derandomization Hypothesis 2.2), our Δ_3^{E} result improves by one level in the exponential hierarchy, showing X_α has measure 0 in $\Delta_2^{\mathsf{E}} = \mathsf{E}^{\mathsf{NP}}$, for all $\alpha < 1$.

We also improve previous dimension results on circuit-size complexity [40, 57] and the density of hard sets [27, 34, 59, 63]. Additionally, we use GapP-martingales to apply our counting measure framework to analyze quantum circuit complexity. We show that the quantum circuit-size class $\mathsf{BQSIZE}\left(o\left(\frac{2^n}{n}\right)\right)$ has GapP-dimension 0. We also show that the class of problems that P/poly-Turing reduce to subexponentially dense sets has #P-measure 0.

See Figure 1.3 for a summary of our results. We anticipate many further applications of counting measures to refine results where the PSPACE-measure is known and the P-measure is unknown. We discuss some of these directions and open questions in Section 7.

1.5 Organization

This paper is organized as follows. Section 2 covers preliminaries. Section 3 introduces counting martingales, counting measures, and counting dimensions. In Section 4, we detail the five constructions of counting martingales. Section 5 presents our tools on entropy rates and Kolmogorov complexity. Our primary applications on circuit complexity are presented in Section 6. Finally, Section 7 provides concluding remarks and open questions.

2 Preliminaries

The set of all finite binary strings is $\{0,1\}^*$. The empty string is denoted by λ. We use the standard enumeration of binary strings $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, \ldots$. For two strings $x, y \in \{0,1\}^*$, we say $x \leq y$ if x precedes y in the standard enumeration and $x < y$ if x precedes y and is not equal to y. Given two strings x and y, we denote by $[x, y]$ the set of all strings z such that $x \leq z \leq y$. Other types of intervals are defined similarly. We write $x - 1$ for the predecessor of x in the standard enumeration. We use the notation $x \sqsubseteq y$ to say that x is a prefix of y. The length of a string $x \in \{0,1\}^*$ is denoted by $|x|$.

All *languages* (decision problems) in this paper are encoded as subsets of $\{0,1\}^*$. For a language $A \subseteq \{0,1\}^*$ and $n \geq 0$, we define $A_{\leq n} = A \cap \{0,1\}^{\leq n}$ and $A_{=n} = A \cap \{0,1\}^n$.

The *Cantor space* of all infinite binary sequences is C. For a string $w \in \{0,1\}^*$, the *cylinder* $\mathsf{C}_w = w \cdot \mathsf{C}$ consists of all elements of C that begin with w. We routinely identify a language $A \subseteq \{0,1\}^*$ with the element of Cantor space that is A's characteristic sequence according to the standard enumeration of binary strings. In this way, each complexity class is identified with a subset of Cantor space. We write $A \upharpoonright n$ for the n-bit prefix of the characteristic sequence of A, and $A[n]$ for the n^{th}-bit of its characteristic sequence. We use log for the base 2 logarithm.

Our definitions of most complexity classes are standard [6]. For any function $s : \mathbb{N} \to \mathbb{N}$, $\mathsf{SIZE}(s(n))$ is the class of all languages A where for all sufficiently large n, $A_{=n}$ can be decided by a circuit with no more than $s(n)$ gates. We write $\mathsf{SIZE}^{\text{i.o.}}(s(n))$ for the class of all A where $A_{=n}$ has an $s(n)$-size circuit for infinitely many n.

2.1 Resource-Bounded Measure and Dimension

Lutz used martingales to define resource-bounded measure [55] and dimension [57]. Athreya et al. [9] defined strong dimension. We review the basic definitions. More background is available in the survey papers [4, 37, 56, 58, 61, 67, 68, 81].

Definition. (Martingale) A *martingale* is a function $d : \{0,1\}^* \to [0,\infty)$ such that for all $w \in \{0,1\}^*$,

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

If we relax the equality to a $\geq$ inequality in the above equation, we call d a *supermartingale*.

Definition. (Martingale Success) Let d be a supermartingale or martingale.

1. We say *d succeeds on* a sequence $A \in \mathsf{C}$ if $\limsup\limits_{n\to\infty} d(A \upharpoonright n) = \infty$.
2. The *success set* $S^\infty[d]$ is the class of sequences that d succeeds on.
3. The *unitary success set* of d is the set $S^1[d] = \{A \in \mathsf{C} \mid (\exists n)\ d(A \upharpoonright n) \geq 1\}$.
4. For $s > 0$, we say *d s-succeeds on A* if $(\exists^\infty n)\ d(A \upharpoonright n) \geq 2^{(1-s)n}$.
5. For $s > 0$, we say *d s-strongly succeeds on A* if $(\forall^\infty n)\ d(A \upharpoonright n) \geq 2^{(1-s)n}$.
6. We say *d 0-succeeds on A* if d s-succeeds on A for all $s > 0$.
7. We say *d 0-strongly succeeds on A* if d s-strongly succeeds on A for all $s > 0$.
8. For $s \geq 0$, we say *d s-succeeds on* a class $X \subseteq \mathsf{C}$ if d s-succeeds on every member of X.
9. For $s \geq 0$, we say *d s-strongly succeeds on* a class $X \subseteq \mathsf{C}$ if d s-strongly succeeds on every member of X.

In the following definition Δ can be any of the time or space resource bounds including P and PSPACE considered by Lutz [55], and their relativizations including $\Delta_2^{\mathsf{P}} = \mathsf{P}^{\mathsf{NP}}$ and $\Delta_3^{\mathsf{P}} = \mathsf{P}^{\Sigma_2^{\mathsf{P}}}$ [40, 66].

Definition. (Resource-Bounded Measure and Dimension) Let Δ be a resource bound and let $X \subseteq \mathsf{C}$.

1. A class $X \subseteq \mathsf{C}$ has Δ-*measure 0*, and we write $\mu_\Delta(X) = 0$, if there is a Δ-computable martingale d with $X \subseteq S^\infty[d]$.

2. A class $X \subseteq \mathsf{C}$ has Δ-*measure 1*, and we write $\mu_\Delta(X) = 1$, if $\mu_\Delta(X^c) = 0$, where X^c is the complement of X within C.

3. The Δ-*dimension* of a class $X \subseteq \mathsf{C}$ is

$$\mathsf{dim}_\Delta(X) = \inf\{s \mid \exists\ \Delta\text{-martingale } d \text{ that } s\text{-succeeds on all of } X\}.$$

4. The Δ-*strong dimension* of a class $X \subseteq \mathsf{C}$ is

$$\mathsf{Dim}_\Delta(X) = \inf\{s \mid \exists\ \Delta\text{-martingale } d \text{ that } s\text{-strongly succeeds on all of } X\}.$$

5. The Δ-*dimension* of a sequence $S \in \mathsf{C}$ is $\mathsf{dim}_\Delta(S) = \mathsf{dim}_\Delta(\{S\})$.

6. The Δ-*strong dimension* of a sequence $S \in \mathsf{C}$ is $\mathsf{Dim}_\Delta(S) = \mathsf{Dim}_\Delta(\{S\})$.

We note that for all of the classical resource bounds, martingales and supermartingales are equivalent [5].

2.2 Counting Complexity

Valiant introduced #P in the seminal paper for counting complexity [84].

Definition. (#P [84]) Let M be a polynomial-time probabilistic Turing machine that accepts or rejects on each computation path. The #P function computed by M is defined as

$$f(x) = \text{number of accepting computation paths of } M \text{ on input } x$$

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

Köbler, Schöning, and Toran [46] introduced SpanP as an extension of #P.

Definition. (SpanP [46]) Let M be a polynomial-time probabilistic Turing machine that on each computation path either outputs a string or outputs nothing. The SpanP function computed by M is defined as

$$f(x) = \text{number of distinct strings output by } M \text{ on input } x$$

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

Every #P function is also a SpanP function. Köbler et al. [46] showed that #P = SpanP if and only if UP = NP. They also extended Stockmeyer's approximate counting [80] of #P functions in polynomial-time with a Σ_2^{P} oracle to SpanP.

Theorem 2.1. (Köbler, Schöning, and Toran [46]) *Let $f \in \mathsf{SpanP}$. Then there is a function $g \in \Delta_3^{\mathsf{P}}$ such that for all n, for all $x \in \{0,1\}^n$, $(1 - 1/n)g(x) \le f(x) \le (1 + 1/n)g(x)$.*

Shaltiel and Umans [77] showed that under a derandomization assumption, #P functions can be approximated by a deterministic polynomial-time algorithm with nonadaptive access to an NP oracle. Hitchcock and Vinodchandran [40] noted this extends to SpanP functions.

Derandomization Hypothesis 2.2. $\mathsf{E}_{\|}^{\mathsf{NP}}$ requires exponential-size SV-nondeterministic circuits.

We refer to [77] for the details of Derandomization Hypothesis 2.2, including equivalent hypotheses. We note that Derandomization Hypothesis 2.2 is true under more familiar hypotheses like NP does not have P-measure 0 [40] or E requires exponential-size NP-oracle circuits.

Theorem 2.3. ([40, 77]) *If Derandomization Hypothesis 2.2 is true, then for any function* $f \in$ SpanP*, there is a function g computable in polynomial time with nonadaptive access to an* NP *oracle such that for all n, for all* $x \in \{0,1\}^n$*,* $g(x) \leq f(x) \leq g(x)(1 + 1/n)$*.*

Fenner, Fortnow, and Kurtz [20] and Li [50] introduced the class GapP.

Definition. (GapP [20, 50]) Let M be a polynomial-time probabilistic Turing machine that accepts or rejects on each computation path. The GapP function computed by M is defined as

$$\begin{aligned} f(x) \quad = \quad & \text{number of accepting computation paths of } M \text{ on input } x \\ & -\text{number of rejecting computation paths of } M \text{ on input } x \end{aligned}$$

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

Equivalently, GapP is the closure of #P under subtraction [20]. Note that every #P function is also a GapP function and $\mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{GapP}}$. The class SPP consists of all languages L where the characteristic function of L is a GapP function.

3 Counting Martingales

In this section, we define *counting martingales* and use them to define *counting measures and dimensions*. We then work out their foundations including union lemmas, Borel-Cantelli lemmas, and measure conservation that will be used in later sections.

3.1 Counting Martingales Definitions

We define *counting martingales* as martingales that are the ratio of a counting function from #P, SpanP, or GapP and a polynomial-time function that is always a power of 2. We consider both approximately computable and exactly computable martingales.

Definition. (Counting Martingales) Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound.

1. A Δ-*martingale* is a martingale $d(w)$ where there exist $f \in \Delta$ and $g \in \mathsf{FP}$ with $g(w, r)$ being a power of 2 for all $w \in \{0,1\}^*$, such that for all $w \in \{0,1\}^*$ and $r \in \mathbb{N}$,

   $$\left| d(w) - \frac{f(w,r)}{g(w,r)} \right| \leq 2^{-r}.$$

   Here r is encoded in unary.

2. An *exact* Δ-*martingale* is a martingale

   $$d(w) = \frac{f(w)}{g(w)},$$

   where $f \in \Delta$, $g \in \mathsf{FP}$, and $g(w)$ is a power of 2 for all $w \in \{0,1\}^*$.

3.2 Counting Measures and Dimensions Definitions

Analogous to the original definitions of resource-bounded measure [55], we use counting martingales to define counting measures.

Definition. (Counting Measure Zero) Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound. A class $X \subseteq \mathbf{C}$ has Δ-*measure 0*, written $\mu_\Delta(X) = 0$, if there is a Δ-martingale d with $X \subseteq S^\infty[d]$.

Definition. (Counting Random Sequences) Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound. A sequence $S \in \mathbf{C}$ is Δ-*random* if $\{S\}$ does not have Δ-measure 0.

Equivalently, S is Δ-random if no Δ-martingale succeeds on S. We similarly extend the definitions of resource-bounded dimension [57] using stricter notions of martingale success.

Definition. (Counting Dimensions) Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound.

1. The Δ-*dimension* of a class $X \subseteq \mathbf{C}$ is

$$\mathrm{dim}_\Delta(X) = \inf\{s \mid \exists\ \Delta\text{-martingale } d \text{ that } s\text{-succeeds on all of } X\}.$$

2. The Δ-*strong dimension* of a class $X \subseteq \mathbf{C}$ is

$$\mathrm{Dim}_\Delta(X) = \inf\{s \mid \exists\ \Delta\text{-martingale } d \text{ that } s\text{-strongly succeeds on all of } X\}.$$

3. The Δ-*dimension* of a sequence $S \in \mathbf{C}$ is $\mathrm{dim}_\Delta(X) = \mathrm{dim}_\Delta(\{S\})$.

4. The Δ-*strong dimension* of a sequence $S \in \mathbf{C}$ is $\mathrm{Dim}_\Delta(X) = \mathrm{Dim}_\Delta(\{S\})$.

The following relationships are immediate.

Proposition 3.1. *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound and let $X \subseteq \mathbf{C}$.*

1. $0 \le \mathrm{dim}_\Delta(X) \le \mathrm{Dim}_\Delta(X) \le 1$.

2. If $\mathrm{dim}_\Delta(X) < 1$*, then* $\mu_\Delta(X) = 0$.

In the following proposition, μ is Lebesgue measure [49], dim_H is Hausdorff dimension [30] and $\mathrm{Dim}_\mathsf{pack}$ is packing dimension [83]. (We use the notation $\mathrm{Dim}_\mathsf{pack}$ to differentiate it from the polynomial-time dimensions dim_P and Dim_P.)

Proposition 3.2. *For all $X \subseteq \mathbf{C}$,*

$$\begin{array}{ccccccc} \mu_\mathsf{P}(X)=0 & \Rightarrow & \mu_{\#\mathsf{P}}(X)=0 & \Rightarrow & \mu_\mathsf{GapP}(X)=0 & & \\ & & \Downarrow & & \Downarrow & & \\ & & \mu_\mathsf{SpanP}(X)=0 & \Rightarrow & \mu_\mathsf{PSPACE}(X)=0 & \Rightarrow & \mu(X)=0, \end{array}$$

$$\begin{array}{ccccccc} 0 \le \mathrm{dim}_\mathsf{H}(X) & \le & \mathrm{dim}_\mathsf{PSPACE}(X) & \le & \mathrm{dim}_\mathsf{GapP}(X) & & \\ & & \text{|}\wedge & & \text{|}\wedge & & \\ & & \mathrm{dim}_\mathsf{SpanP}(X) & \le & \mathrm{dim}_{\#\mathsf{P}}(X) & \le & \mathrm{dim}_\mathsf{P}(X) \le 1, \end{array}$$

and

$$\begin{array}{ccccccc} 0 \le \mathrm{Dim}_\mathsf{pack}(X) & \le & \mathrm{Dim}_\mathsf{PSPACE}(X) & \le & \mathrm{Dim}_\mathsf{GapP}(X) & & \\ & & \text{|}\wedge & & \text{|}\wedge & & \\ & & \mathrm{Dim}_\mathsf{SpanP}(X) & \le & \mathrm{Dim}_{\#\mathsf{P}}(X) & \le & \mathrm{Dim}_\mathsf{P}(X) \le 1. \end{array}$$

Proof. By the Exact Computation Lemma [42], the outputs of a P-martingale d may be expressed as dyadic rationals of the form $\frac{n}{2^m}$. It is easy to see that the numerator is computed by a $\#\mathsf{P}$ function. The polynomial-time PTM $M(s, w)$ associated with the $\#\mathsf{P}$ function takes input a string s and witness w and computes $d(s) = \frac{n}{2^m}$ in $\mathsf{poly}(s)$ time. If w encodes an integer in $[1, n]$ with no leading zeros, then $M(s, w)$ accepts. Then $M(s, w)$ has n accepting paths, and the denominator 2^m is polynomial-time computable. This implies that every exactly computable P-martingale is also a $\#\mathsf{P}$-martingale. The other relationships follow by complexity class containments and the martingale characterizations of Lebesgue measure [86], Hausdorff dimension [57], and packing dimension [9]. □

3.3 Basic Properties of Counting Martingales

We first note that counting martingales are closed under finite sums, which implies finite unions of counting measure 0 sets have counting measure 0.

Lemma 3.3. *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound. Exact Δ-martingales are closed under finite sums.*

Proof. Let $d_1 = \frac{f_1}{g_1}$ and $d_2 = \frac{f_2}{g_2}$ be exact Δ-martingales. We have

$$d_1(w) + d_2(w) = \frac{f_1(w)g_2(w) + f_2(w)g_1(w)}{g_1(w)g_2(w)}.$$

The numerator is a Δ-function by closure properties of Δ and the denominator is an FP function that is always a power of 2.

We can be more efficient because the denominators are powers of 2. Suppose $g_2(w) \leq g_1(w)$. Then $\frac{g_1(w)}{g_2(w)}$ is a power of 2. Therefore

$$d_1(w) + d_2(w) = \frac{f_1(w) + f_2(w)\frac{g_1(w)}{g_2(w)}}{g_1(w)}.$$

The case $g_1(w) < g_2(w)$ is analogous. □

Corollary 3.4. *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound and let $X, Y \subseteq \mathsf{C}$.*

1. *If $\mu_\Delta(X) = 0$ and $\mu_\Delta(Y) = 0$, then $\mu_\Delta(X \cup Y) = 0$.*
2. $\mathsf{dim}_\Delta(X \cup Y) = \max\{\mathsf{dim}_\Delta(X), \mathsf{dim}_\Delta(Y)\}$.
3. $\mathsf{Dim}_\Delta(X \cup Y) = \max\{\mathsf{Dim}_\Delta(X), \mathsf{Dim}_\Delta(Y)\}$.

Lutz showed that uniform countable unions of Δ-measure 0 sets have Δ-measure 0 for time and space resource bounds Δ. This was proved by summing martingales. We establish an analogue for a uniform family of exact counting martingales.

Definition. (Uniform Family of Exact Counting Martingales) Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound. We say that a family $\left(d_n = \frac{f_n}{g_n} \mid n \in \mathbb{N}\right)$ of exact Δ-martingales is uniform if $(f_n \mid n \in \mathbb{N})$ is uniformly Δ-computable and $(g_n \mid n \in \mathbb{N})$ is uniformly FP.

Definition. (P-convergence) A series $\sum_{n=0}^{\infty} a_n$ of nonnegative real numbers a_n is P-convergent if there is a polynomial-time function $m : \mathbb{N} \to \mathbb{N}$ with $\sum_{n=m(i)}^{\infty} a_n \leq 2^{-i}$ for all $i \in \mathbb{N}$. Such a function m is called a modulus of the convergence. A sequence $\sum_{k=0}^{\infty} a_{j,k}$ $(j = 0, 1, 2, \ldots)$ of series of nonnegative real numbers is uniformly Δ-convergent if there is a function $m : \mathbb{N}^2 \to \mathbb{N}$ such that $m \in \Delta$ and, for all $j \in \mathbb{N}$, m_j is a modulus of the convergence of the series $\sum_{k=0}^{\infty} a_{j,k}$.

Lemma 3.5. (Counting Martingale Summation Lemma) *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound. Suppose $\left(d_n = \frac{f_n}{g_n} \mid n \in \mathbb{N}\right)$ is a uniform family of exact Δ-martingales with $\sum\limits_{n=0}^{\infty} d_n(w)$ uniformly* P*-convergent for all $w \in \{0,1\}^*$. Then $d(w) = \sum\limits_{n=0}^{\infty} d_n(w)$ is a Δ-martingale.*

Proof. Let $m(w, r)$ be the modulus of P-convergence for $\sum\limits_{n=0}^{\infty} d_n(w)$. Let $w \in \{0,1\}^*$ and $r \in \mathbb{N}$. Define

$$t(w, r) = \mathsf{max}(g_1(w), \ldots, g_{m(w,r)}(w)) = \mathsf{lcm}(g_1(w), \ldots, g_{m(w,r}(w)).$$

Define

$$\hat{d}(w, r) = \sum_{n=0}^{m(w,r)} d_n(w).$$

Then

$$|d(w) - \hat{d}(w, r)| = \sum_{n=m(w,r)+1}^{\infty} d_n(w) \leq 2^{-r}.$$

We have

$$\hat{d}(w, r) = \frac{\sum\limits_{n=0}^{m(w,r)} f_n(w) \cdot \frac{t(w,r)}{g_n(w)}}{t(w, r)}.$$

This is a ratio of a Δ function and an FP function that is a power of 2. □

We now have our countable union lemmas.

Lemma 3.6. (Counting Measure Union Lemma) *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound. Suppose $\left(d_n = \frac{f_n}{g_n} \mid n \in \mathbb{N}\right)$ is a uniform family of exact Δ-martingales with $\sum\limits_{n=0}^{\infty} d_n(w)$ uniformly* P*-convergent for all $w \in \{0,1\}^*$. Then $\bigcup\limits_{n=0}^{\infty} S^{\infty}[d_n]$ has Δ-measure 0.*

Proof. This is immediate from Lemma 3.5. □

Lemma 3.7. (Counting Dimension Union Lemma) *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound and let $s > 0$. Suppose $\left(d_n = \frac{f_n}{g_n} \mid n \in \mathbb{N}\right)$ is a uniform family of exact Δ-martingales with $\sum\limits_{n=0}^{\infty} d_n(w)$ uniformly* P*-convergent for all $w \in \{0,1\}^*$.*

1. *Suppose $X_0, X_1, \ldots$ are classes where each d_n s-succeeds on X_n. Then $\bigcup\limits_{n=0}^{\infty} X_n$ has Δ-dimension at most s.*
2. *Suppose $X_0, X_1, \ldots$ are classes where each d_n s-strongly succeeds on X_n. Then $\bigcup\limits_{n=0}^{\infty} X_n$ has Δ-strong dimension at most s.*

Proof. This is immediate from Lemma 3.5. □

3.4 Borel-Cantelli Lemmas

Lutz [55] proved a resource-bounded Borel-Cantelli Lemma. We now present the counting measure version.

Lemma 3.8. (Counting Measure Borel-Cantelli Lemma) *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound. Suppose $(d_n = \frac{f_n}{g_n} \mid n \in \mathbb{N})$ is a uniform family of exact Δ-martingales with $\sum_{n=0}^{\infty} d_n(w)$ being uniformly Δ-convergent for all $w \in \{0,1\}^*$. Then*

$$\limsup_{n\to\infty} S^1[d_n] = \bigcap_{i=0}^{\infty} \bigcup_{j\geq i}^{\infty} S^1[d_j] = \{S \in \mathsf{C} \mid (\exists^\infty n)\ S \in S^1[d_n]\}$$

has Δ-measure 0.

Proof. By Lemma 3.5, the exact Δ-martingale family sums to Δ-martingale d. Then $\bigcap\limits_{i=0}^{\infty} \bigcup\limits_{j\geq i}^{\infty} S^1[d_j] \subseteq S^\infty[d]$. □

Analogously, we extend Lutz's Borel-Cantelli lemma for time- and space-bounded dimension [57] to counting dimensions.

Lemma 3.9. (Counting Dimension Borel-Cantelli Lemma) *Let $\Delta \in \{\#\mathsf{P}, \mathsf{SpanP}, \mathsf{GapP}\}$ be a counting resource bound and let $s > 0$. Suppose $\left(d_n = \frac{f_n}{g_n} \mid n \in \mathbb{N}\right)$ is a uniform family of exact Δ-martingales with $d_n(\lambda) \leq 2^{(s-1)n}$. Then*

$$\limsup_{n\to\infty} S^1[d_n] = \bigcap_{i=0}^{\infty} \bigcup_{j\geq i}^{\infty} S^1[d_j] = \{S \in \mathsf{C} \mid (\exists^\infty n)\ S \in S^1[d_n]\}$$

has Δ-dimension at most s and

$$\liminf_{n\to\infty} S^1[d_n] = \bigcup_{i=0}^{\infty} \bigcap_{j\geq i}^{\infty} S^1[d_j] = \{S \in \mathsf{C} \mid (\forall^\infty n)\ S \in S^1[d_n]\}$$

has Δ-strong dimension at most s.

Proof. Let $t > s$ and $0 < \epsilon < t - s$ be rational numbers. Define

$$d'_n(w) = 2^{\lceil (1-t)n \rceil} d_n(w)$$

for all $n \in \mathbb{N}$ and $w \in \{0,1\}^*$. Then d'_n is a uniform family of exact Δ-martingales with

$$d'_n(\lambda) \leq 2^{(s-1)n} 2^{(1-t)n+1} = 2^{-(t-s)n+1} < 2^{-\epsilon n},$$

with the last inequality holding for sufficiently large n. Therefore $d' = \sum\limits_{n=0}^{\infty} d'_n$ is a Δ-martingale by Lemma 3.5. When $d_n(w) \geq 1$, we have $d'(w) \geq d'_n(w) \geq 2^{(1-t)n}$. Therefore d' t-succeeds on $\limsup\limits_{n\to\infty} S^1[d_n]$ and d' t-strongly succeeds on $\liminf\limits_{n\to\infty} S^1[d_n]$. □

3.5 Measure Conservation

Lutz [55] defined a *constructor* to be a function $\delta : \{0,1\}^* \to \{0,1\}^*$ that properly extends its input string. The *result* $R(\delta)$ of constructor δ is the infinite sequence obtained by repeatedly applying δ to the empty string. For a resource bound Δ, the *result class* $R(\Delta)$ is $R(\Delta) = \{R(\delta) \mid \delta \in \Delta\}$. Lutz's Measure Conservation Theorem [55] showed that $R(\Delta)$ does not have Δ-measure 0 for the time and space resource bounds. Our counting measures do not fit into this framework. It is not clear what a $\#\mathsf{P}$ constructor would be. The best measure conservation theorem we can prove using a constructor approach for counting measures is the following.

Theorem 3.10. *1.* $\mathsf{E}^{\#\mathsf{P}}$ *does not have* $\#\mathsf{P}$*-measure 0.*

2. $\mathsf{E}^{\mathsf{SpanP}}$ *does not have* SpanP*-measure 0.*

3. $\mathsf{E}^{\#\mathsf{P}} = \mathsf{E}^{\mathsf{GapP}}$ *does not have* GapP*-measure 0.*

Proof. Let d be a $\#\mathsf{P}$ martingale. We recursively construct a language $L \in \mathsf{E}^{\#\mathsf{P}}$ that d does not succeed on. Let x be any length n string and w be the characteristic string for all the strings that lexicographically come before x. Now we specify the characteristic bit of x. The string x belongs to L if and only if $d(w1) < d(w0)$. Since $d(wb)$ can be computed by a call to a $\#\mathsf{P}$ oracle and computing a polynomial-time function on a length $\Theta(2^n)$ string, we can decide any x in $\mathsf{E}^{\#\mathsf{P}}$. Since d cannot grow on $L \in \mathsf{E}^{\#\mathsf{P}}$, it follows that $\mathsf{E}^{\#\mathsf{P}}$ does not have $\#\mathsf{P}$-measure 0. If d is a SpanP martingale, we can construct a language $L \in \mathsf{E}^{\mathsf{SpanP}}$. If d is a GapP martingale, we can construct a language $L \in \mathsf{E}^{\mathsf{GapP}} = \mathsf{E}^{\#\mathsf{P}}$. □

In the proof of Theorem 3.10 the constructor we obtain from a $\#\mathsf{P}$-martingale is computable in $\mathsf{P}^{\#\mathsf{P}}$, resulting in the $\mathsf{E}^{\#\mathsf{P}}$ upper bound. We will use approximate counting to improve this to the class $\Delta_3^{\mathsf{E}} = \mathsf{E}^{\Sigma_2^{\mathsf{P}}}$. By padding Toda's theorem [13, 82], $\Delta_3^{\mathsf{E}} \subseteq \mathsf{E}^{\#\mathsf{P}}$. Under suitable derandomization assumptions, we get an improvement to $\Delta_2^{\mathsf{E}} = \mathsf{E}^{\mathsf{NP}}$. The results in the remainder of this section hold not only for $\#\mathsf{P}$ but for the larger class SpanP. It is open whether GapP can be approximately counted in the same way, so Theorem 3.10 is the best we have for GapP.

Lemma 3.11. *1. For every* SpanP*-martingale d, there is a* Δ_3^{P}*-supermartingale d' and a $\gamma > 0$ such that $d'(w) \geq \gamma d(w)$ for all $w \in \{0,1\}^*$.*

2. If Derandomization Hypothesis 2.2 is true, then for every SpanP*-martingale d, there is a* Δ_2^{P}*-supermartingale d' and a $\gamma > 0$ such that $d'(w) \geq \gamma d(w)$ for all $w \in \{0,1\}^*$.*

Proof. Let $d = \frac{f}{g}$ be a SpanP-martingale. Let $h \in \Delta_3^{\mathsf{P}}$ be the approximation of f from Theorem 2.1.

For each n, let $\epsilon_n = \frac{1}{n}$ and define a function d_n by

$$d_n(v) = \frac{h(v)}{g(v)} \left(\frac{1-\epsilon_n}{1+\epsilon_n}\right)^n$$

for all $v \in \{0,1\}^{\geq n}$ and $d_n(v) = d_n(v \upharpoonright n)$ for all v with $|v| > n$. Then d_n is Δ_3^{P} exactly computable.

For $v \in \{0,1\}^{<n}$, we have

$$\begin{aligned}
\left(\frac{h(v0)}{g(v0)} + \frac{h(v1)}{g(v1)}\right) &\leq \left(\frac{f(v0)}{g(v0)} + \frac{f(v1)}{g(v1)}\right)\frac{1}{1-\epsilon_n} \\
&= (d(v0)+d(v1))\frac{1}{1-\epsilon_n} \\
&= 2d(v)\frac{1}{1-\epsilon_n} \\
&= \frac{2f(v)}{g(v)}\frac{1}{1-\epsilon_n} \\
&\leq \frac{2h(v)}{g(v)}\frac{1+\epsilon_n}{1-\epsilon_n}.
\end{aligned}$$

Therefore

$$\begin{aligned}
d_n(v0) + d_n(v1) &= \left(\frac{h(v0)}{g(v0)} + \frac{h(v1)}{g(v1)}\right)\left(\frac{1-\epsilon_n}{1+\epsilon_n}\right)^{n+1} \\
&\leq \frac{2h(v)}{g(v)}\frac{1+\epsilon_n}{1-\epsilon_n}\left(\frac{1-\epsilon_n}{1+\epsilon_n}\right)^{n+1} \\
&= \frac{2h(v)}{g(v)}\left(\frac{1-\epsilon_n}{1+\epsilon_n}\right)^{n} \\
&= 2d_n(v),
\end{aligned}$$

for all $v \in \{0,1\}^{<n}$, so d_n is a supermartingale.

Let $v \in \{0,1\}^n$. Since

$$\left(\frac{1-\epsilon_n}{1+\epsilon_n}\right)^n = \left(1 - \frac{2}{n+1}\right)^n \to \frac{1}{e^2}$$

as $n \to \infty$, let $\gamma \in (0, \frac{1}{e^2})$. We have

$$d_n(v) = d(v)\left(\frac{1-\epsilon_n}{1+\epsilon_n}\right)^n \geq \gamma d(v).$$

when n is sufficiently large.

For part 2, under Derandomization Hypothesis 2.2, we obtain the approximation $h \in \Delta_2^{\mathsf{P}}$ from Theorem 2.3 and follow the same proof. □

The following two theorems and their corollaries are immediate from the previous lemma.

Theorem 3.12. *Let $X \subseteq \mathsf{C}$.*

1. *If $\mu_{\mathsf{SpanP}}(X) = 0$, then $\mu_{\Delta_3^{\mathsf{P}}}(X) = 0$.*
2. $\mathsf{dim}_{\Delta_3^{\mathsf{P}}}(X) \leq \mathsf{dim}_{\mathsf{SpanP}}(X)$.
3. $\mathsf{Dim}_{\Delta_3^{\mathsf{P}}}(X) \leq \mathsf{Dim}_{\mathsf{SpanP}}(X)$.

Corollary 3.13. Δ_3^{E} *does not have* SpanP*-measure 0.*

Theorem 3.14. *Assume Derandomization Hypothesis 2.2. Let $X \subseteq \mathsf{C}$.*

1. *If* $\mu_{\mathsf{SpanP}}(X) = 0$*, then* $\mu_{\Delta_2^{\mathsf{P}}}(X) = 0$.

2. $\mathsf{dim}_{\Delta_2^{\mathsf{P}}}(X) \le \mathsf{dim}_{\mathsf{SpanP}}(X)$.

3. $\mathsf{Dim}_{\Delta_2^{\mathsf{P}}}(X) \le \mathsf{Dim}_{\mathsf{SpanP}}(X)$.

Corollary 3.15. *If Derandomization Hypothesis 2.2 is true, then* $\Delta_2^{\mathsf{E}} = \mathsf{E}^{\mathsf{NP}}$ *does not have* SpanP-*measure 0.*

We conclude this section by noting that $\mathsf{P}^{\#\mathsf{P}}$-measure and the $\mathsf{P}^{\#\mathsf{P}}$-dimensions dominate the counting measures and dimensions. This is immediate from Toda's theorem [82] that $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{GapP}}$ and Theorem 3.12. It appears, however, that the $\mathsf{P}^{\#\mathsf{P}}$ notions are much stronger than our counting dimensions and measures.

Corollary 3.16. *Let* $X \subseteq \mathsf{C}$.

1. *If* $\mu_{\mathsf{SpanP}}(X) = 0$*, then* $\mu_{\mathsf{P}^{\#\mathsf{P}}}(X) = 0$.

2. *If* $\mu_{\mathsf{GapP}}(X) = 0$*, then* $\mu_{\mathsf{P}^{\#\mathsf{P}}}(X) = 0$.

3. $\mathsf{dim}_{\mathsf{P}^{\#\mathsf{P}}}(X) \le \mathsf{dim}_{\mathsf{SpanP}}(X)$.

4. $\mathsf{Dim}_{\mathsf{P}^{\#\mathsf{P}}}(X) \le \mathsf{Dim}_{\mathsf{SpanP}}(X)$.

4 Counting Martingale Constructions

In this section we present five techniques for constructing counting martingales: Cover Martingale, Conditional Expectation Martingale, Subset Martingale, Acceptance Probability Martingale, and Bi-immunity Martingale.

4.1 Cover Martingale Construction

The first construction uses a cover set A and defines the martingale using the conditional probability that an extension of the current string is in the cover. The goal is to obtain a value of 1 on nodes in A while having a small initial value at the root λ.

Construction 4.1. (Cover Martingale) Let $A \subseteq \{0,1\}^*$ and $n \ge 0$. Choose x uniformly at random from $\{0,1\}^n$ and let

$$d_n(w) = \mathsf{Pr}[x \in A_{=n} \mid w \sqsubseteq x]$$

for all $w \in \{0,1\}^{\le n}$. For all $w \in \{0,1\}^{>n}$, we let $d_n(w) = d_n(w \upharpoonright n)$ take the value of its length-n prefix. Then we have

$$d_n(\lambda) = \mathsf{Pr}[x \in A_{=n}],$$

and

$$d_n(x) = 1$$

for all $x \in A_{=n}$. For all $x \in \{0,1\}^n - A_{=n}$, note that $d_n(x) = 0$. Therefore

$$S^1[d_n] = \bigcup_{w \in A_{=n}} \mathsf{C}_w.$$

In other words, d_n covers all sequences that have a prefix in $A_{=n}$ with a value of 1. See Figure 1.1 for an example with $n = 4$, where the green nodes are $A_{=n}$.

Depending on the complexity of the cover, we have a uniform family of exact counting martingales.

Lemma 4.2. *1. If $A \in \mathsf{UP}$, then Construction 4.1 produces a uniform family of exact $\#\mathsf{P}$-martingales.*

2. If $A \in \mathsf{NP}$, then Construction 4.1 produces a uniform family of exact SpanP-martingales.

3. If $A \in \mathsf{SPP}$, then Construction 4.1 produces a uniform family of exact GapP-martingales.

Proof. For $w \in \{0,1\}^*$ and $n \geq 0$, define $\mathrm{ext}(w,n) = \{x \in \{0,1\}^n \mid w \sqsubseteq x\}$ and $\mathrm{ext}_A(w,n) = A \cap \mathrm{ext}(w,n)$. Then

$$d_n(w) = \frac{|\mathrm{ext}_A(w,n)|}{2^{n-|w|}} \tag{4.1}$$

for all $w \in \{0,1\}^{\leq n}$. We have

$$\begin{aligned} d_n(w0) + d_n(w1) &= \frac{|\mathrm{ext}_A(w0,n)|}{2^{n-|w0|}} + \frac{|\mathrm{ext}_A(w1,n)|}{2^{n-|w1|}} \\ &= \frac{|\mathrm{ext}_A(w,n)|}{2^{n-(|w|+1)}} \\ &= 2d(w), \end{aligned}$$

for all $w \in \{0,1\}^{<n}$ and $d_n(w0) + d_n(w1) = 2d_n(w \upharpoonright n) = 2d_n(w)$ for all $w \in \{0,1\}^{\geq n}$, so d_n is a martingale.

If $A \in \mathsf{UP}$, then the numerator $|\mathrm{ext}_A(w,n)|$ in (4.1) is computed by the $\#\mathsf{P}$ function $M(0^n, w)$ that guesses an extension $x \in \mathrm{ext}(w,n)$, guess a witness v for x, and accepts if v is a valid witness for $x \in A$. Because A has unique witnesses, there is exactly one accepting computation path for each $x \in \mathrm{ext}(w,n)$.

If $A \in \mathsf{NP}$, then we compute the numerator $|\mathrm{ext}_A(w,n)|$ in (4.1) by the SpanP function $M(0^n, w)$ that guesses an extension $x \in \mathrm{ext}(w,n)$, guesses a witness v for x, and prints $\langle x, v\rangle$ if v is a valid witness for $x \in A$.

If $A \in \mathsf{SPP}$, let M be a PTM such that $M(x)$ has gap 1 when $x \in A$ and $M(x)$ has gap 0 when $x \notin A$. Consider the GapP function $N(0^n, w)$ that guesses an extension $x \in \mathrm{ext}(w,n)$ and runs $M(x)$. If $M(x)$ accepts, then N accepts. If $M(x)$ rejects, then N rejects. The gap of $N(0^n, w)$ is $|\mathrm{ext}_A(w,n)|$. □

We will use Construction 4.1 in Section 5.1 to develop tools relating counting dimensions and entropy rates, with applications in Section 6 to circuit complexity.

4.2 Conditional Expectation Martingale Construction

Here is a more general martingale construction using a counting function $f(x)$ as a random variable and taking the conditional expectation of f given the current prefix w. This generalizes Construction 4.1 when $f(x)$ is the indicator random variable for the membership of x in the cover A.

Construction 4.3. (Conditional Expectation Martingale) Let $f : \{0,1\}^* \to \mathbb{N}$ and view $f(x)$ as a random variable where x is chosen uniformly from $\{0,1\}^n$. Define

$$d_n(w) = E[f(x) \mid w \sqsubseteq x]$$

for all $w \in \{0,1\}^{\leq n}$. For all $w \in \{0,1\}^{>n}$, we let $d_n(w) = d_n(w \upharpoonright n)$ take the value of its length-n prefix. Then

$$d_n(\lambda) = E[f(x)],$$

and

$$d_n(x) = f(x)$$

for all $x \in \{0,1\}^n$. See Figure 1.2 for an example with $n = 4$. The green nodes are the $x \in \{0,1\}^n$ that have $f(x) > 0$.

We think of Construction 4.3 as covering the sequences that have a prefix x with $f(x) > 0$. Depending on the counting complexity of f, we have a uniform family of exact counting martingales.

Lemma 4.4. *1. If $f \in \#\mathsf{P}$, then Construction 4.3 produces a uniform family of exact $\#\mathsf{P}$-martingales.*

2. If $f \in \mathsf{SpanP}$, then Construction 4.3 produces a uniform family of exact SpanP-martingales.

3. If $f \in \mathsf{GapP}$, then Construction 4.3 produces a uniform family of exact GapP-martingales.

Proof. Let $\mathrm{ext}(w,n) = \{x \in \{0,1\}^n \mid w \sqsubseteq x\}$. Then

$$d_n(w) = \frac{\sum\limits_{x \in \mathrm{ext}(w,n)} f(x)}{2^{n-|w|}} \tag{4.2}$$

for all $w \in \{0,1\}^{\leq n}$. We have

$$\begin{aligned} d_n(w0) + d_n(w1) &= \frac{\sum\limits_{x \in \mathrm{ext}(w0,n)} f(x)}{2^{n-|w0|}} + \frac{\sum\limits_{x \in \mathrm{ext}(w1,n)} f(x)}{2^{n-|w1|}} \\ &= \frac{\sum\limits_{x \in \mathrm{ext}(w,n)} f(x)}{2^{n-(|w|+1)}} \\ &= 2d(w), \end{aligned}$$

for all $w \in \{0,1\}^{<n}$ and $d_n(w0) + d_n(w1) = 2d_n(w \upharpoonright n) = 2d_n(w)$ for all $w \in \{0,1\}^{\geq n}$, so d_n is a martingale.

Suppose $f \in \#\mathsf{P}$. We compute the numerator of $d_n(w)$ in (4.2) by the PTM $M(0^n, w)$ that guesses an extension $x \in \mathrm{ext}(w,n)$ and then runs the $\#\mathsf{P}$ algorithm for f on x. If $f(x)$ accepts, then M accepts. If $f(x)$ rejects, then M rejects.

Suppose $f \in \mathsf{SpanP}$. We compute the numerator of $d_n(w)$ in (4.2) by the PTM $N(0^n, w)$ that guesses an extension $x \in \mathrm{ext}(w,n)$ and then runs the SpanP algorithm for f on x. If $f(x)$ has an output v, then N prints $\langle x, v\rangle$.

Suppose $f \in \mathsf{GapP}$. We compute the numerator of $d_n(w)$ in (4.2) by the PTM $G(0^n, w)$ that guesses an extension $x \in \mathrm{ext}(w,n)$ and then runs the GapP algorithm for f on x. If $f(x)$ accepts, then G accepts. If $f(x)$ rejects, then G rejects. □

We will use Construction 4.3 in Section 5.2 to develop tools relating counting measures and dimensions to Kolmogorov Complexity, with applications to circuit complexity in Section 6.

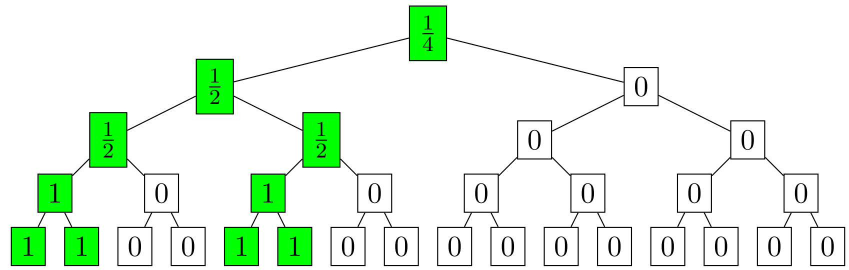

Figure 4.1: Subset Martingale Construction (Construction 4.5)

4.3 Subset Martingale Construction

Next, we present a construction that builds upon Construction 4.1. For a language $B \subseteq \{0,1\}^*$, the *census function of* B is defined by $c_B(n) = |B \cap [s_0, s_n)|$ for all $n \geq 0$. For a string $w \in \{0,1\}^*$, let

$$L(w) = \{s_i \mid w[i] = 1\}$$

be the language with characteristic string w.

Construction 4.5. (Subset Martingale) Let $B \subseteq \{0,1\}^*$ and define the cover

$$\begin{aligned} A &= \{w \in \{0,1\}^* \mid L(w) \subseteq B\} \\ &= \{w \in \{0,1\}^* \mid (\forall i < |w|)\ w[i] = 1 \Rightarrow s_i \in B\}. \end{aligned}$$

Then apply Construction 4.1. We have $|A_{=n}| = 2^{c_B(n)}$, so

$$d_n(\lambda) = \mathsf{Pr}[x \in A_{=n}] = 2^{c_B(n)-n}.$$

For all $w \in \{0,1\}^n$,

$$d_n(w) = \begin{cases} 1 & \text{if } L(w) \subseteq B \\ 0 & \text{otherwise.} \end{cases}$$

See Figure 4.1 for an example with $n = 4$ and $B \cap [s_0, s_3] = \{s_1, s_3\}$. The nodes $w \in \{0,1\}^{\leq 4}$ that are colored green in the tree are those with $L(w) \subseteq B$.

In the following lemma, UE is the exponential ($2^{O(n)}$ time) version of UP, NE is the exponential version of NP, and SPE is the exponential version of SPP.

Lemma 4.6. *1. If $B \in \mathsf{UE}$, then Construction 4.5 produces a uniform family of $\#\mathsf{P}$-martingales.*

2. If $B \in \mathsf{NE}$, then Construction 4.5 produces a uniform family of SpanP-martingales.

3. If $B \in \mathsf{SPE}$, then Construction 4.5 produces a uniform family of GapP-martingales.

Proof. If $B \in \mathsf{UE}$, then we claim $A \in \mathsf{UP}$. Given $w \in \{0,1\}^n$, for each $i < n$, if $w[i] = 1$, guess a witness for $s_i \in B$. If all witnesses are found, accept w. Because A has unique witnesses, B also has unique witnesses. Because the s_i's have length logarithmic in the length of w, the total length of the witness for $w \in B$ is at most $|w| 2^{O(\log |w|)} = |w|^{O(1)}$. Therefore Construction 4.1 produces a uniform family of $\#\mathsf{P}$-martingales.

The other two cases follow similarly. □

Lemma 4.7. *Let $B \subseteq \{0,1\}^*$ and assume the series* $\sum\limits_{n=0}^{\infty} 2^{c_B(n)-n}$ *is* P*-convergent.*

1. *If $B \in$ UE, then the class of all infinite subsets of B has* #P*-measure 0.*
2. *If $B \in$ NE, then the class of all infinite subsets of B has* SpanP*-measure 0.*
3. *If $B \in$ SPE, then the class of all infinite subsets of B has* GapP*-measure 0.*

Proof. Combine Lemma 4.6 and the Counting Measure Borel-Cantelli Lemma (Lemma 3.8). □

We now apply the subset construction along with the law of large numbers for P-random languages to conclude that counting random languages do not belong to particular complexity classes.

Corollary 4.8. 1. *Every* #P*-random language is not in* UE*.*

2. *Every* SpanP*-random language is not in* NE*.*
3. *Every* GapP*-random language is not in* SPE*.*

Proof. Let R be #P-random. Since R is also P-random, it satisfies the law of large numbers [56] and $c_R(n) \leq (\frac{1}{2} + \epsilon)n$ for any $\epsilon > 0$ and all sufficiently large n. The previous lemma applies to contradict the #P-randomness of R. The proofs for SpanP-random and GapP-random languages are analogous. □

4.4 Acceptance Probability Construction

Determining the P-measure of BPP is an open problem. Van Melkebeek [85] used the weak derandomization of BPP from the uniform hardness assumption BPP $\neq$ EXP [41] to prove a zero-one law for the P-measure of BPP: either $\mu_{\mathsf{P}}(\mathsf{BPP}) = 0$ or BPP = EXP. Since BPP = EXP is equivalent to $\mu(\mathsf{BPP} \mid \mathsf{EXP}) = 1$ [74], it follows that determining the P-measure of BPP is equivalent to resolving the BPP versus EXP problem. However, in this section we will show that BPP has #P-measure 0. We will also show that BQP has GapP-measure 0 by building on the work of Fortnow and Rogers [24, 25] that BQP $\subseteq$ AWPP. Both of these results will be proved using the following martingale construction that tracks acceptance probabilities of classical or quantum machines.

Construction 4.9. (Acceptance Probability Martingale) Let $f : \{0,1\}^* \times \{0,1\} \to \mathbb{N}$ be a function such that for some function $q(n)$ and all $x \in \{0,1\}^*$,

$$f(x,0) + f(x,1) = 2^{q(|x|)}.$$

For each $w \in \{0,1\}^*$, let $n = |w|$ and define

$$M(w) = \prod_{i=0}^{n-1} 2f(s_i, w[i]) = 2^n \prod_{i=0}^{n-1} f(s_i, w[i]),$$

$$N(w) = \prod_{i=0}^{n-1} 2^{q(|s_i|)} = 2^{\sum\limits_{i=0}^{n-1} q(|s_i|)},$$

and

$$d(w) = \frac{M(w)}{N(w)} = 2^n \prod_{i=0}^{n-1} \frac{f(s_i, w[i])}{2^{q(|s_i|)}}.$$

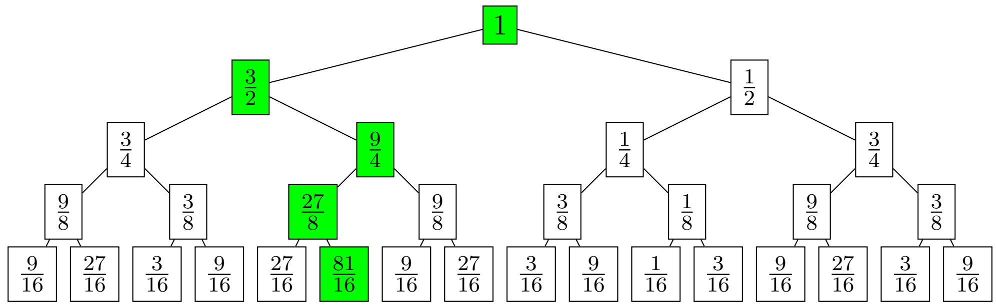

Figure 4.2: Acceptance Probability Martingale Construction (Construction 4.9)

Then d is a martingale with $d(\lambda) = 1$. See Figure 4.2 for an example with $n = 4$, $A \cap [s_0, s_3] = \{s_1, s_3\}$, and correctness probability $\frac{3}{4}$. The green path highlights the prefix 0101 of the characteristic sequence of A.

For example, the function f in Construction 4.9 could be the #P function where $f(x, 0)$ is the number of rejecting paths and $f(x, 1)$ is the number of accepting paths in a PTM Q on input x. Let $q(n)$ be the random seed length of Q. Then

$$\frac{f(x,0)}{2^{q(|x|)}} = \mathsf{Pr}[Q \text{ rejects } x] = \mathsf{Pr}[Q(x) = 0],$$

$$\frac{f(x,1)}{2^{q(|x|)}} = \mathsf{Pr}[Q \text{ accepts } x] = \mathsf{Pr}[Q(x) = 1],$$

and

$$d(w) = 2^n \prod_{i=0}^{n-1} \mathsf{Pr}[Q(s_i) = w[i]].$$

In particular, if $A \in \mathsf{BPE} = \mathsf{BPTIME}(2^{O(n)})$, then for some $c \geq 1$, there exists a 2^{cn}-time PTM Q that decides A with error probability at most 2^{-2n}, where the random seed length is $q(n) = 2^{cn}$.

Lemma 4.10. *If $A \in \mathsf{BPE}$, then the martingale d produced by Construction 4.9 is a #P-martingale that 0-strongly succeeds on A.*

Proof. Let $t(n) = 2^{cn}$ and $p(n) = 2n$. Then $M(w)$ is #P-computable with run time on the order of

$$\sum_{i=0}^{n-1} t(|s_i|) \leq n \cdot t(|s_n|) \leq n 2^{c \log n} = n^{c+1}.$$

Similarly, $N(w)$ is computable in $O(n^{c+1})$ time. Therefore d is a #P-martingale. We have

$$d(A \upharpoonright n) = \frac{M(A \upharpoonright n)}{N(A \upharpoonright n)} = 2^n \prod_{i=0}^{n-1} \mathsf{Pr}[M(s_i) = A[i]] \geq 2^n \prod_{i=0}^{n-1} (1 - 2^{-p(|s_i|)})$$

Using $1 - x \approx e^{-x}$, we have $d(A \upharpoonright n) = \Omega(2^n)$ because

$$2^n \prod_{i=0}^{n-1} e^{-2^{-p(|s_i|)}} = 2^n e^{-\sum\limits_{i=0}^{n-1} 2^{-p(|s_i|)}} = \Omega(2^n).$$

The last line holds because

$$\sum_{i=0}^{\infty} 2^{-p(|s_i|)} = \sum_{n=0}^{\infty} 2^n \cdot 2^{-2n}$$

converges. Therefore d 0-strongly succeeds on A. □

Analogously, one can handle $\mathsf{BQE} = \mathsf{BQTIME}(2^{O(n)})$ [7, 18] with GapP functions. For this, we need the class AWPP that was introduced by Fenner, Fortnow, Kurtz, and Li [21]. The following definition is due to Fenner [22]. See [20, 22, 24] for more details.

Definition. The class AWPP (almost-wide probabilistic polynomial-time) consists of the languages L such that for all polynomials r, there is a polynomial t and a GapP function g such that, for all n, for all $x \in \{0,1\}^n$,

- if $x \in L$, then $1 - 2^{-r(n)} \leq \frac{g(x)}{2^{t(n)}} \leq 1$, and
- if $x \notin L$, then $0 \leq \frac{g(x)}{2^{t(n)}} \leq 2^{-r(n)}$.

We define an exponential version AWPE by allowing g to be computable in time $2^{O(n)}$ in the definition above. The class GapE is defined just like GapP but using PTMs that run in $2^{O(n)}$ time.

Definition. The class AWPE (almost-wide probabilistic exponential-time) consists of the languages L such that for all $r(n) = 2^{O(n)}$, there is $t(n) = 2^{O(n)}$ and a GapE function g such that, for all n, for all $x \in \{0,1\}^n$,

- if $x \in L$, then $1 - 2^{-r(n)} \leq \frac{g(x)}{2^{t(n)}} \leq 1$, and
- if $x \notin L$, then $0 \leq \frac{g(x)}{2^{t(n)}} \leq 2^{-r(n)}$.

Theorem 4.11. *If $A \in \mathsf{AWPE}$, then Construction 4.9 is a GapP-martingale that 0-strongly succeeds on A.*

Proof. Assume $A \in \mathsf{AWPE}$, pick $r(n) = 2^n$, and let $t(n) = 2^{cn}$ and $g \in \mathsf{GapE}$ be the corresponding functions from the definition of AWPE such that for all n and for all $x \in \{0,1\}^n$,

- if $x \in A$, then $1 - 2^{-r(n)} \leq \frac{g(x)}{2^{t(n)}} \leq 1$,
- if $x \notin A$, then $0 \leq \frac{g(x)}{2^{t(n)}} \leq 2^{-r(n)}$.

To adapt the acceptance probability construction, define $f(x,0) = 2^{t(n)} - g(x)$ and $f(x,1) = g(x)$, and define

$$M(w) = \prod_{i=0}^{n-1} 2f(s_i, w[i]) = 2^n \prod_{i=0}^{n-1} f(s_i, w[i]).$$

An argument similar to the proof of Lemma 4.10 together with the closure properties of GapP [20] shows that M computes a GapP function. Also define

$$N(w) = \prod_{i=0}^{n-1} 2^{t(|w_i|)}$$

Now we have

$$d(A\restriction n) = \frac{M(A\restriction n)}{N(A\restriction n)} = 2^n \prod_{i=0}^{n-1} \frac{f(s_i, w[i])}{2^{t(|w_i|)}} \geq 2^n \prod_{i=0}^{n-1} (1 - 2^{-r(|s_i|)})$$

Using $1 - x \approx e^{-x}$, this yields $d(A \upharpoonright n) = \Omega(2^n)$ because

$$2^n \prod_{i=0}^{n-1} e^{-2^{-r(|s_i|)}} = 2^n e^{-\sum_{i=0}^{n-1} 2^{-r(|s_i|)}} = \Omega(2^n).$$

Therefore d 0-strongly succeeds on A. □

A straightforward extension of Fortnow and Rogers' proof that $\mathsf{BQP} \subseteq \mathsf{AWPP}$ to exponential-time classes shows that $\mathsf{BQE} \subseteq \mathsf{AWPE}$. Combining this with Theorem 4.11 gives us the following result.

Theorem 4.12. *If $A \in \mathsf{BQE}$, then there is a* GapP*-martingale that* 0*-strongly succeeds on A.*

Athreya et al. [9] showed that $\mathsf{DTIME}(2^{cn})$ has P-strong dimension 0 for all $c \geq 1$. Using the above results and the Counting Measure Union lemma 3.6, we can extend this result to BPTIME and BQTIME under #P and GapP strong dimensions.

Corollary 4.13. *For all $c \geq 1$,*

1. $\mathsf{BPTIME}(2^{cn})$ *has #P-strong dimension 0.*
2. $\mathsf{BQTIME}(2^{cn})$ *has* GapP*-strong dimension 0.*

Corollary 4.14.
1. BPP *has #P-strong dimension 0.*
2. BQP *has* GapP*-strong dimension 0.*

We have the following Corollary to this section as a companion to Corollary 4.8.

Corollary 4.15.
1. *Every #P-random oracle is not in* BPE*.*
2. *Every* GapP*-random oracle is not in* BQE*.*

4.5 Bi-immunity Martingale Construction

Mayordomo [65] showed that P-random languages are E-bi-immune. We extend her construction to show that #P-random languages are $\mathsf{UE} \cap \mathsf{coUE}$-immune. The same construction also shows SpanP-random languages are $\mathsf{NE} \cap \mathsf{coNE}$-bi-immune and GapP-random languages are SPE-bi-immune.

Construction 4.16. (Bi-immunity Martingale) Let $A \subseteq \{0,1\}^*$. Define a martingale d by $d(\lambda) = 1$ and for all $w \in \{0,1\}^*$,

$$d(w1) = \begin{cases} 2d(w) & \text{if } s_{|w|} \in A \\ d(w) & \text{if } s_{|w|} \notin A \end{cases}$$

and

$$d(w0) = \begin{cases} 0 & \text{if } s_{|w|} \in A \\ d(w) & \text{if } s_{|w|} \notin A. \end{cases}$$

For all $w \in \{0,1\}^*$, again writing $L(w) = \{s_i \mid w[i] = 1\}$, we have

$$d(w) = \begin{cases} 2^{\#_1(A \upharpoonright n)} & \text{if } A \subseteq L(w) \\ 0 & \text{otherwise.} \end{cases}$$

See Figure 4.3 for an example with $n = 4$ and $A \cap [s_0, s_3] = \{s_1, s_3\}$. The nodes $w \in \{0,1\}^{\leq 4}$ that are colored green in the tree are those with $A \subseteq L(w)$.

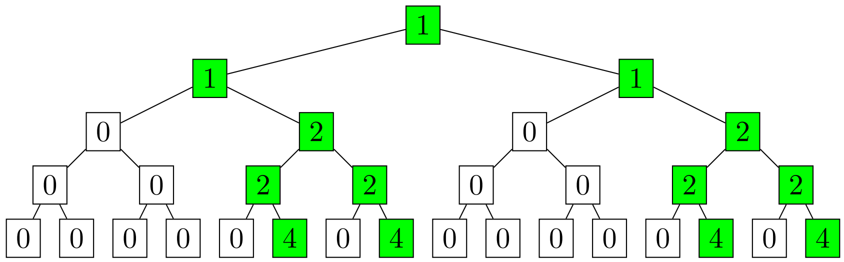

Figure 4.3: Bi-immunity Martingale Construction (Construction 4.16)

Mayordomo [65] showed that if $A \in \mathsf{E}$, then Construction 4.16 is a P-martingale and if $A \in \mathsf{ESPACE}$, then Construction 4.16 is a PSPACE-martingale. For any infinite language A, Mayordomo showed Construction 4.16 succeeds on all languages that contain A.

Lemma 4.17. (Mayordomo [65]) *If A is infinite, then Construction 4.16 has $S^\infty[d] = \{B \mid A \subseteq B\}$.*

We generalize Mayordomo's construction to counting martingales.

Lemma 4.18. *1. If $A \in \mathsf{UE} \cap \mathsf{coUE}$, then Construction 4.16 is an exact #P-martingale.*

2. If $A \in \mathsf{NE} \cap \mathsf{coNE}$, then Construction 4.16 is an exact SpanP-martingale.

3. If $A \in \mathsf{SPE}$, then Construction 4.16 is an exact GapP-martingale.

Proof. For parts 1 and 2, on input w, for each $i < |w|$, guess whether $s_i \in A$ or $s_i \notin A$ and a witness that proves this. Note that the witnesses have total length $2^{O(n)}$ which is polynomial in $|w|$. If witnesses are found for all s_i and prove that $A \upharpoonright |w| \subseteq L(w)$, output $d(w) = 2^{|A \upharpoonright |w||}$; otherwise output 0.

1. If $A \in \mathsf{UE} \cap \mathsf{coUE}$, then d is a UPSV function which may be implemented in #P.
2. If $A \in \mathsf{NE} \cap \mathsf{coNE}$, then d is an NPSV function which may be implemented in SpanP.

For part 3, let $g \in \mathsf{GapE}$ such that $g(x) = 1$ if $x \in A$ and $g(x) = 0$ if $x \notin A$. Define

$$\begin{aligned} f(w,1) &= 1 + g(s_{|w|}) \\ f(w,0) &= 1 - g(s_{|w|}) \end{aligned}$$

for all $w \in \{0,1\}^*$. Then $f \in \mathsf{GapP}$ and

$$d(wb) = f(w,b)d(w)$$

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

$$d(w) = \prod_{i=0}^{|w|-1} f(w \upharpoonright i, w[i])$$

is a GapP function. □

We can now conclude bi-immunity results for counting random languages. Part 3 of the following corollary improves part 3 of Corollary 4.8.

Corollary 4.19. *1. Every* $\#\mathsf{P}$*-random language is* $\mathsf{UE} \cap \mathsf{coUE}$*-bi-immune.*

2. Every SpanP*-random language is* $\mathsf{NE} \cap \mathsf{coNE}$*-bi-immune.*

3. Every GapP*-random language is* SPE*-bi-immune.*

Proof. Let R be GapP-random and let $A \in \mathsf{SPE}$. By the previous two lemmas, R is A-immune. Since SPE is closed under complement, R^c is also A-immune. The other two parts are analogous. □

Since SPP contains the counting classes UP, FewP, and Few, GapP-random languages are also immune to these classes.

5 Entropy Rates and Kolmogorov Complexity

We will use the Cover Martingale and Conditional Expectation Martingale Constructions (Constructions 4.1 and 4.3) to develop a few tools for working with counting measures and dimensions. First, we extend the entropy rates used by Hitchcock and Vinodchandran [40] to our setting. Then we extend Lutz's results on Kolmogorov complexity and PSPACE-measure to counting measure.

5.1 Entropy Rates

We will show in this section that the Cover Martingale Construction (Construction 4.1) may be combined with the concept of entropy rates to build counting martingales.

Definition. The *entropy rate* of a language $A \subseteq \{0,1\}^*$ is

$$H_A = \limsup_{n\to\infty} \frac{\log |A_{=n}|}{n}.$$

Intuitively, H_A gives an asymptotic measurement of the amount by which every string in $A_{=n}$ is compressed in an optimal code [48].

Definition. Let $A \subseteq \{0,1\}^*$. The *i.o.-class of* A is

$$A^{\mathsf{i.o.}} = \{S \in \mathsf{C} \mid (\exists^\infty n)\ S\restriction n \in A\}.$$

The *a.e.-class of* A is

$$A^{\mathsf{a.e.}} = \{S \in \mathsf{C} \mid (\forall^\infty n)\ S\restriction n \in A\}.$$

That is, $A^{\mathsf{i.o.}}$ is the class of sequences that have infinitely many prefixes in A and $A^{\mathsf{a.e.}}$ is the class of sequences that have all but finitely many prefixes in A.

Definition. (Hitchcock [31, 33]) Let $\mathcal{C}$ be a class of languages and $X \subseteq \mathsf{C}$. The $\mathcal{C}$*-entropy rate* of X is

$$\mathcal{H}_{\mathcal{C}}(X) = \inf\{H_A \mid A \in \mathcal{C} \text{ and } X \subseteq A^{\mathsf{i.o.}}\}.$$

The $\mathcal{C}$*-strong entropy rate* of X is

$$\mathcal{H}^{\mathsf{str}}_{\mathcal{C}}(X) = \inf\{H_A \mid A \in \mathcal{C} \text{ and } X \subseteq A^{\mathsf{a.e.}}\}.$$

Informally, $\mathcal{H}_{\mathcal{C}}(X)$ is the lowest entropy rate with which every element of X can be covered infinitely often by a language in $\mathcal{C}$. We may also interpret $\mathcal{H}_{\mathcal{C}}(X)$ as a notion of dimension. For all $X \subseteq \mathsf{C}$, it is known that $\mathsf{dim}_{\mathsf{H}}(X) = \mathcal{H}_{\mathsf{ALL}}(X)$, where ALL is the class of all languages and $\mathsf{dim}_{\mathsf{H}}$ is Hausdorff dimension (see [75, 79]). Hitchcock [31, 33] showed that $\mathsf{Dim}_{\mathsf{pack}}(X) = \mathcal{H}^{\mathsf{str}}_{\mathsf{ALL}}(X)$ and using other classes gives equivalent definitions of the constructive dimension ($\mathsf{cdim}(X) = \mathcal{H}_{\mathsf{CE}}(X)$ and $\mathsf{cDim}(X) = \mathcal{H}^{\mathsf{str}}_{\mathsf{CE}}$), computable dimension ($\mathsf{dim}_{\mathsf{comp}}(X) = \mathcal{H}_{\mathsf{DEC}}(X)$ and $\mathsf{Dim}_{\mathsf{comp}}(X) = \mathcal{H}^{\mathsf{str}}_{\mathsf{DEC}}(X)$), and polynomial-space dimension ($\mathsf{dim}_{\mathsf{PSPACE}}(X) = \mathcal{H}_{\mathsf{PSPACE}}(X)$ and $\mathsf{Dim}_{\mathsf{PSPACE}}(X) = \mathcal{H}^{\mathsf{str}}_{\mathsf{PSPACE}}(X)$). For time-bounded dimension, no analogous result is known. However, the following upper bounds are true [31, 33]: for all $X \subseteq \mathsf{C}$, $\mathcal{H}_{\mathsf{P}}(X) \leq \mathsf{dim}_{\mathsf{P}}(X)$ and $\mathcal{H}^{\mathsf{str}}_{\mathsf{P}}(x) \leq \mathsf{Dim}_{\mathsf{P}}(X)$, where $\mathsf{dim}_{\mathsf{P}}$ is the polynomial-time dimension and $\mathsf{Dim}_{\mathsf{P}}$ is the polynomial-time strong dimension.

The NP-entropy rate is an upper bound for Δ^{P}_3-dimension.

Theorem 5.1. (Hitchcock and Vinodchandran [40]) *For all* $X \subseteq \mathsf{C}$*,*

$$\mathsf{dim}_{\Delta^{\mathsf{P}}_3}(X) \leq \mathcal{H}_{\mathsf{NP}}(X).$$

The strong dimension analogue of Theorem 5.1 also holds:

$$\mathsf{Dim}_{\Delta^{\mathsf{P}}_3}(X) \leq \mathcal{H}^{\mathsf{str}}_{\mathsf{NP}}(X)$$

for all $X \subseteq \mathsf{C}$.

We now show that the NP-entropy rate upper bounds SpanP-dimension. Analogously, the UP-entropy rate upper bounds $\#\mathsf{P}$-dimension and the SPP-entropy rate upper bounds GapP-dimension. The proof uses Construction 4.1 and Lemma 4.2.

Theorem 5.2. *For all* $X \subseteq \mathsf{C}$*,*

1. $\mathsf{dim}_{\#\mathsf{P}}(X) \leq \mathcal{H}_{\mathsf{UP}}(X) \leq \mathcal{H}_{\mathsf{P}}(X)$
2. $\mathsf{dim}_{\mathsf{SpanP}}(X) \leq \mathcal{H}_{\mathsf{NP}}(X)$.
3. $\mathsf{dim}_{\mathsf{GapP}}(X) \leq \mathcal{H}_{\mathsf{SPP}}(X)$.
4. $\mathsf{Dim}_{\#\mathsf{P}}(X) \leq \mathcal{H}^{\mathsf{str}}_{\mathsf{UP}}(X) \leq \mathcal{H}^{\mathsf{str}}_{\mathsf{P}}(X)$
5. $\mathsf{Dim}_{\mathsf{SpanP}}(X) \leq \mathcal{H}^{\mathsf{str}}_{\mathsf{NP}}(X)$.
6. $\mathsf{Dim}_{\mathsf{GapP}}(X) \leq \mathcal{H}^{\mathsf{str}}_{\mathsf{SPP}}(X)$.

Proof. We prove the second inequality, the proofs of the other inequalities are analogous.

Let $\alpha > \mathcal{H}_{\mathsf{NP}}(X)$ and $\epsilon > 0$ such that 2^α and 2^ϵ are rational. Let $A \in \mathsf{NP}$ such that $X \subseteq A^{\mathsf{i.o.}}$ and $H_A < \alpha$. We can assume that $|A_{=n}| \leq 2^{\alpha n}$ for all n. It suffices to show that $\mathsf{dim}_{\mathsf{SpanP}}(X) \leq \alpha + \epsilon$.

We use Construction 4.1 and Lemma 4.2 to obtain a uniform family $(d_n \mid n \geq 0)$ of SpanP martingales with

$$d_n(\lambda) = \frac{|A_{=n}|}{2^n} \leq 2^{(\alpha-1)n}$$

and $d_n(v) = 1$ for all $v \in A_{=n}$. We now apply the Counting Dimension Borel-Cantelli Lemma (Lemma 3.9) to complete the proof. □

We note that combining Theorems 5.2 and 3.12 gives a new proof of Theorem 5.1.

We will next extend Theorem 5.2 to the measure setting. First, we define an entropy rate version of measure 0. The idea in this definition is to extend the entropy rate $\mathcal{H}_{\mathcal{C}}$ to define a measure $\mathcal{M}_{\mathcal{C}}$.

Definition. (Entropy Rate Measure) Let $X \subseteq \mathsf{C}$ and let $\mathcal{C}$ be a complexity class. If there exist $A \in \mathcal{C}$ and $f \in \mathsf{FP}$ such that

1. $X \subseteq A^{\mathsf{i.o.}}$,
2. $\log |A_{=n}| < n - f(n)$ for sufficiently large n, and
3. $\sum\limits_{n=0}^{\infty} 2^{-f(n)}$ is P-convergent,

then X has $\mathcal{M}_{\mathcal{C}}$-measure 0 and we write $\mathcal{M}_{\mathcal{C}}(X) = 0$.

We observe that $\mathcal{M}_{\mathcal{C}}$-measure has many of the standard measure properties. When using $\mathcal{C} = \mathsf{ALL}$, the class of all languages, it refines Lebesgue measure: if $\mathcal{M}_{\mathsf{ALL}}(X) = 0$, then X has Lebesgue measure 0. Using $\mathcal{C} = \mathsf{PSPACE}$, we have if $\mathcal{M}_{\mathsf{PSPACE}}(X) = 0$, then $\mu_{\mathsf{PSPACE}}(X) = 0$.

Proposition 5.3. *Let $\mathcal{C}, \mathcal{D}$ be classes of languages and $X, Y \subseteq \mathsf{C}$.*

1. *If $\mathcal{C} \subseteq \mathcal{D}$, $\mathcal{M}_{\mathcal{C}}(X) = 0$ implies $\mathcal{M}_{\mathcal{D}}(X) = 0$.*
2. *If $X \subseteq Y$, then $\mathcal{M}_{\mathcal{C}}(Y) = 0$ implies $\mathcal{M}_{\mathcal{C}}(X) = 0$.*
3. *If $\mathcal{C}$ is closed under union, then $\mathcal{M}_{\mathcal{C}}(X) = 0$ and $\mathcal{M}_{\mathcal{C}}(Y) = 0$ implies $\mathcal{M}_{\mathcal{C}}(X \cup Y) = 0$.*
4. *If $\mathcal{H}_{\mathcal{C}}(X) < 1$, then $\mathcal{M}_{\mathcal{C}}(X) = 0$.*

We now establish our measure-theoretic extension of Theorem 5.2. This proof also uses Construction 4.1 and Lemma 4.2.

Theorem 5.4. *Let $X \subseteq \mathsf{C}$.*

1. *If $\mathcal{M}_{\mathsf{UP}}(X) = 0$, then $\mu_{\#\mathsf{P}}(X) = 0$.*
2. *If $\mathcal{M}_{\mathsf{NP}}(X) = 0$, then $\mu_{\mathsf{SpanP}}(X) = 0$.*
3. *If $\mathcal{M}_{\mathsf{SPP}}(X) = 0$, then $\mu_{\mathsf{GapP}}(X) = 0$.*

Proof. Assume $\mathcal{M}_{\mathsf{NP}}(X) = 0$ and obtain the cover $A \in \mathsf{NP}$ and the function $f \in \mathsf{FP}$ satisfying the definition of $\mathcal{M}_{\mathsf{NP}}(X) = 0$. We use Construction 4.1 and Lemma 4.2 to obtain a uniform family of exact SpanP martingales $(d_n \mid n \geq 0)$ with

$$d_n(\lambda) = \frac{|A_{=n}|}{2^n} \leq \frac{2^{n-f(n)}}{2^n} = 2^{-f(n)}$$

and $d_n(w) = 1$ for all $w \in A_{=n}$. The Counting Measure Borel-Cantelli lemma (Lemma 3.8) completes the proof. The proofs of the other items are analogous. □

5.2 Kolmogorov Complexity

Lutz [55] showed that the space-bounded Kolmogorov complexity class

$$\{S \mid (\exists^{\infty} n)\, KS^p(S \upharpoonright n) < n - f(n)\}$$

has PSPACE-measure 0 where p is a polynomial, and $\sum\limits_{n=0}^{\infty} 2^{-f(n)}$ is P-convergent. In other words, if S is PSPACE-random, then $KS^p(S \upharpoonright n) \geq n - f(n)$ a.e. For P-random sequences, Lutz proved that the time-bounded Kolmogorov complexity $K^p(S \upharpoonright n) \geq c \log n$ a.e. for any polynomial p.

We use the Conditional Expectation Martingale Construction (Construction 4.3) to obtain an intermediate result for time-bounded Kolmogorov complexity and $\#\mathsf{P}$-measure.

Theorem 5.5. *Suppose $f \in \mathsf{FP}$ and the series $\sum_{n=0}^{\infty} 2^{-f(n)}$ is P-convergent. Let p be a polynomial and*

$$X = \{S \mid (\exists^\infty n)\, K^p(S\upharpoonright n) < n - f(n)\}.$$

Then X has $\#\mathsf{P}$-measure 0.

Proof. For each n, let

$$X_n = \{x \in \{0,1\}^n \mid K^p(x) < n - f(n)\}.$$

For $w \in \{0,1\}^{\leq n}$, let

$$d_n(w) = \mathsf{Pr}(X_n \mid w) = \frac{|\{x \in X_n \mid w \sqsubseteq x\}|}{2^{n-|w|}}.$$

This martingale satisfies

$$d_n(\lambda) \leq \frac{|X_n|}{2^n} \leq \frac{2^{n-f(n)}}{2^n} = 2^{-f(n)}$$

and $d_n(x) = 1$ for all $x \in X_n$. However, d_n does not appear to be a $\#\mathsf{P}$ martingale because its numerator is a SpanP function. We will upper bound the SpanP-martingale d_n by another martingale d'_n that is $\#\mathsf{P}$-computable and still satisfies $d'_n(\lambda) \leq 2^{-f(n)}$.

Let U be a universal Turing machine and define

$$C = \left\{ \langle 0^n, w, x, \pi\rangle \;\middle|\; \begin{array}{l} w \in \{0,1\}^{\leq n}, x \in \{0,1\}^n, \pi \in \{0,1\}^{<n-f(n)}, \\ w \sqsubseteq x, \text{ and } U(\pi) = x \text{ in} \leq p(n) \text{ time} \end{array} \right\}.$$

Then $C \in \mathsf{P}$, so the function

$$g(0^n, w) = \left| \left\{ \langle x, \pi\rangle \;\middle|\; \begin{array}{l} x \in \{0,1\}^n, \pi \in \{0,1\}^{<n-f(n)}, w \sqsubseteq x \\ \text{and } U(\pi) = x \text{ in} \leq p(n) \text{ time} \end{array} \right\} \right|.$$

is in $\#\mathsf{P}$. We use Construction 4.3. Define the $\#\mathsf{P}$-martingale

$$d'_n(w) = \frac{g(0^n, w)}{2^{n-|w|}}$$

for all $w \in \{0,1\}^{\leq n}$ and $d'_n(y) = d'_n(y \upharpoonright n)$ for $y \in \{0,1\}^{>n}$. Notice that $g(0^n, w) \leq 2^{n-f(n)}$, so $d'_n(\lambda) \leq 2^{-f(n)}$. Also, $d'_n(x) \geq d_n(x)$ for all $x \in \{0,1\}^*$. If $x \in X_n$, then

$$g(0^n, x) = \left| \left\{ \pi \;\middle|\; \begin{array}{l} x \in \{0,1\}^n, \pi \in \{0,1\}^{<n-f(n)}, \\ \text{and } U(\pi) = x \text{ in } \leq p(n) \text{ time} \end{array} \right\} \right| \geq 1.$$

and $d'_n(x) \geq 1 = d_n(x)$. Therefore $X_n \subseteq S^1[d'_n]$. Also, $(d'_n \mid n \in \mathbb{N})$ is exactly and uniformly $\#\mathsf{P}$-computable by Lemma 4.4. We apply the Counting Measure Borel-Cantelli Lemma (Lemma 3.8) to conclude that

$$X \subseteq \bigcap_{i=0}^{\infty} \bigcup_{j \geq i}^{\infty} S^1[d'_n]$$

has $\#\mathsf{P}$-measure 0. □

Corollary 5.6. *Suppose $f \in \mathsf{FP}$ and the series $\sum_{n=0}^{\infty} 2^{-f(n)}$ is P-convergent. If S is $\#\mathsf{P}$-random, then $K^p(S\upharpoonright n) \geq n - f(n)$ a.e.*

The following Theorem is a variation of Theorem 5.5 which will be used in Section 6.

Theorem 5.7. *Suppose $f \in \mathsf{FP}$ and the series $\sum_{n=0}^{\infty} 2^{-f(n)}$ is P-convergent. Let p be a polynomial and*

$$X = \{A \mid (\exists^\infty n)\, K^p(A_{=n}) < 2^n - f(2^n)\}.$$

Then X has $\#\mathsf{P}$-measure 0.

Proof. If $K^p(A_{=n}) < 2^n - f(2^n)$ then we have

$$\begin{aligned} K^p(A_{\le n}) &\le K^p(A_{<n}) + K^p(A_{=n}) + O(n) \\ &\le 2^n + 2^n - f(2^n) + O(n) \\ &= 2^{n+1} - f(2^n) + O(n). \end{aligned}$$

It follows from Theorem 5.5 that X has $\#\mathsf{P}$-measure 0. □

We next consider Kolmogorov complexity rates, which leads to an interesting connection with one-way functions.

Definition. ([31, 40]) Let $X \subseteq \mathsf{C}$.

1. The *polynomial-time Kolmogorov complexity rate of X* is

$$\mathcal{K}_{\mathsf{poly}}(X) = \inf_{p \in \mathsf{poly}} \sup_{S \in X} \liminf_{n\to\infty} \frac{K^p(S\upharpoonright n)}{n}.$$

2. The *polynomial-time strong Kolmogorov complexity rate of X* is

$$\mathcal{K}^{\mathsf{str}}_{\mathsf{poly}}(X) = \inf_{p \in \mathsf{poly}} \sup_{S \in X} \limsup_{n\to\infty} \frac{K^p(S\upharpoonright n)}{n}.$$

1. The *polynomial-space Kolmogorov complexity rate of X* is

$$\mathcal{KS}_{\mathsf{poly}}(X) = \inf_{p \in \mathsf{poly}} \sup_{S \in X} \liminf_{n\to\infty} \frac{KS^p(S\upharpoonright n)}{n}.$$

2. The *polynomial-space strong Kolmogorov complexity rate of X* is

$$\mathcal{KS}^{\mathsf{str}}_{\mathsf{poly}}(X) = \inf_{p \in \mathsf{poly}} \sup_{S \in X} \limsup_{n\to\infty} \frac{KS^p(S\upharpoonright n)}{n}.$$

Hitchcock and Vinodchandran [40] showed that for all $X \subseteq \mathsf{C}$,

$$\left\{ \begin{array}{c} \mathsf{dim}_{\mathsf{PSPACE}}(X) \\ = \\ \mathcal{H}_{\mathsf{PSPACE}}(X) \\ = \\ \mathcal{KS}^{\mathsf{poly}}(X) \end{array} \right\} \le \mathsf{dim}_{\Delta^{\mathsf{P}}_3}(X) \le \mathcal{H}_{\mathsf{NP}}(X) \le \left\{ \begin{array}{c} \mathcal{H}_{\mathsf{P}}(X), \\ \mathcal{K}_{\mathsf{poly}}(X) \end{array} \right\} \le \mathsf{dim}_{\mathsf{P}}(X). \tag{5.1}$$

At the polynomial-space level, PSPACE-dimension, the PSPACE-entropy rate, and the Kolmogorov complexity rate all coincide. At the polynomial-time level, the P-dimension, P-entropy rate, and time-bounded Kolmogorov complexity rate are not known to be equal. No relationship is known

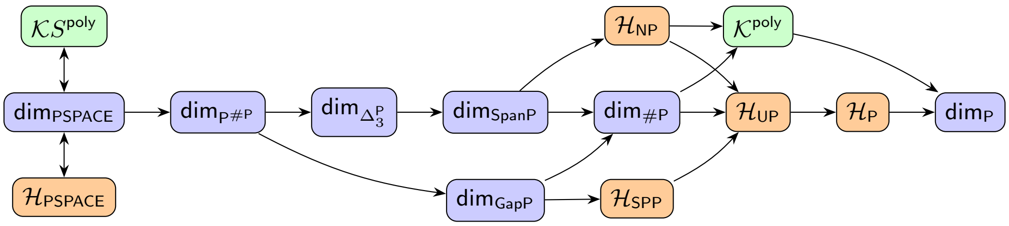

Figure 5.1: Relationships between Dimensions, Entropy Rates, and Kolmogorov Complexity Rates

between $\mathcal{H}_{\mathsf{P}}(X)$ and $\mathcal{K}_{\mathsf{poly}}(X)$. Analogous inequalities hold for the strong dimension versions of the quantities in (5.1): for all $X \subseteq \mathsf{C}$,

$$\left\{ \begin{array}{c} \mathsf{Dim}_{\mathsf{PSPACE}}(X) \\ = \\ \mathcal{H}^{\mathsf{str}}_{\mathsf{PSPACE}}(X) \\ = \\ \mathcal{KS}^{\mathsf{str}}_{\mathsf{poly}}(X) \end{array} \right\} \leq \mathsf{Dim}_{\Delta_3^{\mathsf{P}}}(X) \leq \mathcal{H}^{\mathsf{str}}_{\mathsf{NP}}(X) \leq \left\{ \begin{array}{c} \mathcal{H}^{\mathsf{str}}_{\mathsf{P}}(X), \\ \mathcal{K}^{\mathsf{str}}_{\mathsf{poly}}(X) \end{array} \right\} \leq \mathsf{Dim}_{\mathsf{P}}(X). \tag{5.2}$$

Each quantity in (5.2) is greater than or equal to the corresponding quantity in 5.1.

We now show that the polynomial-time Kolmogorov complexity rates upper bound the #P-dimensions.

Theorem 5.8. *For all $X \subseteq \mathsf{C}$,*

$$\mathsf{dim}_{\#\mathsf{P}}(X) \leq \mathcal{K}_{\mathsf{poly}}(X)$$

and

$$\mathsf{Dim}_{\#\mathsf{P}}(X) \leq \mathcal{K}^{\mathsf{str}}_{\mathsf{poly}}(X).$$

Proof. Let $s > \mathcal{K}^{\mathsf{poly}}(X)$ be rational. For each n, let

$$X_n = \{x \in \{0,1\}^n \mid K^p(x) \leq s|x|\}.$$

Then use Construction 4.3 as in the proof of Theorem 5.5 to obtain a #P-martingale d_n for each n where $d_n(\lambda) \geq 2^{(s-1)n}$ for all $x \in X_n$. We then apply the Counting Dimension Borel-Cantelli Lemma (Lemma 3.9). This shows $\mathsf{dim}_{\#\mathsf{P}}(X) \leq s$. The proof of the lower bounds $\mathsf{dim}_{\#\mathsf{P}}(X) \geq s$ follows from [36]. The proof for strong dimension is analogous. □

Combining Theorem 5.2, Theorem 5.8, Corollary 3.16, and the inequalities in (5.1), we have the refined picture in Figure 5.1. An arrow denotes that the dimension notion on the left is at most the dimension notion on the right. A double arrow denotes that the two dimension notions are equal. Analogous inequalities hold for the strong dimension versions of the quantities in Figure 5.1

Nandakumar, Pulari, Akhil S, and Sarma [72] showed that if one-way functions exist, then for all $\epsilon > 0$, there exists $X \subseteq \mathsf{C}$ with $\mathsf{dim}_{\mathsf{P}}(X) - \mathcal{K}^{\mathsf{str}}_{\mathsf{poly}}(X) \geq 1 - \epsilon$. In fact, X may be taken as a singleton. Combining this result with Theorem 5.8 and the inequalities $\mathcal{K}_{\mathsf{poly}}(X) \leq \mathsf{dim}_{\mathsf{P}}(X)$ and $\mathcal{K}^{\mathsf{str}}_{\mathsf{poly}} \leq \mathsf{Dim}_{\mathsf{P}}(X)$ from (5.1) and (5.2), we obtain the following corollaries.

Corollary 5.9. *If one-way functions exist, then for all $\epsilon > 0$, there exists $S \in \mathsf{C}$ with $\mathsf{dim}_{\mathsf{P}}(S) - \mathsf{dim}_{\#\mathsf{P}}(S) \geq 1 - \epsilon$ and $\mathsf{Dim}_{\mathsf{P}}(S) - \mathsf{Dim}_{\#\mathsf{P}}(S) \geq 1 - \epsilon$.*

In other words: if one-way functions exist, then P-dimension is different from #P-dimension and strong P-dimension is different from strong #P-dimension.

Corollary 5.10. *1. If $\mathsf{dim}_{\#\mathsf{P}}(S) = \mathsf{dim}_{\mathsf{P}}(S)$ for all $S \in \mathsf{C}$, then one-way functions do not exist.*

2. If $\mathsf{Dim}_{\#\mathsf{P}}(S) = \mathsf{Dim}_{\mathsf{P}}(S)$ for all $S \in \mathsf{C}$, then one-way functions do not exist.

6 Applications

This section contains our main applications. We start with classical circuit complexity, then move on to quantum circuit complexity, and lastly the density of hard sets.

6.1 Classical Circuit Complexity

Lutz [55] showed that for all $\alpha < 1$, the class

$$X_\alpha = \mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1 + \frac{\alpha \log n}{n}\right)\right)$$

has PSPACE-measure 0. Additionally, Lutz showed that for any $c \geq 1$ and $k \geq 1$, the classes P/cn and $\mathsf{SIZE}(n^k)$ have polynomial-time measure 0 and quasipolynomial-time measure 0, respectively. Mayordomo [66] used Stockmeyer's approximate counting of $\#\mathsf{P}$ functions [80] to show that P/poly has measure 0 in the third level of the exponential hierarchy.

We begin by extending Lutz's PSPACE-measure result to $\mathcal{M}_{\mathsf{NP}}$-measure, in order to improve the theorem to SpanP-measure. The proof uses the Minimum Circuit Size Problem (MCSP) [44] to form a cover. In MCSP, we are given the full 2^n-length truth-table of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ and a number $s \geq 1$ and asked to decide whether there is a circuit of size at most s computing f. The MCSP problem is in NP and not known to be NP-complete [39, 44, 71]. The MCSP problem fits perfectly into the $\mathcal{M}_{\mathsf{NP}}$ framework to help improve Lutz's result, that X_α has PSPACE-measure 0.

Theorem 6.1. *For all $\alpha < 1$,*

$$\mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1 + \frac{\alpha \log n}{n}\right)\right)$$

has $\mathcal{M}_{\mathsf{NP}}$-measure 0.

Proof. Let $s(n) = \frac{2^n}{n}\left(1 + \frac{\alpha \log n}{n}\right)$ where $\alpha < 1$ and let $X = \mathsf{SIZE}^{\mathsf{i.o.}}(s(n))$.

Define

$$\begin{aligned} A &= \{B_{\leq n} \,|\langle B_{=n}, s(n)\rangle \in \mathsf{MCSP}\,\} \\ &= \{B_{\leq n} \,|B_{=n} \text{ has a circuit of size at most } s(n)\,\}\,. \end{aligned}$$

Then $A \in \mathsf{NP}$, $X \subseteq A^{\mathsf{i.o.}}$, and we need to show that $\log |A_{=N}| < N - f(N)$, where $N = 2^{n+1} - 1$, for some $f \in \mathsf{FP}$ such that $\sum_{n=0}^{\infty} 2^{-f(n)}$ is P-convergent. Using the bound in [55], we have:

$$
\begin{aligned}
\log|A_{=N}| &< \sum_{m=0}^{n-1} 2^m + \log\left(48es\left(n\right)\right)^{s(n)} \\
&= 2^n - 1 + s(n)\left(\log(48e) + \log\left(s\left(n\right)\right)\right) \\
&= 2^n - 1 + \frac{2^n}{n}\left(1 + \frac{\alpha \log n}{n}\right)\left(\log\left(48e\right) + n - \log n + \log\left(1 + \frac{\alpha\log n}{n}\right)\right) \\
&< 2^n - 1 + \frac{2^n}{n}\left(n + \alpha\log n - \log n + 6\right) \\
&< 2^{n+1} - 1 - \frac{2^n}{n}\left(1 - \frac{\alpha}{2}\right)\log n \\
&= N - \frac{2^n}{n}\left(1 - \frac{\alpha}{2}\right)\log n.
\end{aligned}
$$

As a result, set

$$
\begin{aligned}
f(N) &= \left(1 - \frac{\alpha}{2}\right)\frac{2^n}{n}\log n \\
&= \left(1 - \frac{\alpha}{2}\right)\frac{N+1}{2(\log\left(N+1\right) - 1)}\log\left(\log\left(N+1\right) - 1\right).
\end{aligned}
$$

It is easy to see that $f \in \mathsf{FP}$ and $\sum_{n=0}^{\infty} 2^{-f(n)}$ is P-convergent. □

Corollary 6.2. *For all $\alpha < 1$, $\mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1 + \frac{\alpha\log n}{n}\right)\right)$ has SpanP-measure 0.*

Proof. This is immediate from Theorem 6.1 and Theorem 5.4. □

Corollary 6.3. *For all $\alpha < 1$, $\mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1 + \frac{\alpha\log n}{n}\right)\right)$ has Δ_3^{P}-measure 0 and measure 0 in Δ_3^{E}.*

Proof. This is immediate from Corollary 6.2 and Theorem 3.12. □

Under a derandomization hypothesis, Corollary 6.3 improves by one level in the exponential hierarchy to $\Delta_2^{\mathsf{E}} = \mathsf{E}^{\mathsf{NP}}$. This yields a stronger lower bound than other conditional approaches for obtaining lower bounds in E^{NP} [1, 10].

Corollary 6.4. *If Derandomization Hypothesis 2.2 is true, then for all $\alpha < 1$, $\mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1 + \frac{\alpha\log n}{n}\right)\right)$ has Δ_2^{P}-measure 0 and measure 0 in Δ_2^{E}.*

Proof. This is immediate from Corollary 6.2 and Theorem 3.14. □

Lutz [57] showed that for all $\alpha \in [0, 1]$, the class

$$
\mathcal{D}_\alpha = \mathsf{SIZE}\left(\alpha\frac{2^n}{n}\right)
$$

has PSPACE-dimension α. Athreya et al. [9] showed that $\mathcal{D}_\alpha$ also has strong PSPACE-dimension α. Hitchcock and Vinodchandran [40] showed that $\mathcal{H}_{\mathsf{NP}}(\mathcal{D}_\alpha) = \alpha$, yielding the improvement that $\mathcal{D}_\alpha$ has Δ_3^{P}-dimension α. It is immediate from this and Theorem 5.2 that $\mathcal{D}_\alpha$ has SpanP-dimension α. We improve this to $\#\mathsf{P}$-dimension by using a Kolmogorov complexity argument.

Theorem 6.5. *For all $\alpha \in [0, 1]$, $\dim_{\#\mathsf{P}}\left(\mathsf{SIZE}\left(\alpha\frac{2^n}{n}\right)\right) = \mathrm{Dim}_{\#\mathsf{P}}\left(\mathsf{SIZE}\left(\alpha\frac{2^n}{n}\right)\right) = \alpha$.*

Proof. Let $X_\alpha = \left(\mathsf{SIZE}\left(\alpha\frac{2^n}{n}\right)\right)$ and let $B \in X_\alpha$. For all sufficiently large n, $\langle B_{=n}, s\rangle \in \mathsf{MCSP}$ for $s = \alpha\frac{2^n}{n}$. Let C be a circuit of size s on n inputs. Frandsen and Miltersen [26] showed that there exists a stack program of size at most $(s+1)(c+\log(n+s))$ that constructs C. Let $\gamma > \beta > \alpha$ be arbitrarily close rationals. Let $p(n) = n^3$ and $q(n) = n^4$. For all n larger than some n_0,

$$\begin{aligned}
K^{p(2^n)}(B_{=n}) &\leq (s+1)(c+\log(n+s)) + O(\log n)\\
&\leq \left(\alpha\frac{2^n}{n}+1\right)\left(c+\log\left(\alpha\frac{2^n}{n}+n\right)\right) + O(\log n)\\
&\leq \left(\beta\frac{2^n}{n}\right)\left(c+\log\left(\beta\frac{2^n}{n}\right)\right)\\
&\leq \left(\beta\frac{2^n}{n}\right)(c+\log\beta+n-\log n)\\
&\leq \left(\beta\frac{2^n}{n}\right)n\\
&\leq \beta 2^n.
\end{aligned}$$

Let $N = 2^{n+1}-1$. We have

$$\begin{aligned}
K^{q(N)}(B_{\leq n}) &\leq \sum_{k=n_0}^{n} K^{p(2^k)}(B_{=k}) + O(n)\\
&\leq \beta N + O(n)\\
&\leq \gamma N,
\end{aligned}$$

so

$$\frac{K^{q(N)}(B\upharpoonright N)}{N} \leq \gamma$$

for all sufficiently large N of the form $2^{n+1}-1$. Therefore $\mathsf{Dim}_{\#\mathsf{P}}(X_\alpha) \leq \gamma$ by Theorem 5.8. The dimension lower bound holds because $\mathsf{dim}_{\#\mathsf{P}}(X_\alpha) \geq \mathsf{dim}_{\mathsf{H}}(X_\alpha) = \alpha$ [57]. The theorem follows because α and γ are arbitrarily close. □

Corollary 6.6. $\mathsf{P/poly}$ *has* $\#\mathsf{P}$*-strong dimension 0.*

Regarding infinitely-often classes, Hitchcock and Vinodchandran [40] showed that the class $\mathsf{SIZE}^{\text{i.o.}}\left(\alpha\frac{2^n}{n}\right)$ has NP-entropy rate and Δ_3^{P}-dimension $\frac{1+\alpha}{2}$. This extends to $\#\mathsf{P}$-dimension, with a proof similar to Theorem 6.5.

Theorem 6.7. *For all* $\alpha \in [0,1]$, $\mathsf{dim}_{\#\mathsf{P}}\left(\mathsf{SIZE}^{\text{i.o.}}\left(\alpha\frac{2^n}{n}\right)\right) = \frac{1+\alpha}{2}$.

Proof. Let $X_\alpha = \left(\mathsf{SIZE}^{\text{i.o.}}\left(\alpha\frac{2^n}{n}\right)\right)$ and let $B \in X_\alpha$. For all infinitely many n, $\langle B_{=n}, s\rangle \in \mathsf{MCSP}$ for $s = \alpha\frac{2^n}{n}$. Let $\gamma > \beta > \alpha$ be arbitrarily close rationals, and let $p(n) = n^3$ and $q(n) = n^4$. As in the proof of Theorem 6.5,

$$K^{p(2^n)}(B_{=n}) \leq \beta 2^n$$

for infinitely many n. Let $N = 2^{n+1}-1$. We have

$$\begin{aligned}
K^{q(N)}(B_{\leq n}) &\leq K^p(B_{<n}) + K^p(B_{=n}) + O(n)\\
&\leq 2^n - 1 + \beta 2^n + O(n)\\
&\leq \frac{1+\beta}{2}N + O(n)\\
&\leq \frac{1+\gamma}{2}N,
\end{aligned}$$

so

$$\frac{K^{q(N)}(B\upharpoonright N)}{N} \leq \frac{1+\gamma}{2}$$

for infinitely many N of the form $2^{n+1}-1$. Therefore $\mathsf{Dim}_{\#\mathsf{P}}(X_\alpha) \leq \frac{1+\gamma}{2}$ by Theorem 5.8. The dimension lower bound holds because $\mathsf{dim}_{\#\mathsf{P}}(X_\alpha) \geq \mathsf{dim}_{\mathsf{H}}(X_\alpha) = \frac{1+\alpha}{2}$ [40]. The theorem follows because α and γ are arbitrarily close. □

We note that any infinitely-often defined class like $\mathsf{SIZE}^{\mathsf{i.o.}}\left(\alpha\frac{2^n}{n}\right)$ in Theorem 6.5 always has its packing dimension and resource-bounded strong dimensions equal to 1 [28]:

$$\mathsf{Dim}_{\#\mathsf{P}}\left(\mathsf{SIZE}^{\mathsf{i.o.}}\left(\alpha\frac{2^n}{n}\right)\right) = \mathsf{Dim}_{\mathsf{pack}}\left(\mathsf{SIZE}^{\mathsf{i.o.}}\left(\alpha\frac{2^n}{n}\right)\right) = 1.$$

Li [51], building on work of Korten [47] and Chen, Hirahara, and Ren [16], showed that the symmetric exponential-time class $\mathsf{S}_2^{\mathsf{E}}$ requires exponential-size circuits.

Theorem 6.8. (Li [51]) $\mathsf{S}_2^{\mathsf{E}} \not\subseteq \mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\right)$.

Using Lutz's counting argument [55] as in the proof of Theorem 6.1, we improve this lower-bound to $\mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1+\frac{\alpha\log n}{n}\right)\right)$ for any $\alpha < 1$.

Theorem 6.9. *For all* $\alpha < 1$, $\mathsf{S}_2^{\mathsf{E}} \not\subseteq \mathsf{SIZE}^{\mathsf{i.o.}}\left(\frac{2^n}{n}\left(1+\frac{\alpha\log n}{n}\right)\right)$.

Proof. Li [51] showed there is a single-valued $\mathsf{FS}_2^{\mathsf{P}}$ function that given any polynomial-size circuit $C : \{0,1\}^n \to \{0,1\}^{n+1}$ outputs a nonimage of C. Li applies this algorithm to the truth-table generator circuit $\mathsf{TT}_{n,s}$ for $s = \frac{2^n}{n}$ and uses its 2^n-length output to define as the characteristic string of the $\mathsf{S}_2^{\mathsf{E}}$ language at length n. We observe that this proof works with $s = \frac{2^n}{n}\left(1+\frac{\alpha\log n}{n}\right)$ by Lutz's counting argument [55]. □

6.2 Quantum Circuit Complexity

Recent work has also studied circuit-size complexity within quantum models. For instance, Basu and Parida [11] showed that the number of distinct Boolean functions on n variables that can be computed by quantum circuits of size at most $c\frac{2^n}{n}$ is bounded by $2^{2^{n-1}}$, where $0 \leq c \leq 1$ is a constant that depends only on the maximum number of inputs of the gates. They proved this bound in a general setting in which the set of quantum gates is uncountably infinite. Using universal gate sets with constant fan-in, Chia et al. [17, 18] showed that the fraction of Boolean functions on n variables that require quantum circuits of size at least $\frac{2^n}{(c+1)n}$ is at least $1-2^{-\frac{2^n}{c+1}}$. We extend these quantum circuit-size bounds to a counting dimension result. In the following result, the BQSIZE class is independent of the choice of gate set because of the $o\left(\frac{2^n}{n}\right)$ size bound.

Theorem 6.10. $\mathsf{dim}_{\mathsf{GapP}}\left(\mathsf{BQSIZE}\left(o\left(\frac{2^n}{n}\right)\right)\right) = \mathsf{Dim}_{\mathsf{GapP}}\left(\mathsf{BQSIZE}\left(o\left(\frac{2^n}{n}\right)\right)\right) = 0$.

Proof. Let A be a language with quantum circuits of size $o(\frac{2^n}{n})$. We will use the Acceptance Probability Construction (Construction 4.9) technique to construct a GapP-martingale. Let $b \geq 1$ and let $s(n) = \frac{2^n}{bn}$. There exists n_0 such that for all $n \geq n_0$, the quantum circuit for $A_{=n}$ has a size of at most $s(n)$. Let $\vec{C} = (C_{n_0}, C_{n_0+1}, \ldots)$ be these quantum circuits. We assume that the circuits are amplified so that C_k has error probability at most 2^{-2k}.

Let $d_{\vec{C}}$ be a martingale that on input x if $2^{n_0}-1 \leq |x| \leq 2^{n+1}-1$ (i.e., we are betting on a string of length between n_0 and n), runs the Acceptance Probability Construction with circuit C_{n_0}

starting from length n_0 on the bits of x corresponding to length n_0. We bet on length n_0 using C_{n_0}, length n_0+1 using C_{n_0+1}, and so on, up to length n using C_n. If $|x| < 2^{n_0}-1$, $d_{\vec{C}}(x)=1$. Note that $d_{\vec{C}}(\lambda)=1$ and $d_{\vec{C}}$ is a GapP martingale.

For any length k where $n_0 \le k \le n$, $d_{\vec{C}}$ wins $\Omega(2^{2^k})$ by the analysis in Section 4.4. Therefore $d_{\vec{C}}(A_{\le n}) = \Omega(2^{2^{n+1}})$. Let $\gamma > 0$ be a constant so that $d_{\vec{C}}(A_{\le n}) \ge \gamma 2^{2^{n+1}}$ for all sufficiently large n.

Define $g_{n_0,n}$ on input $x \in \{0,1\}^{\le 2^{n+1}-1}$ to guess an extension $w \in \{0,1\}^{2^{n+1}-1}$ with $x \sqsubseteq w$ and guess a vector of quantum circuits $\vec{C} = (C_{n_0}, \ldots, C_n)$ where $\mathrm{size}(C_i) \le s(i)$ for all i from n_0 to n. Then $g_{n_0,n}$ computes $d_{\vec{C}}(w)$. Thus,

$$g_{n_0,n}(x) = \sum_{\vec{C}\,:\,(\forall i\in[n_0,n])\ \mathrm{size}(C_i)\le s(i)} d_{\vec{C}}(x).$$

By [18], there is a constant $c \ge 1$ depending on the universal gate set so that there are at most $2^{cs(n)\log s(n)} \le 2^{\frac{c}{b(c+1)}2^n}$ quantum circuits of size $s(n)$ for all sufficiently large n. Let $\delta = \frac{c}{b(c+1)}$ and let $\epsilon > \delta$ be a dyadic rational.

Define $h_n(x)$ to be $2^{\epsilon 2^{n+1}}$. Then

$$d_{n_0,n}(x) = \frac{g_{n_0,n}(x)}{h_n(x)}$$

is an exact GapP-martingale. We have

$$d_{n_0,n}(\lambda) \le \frac{\prod_{m=n_0}^{n} 2^{\delta 2^m}}{2^{\epsilon 2^{n+1}}} = \frac{2^{\sum_{m=n_0}^{n} \delta 2^m}}{2^{\epsilon 2^{n+1}}} = 2^{\delta(2^{n+1}-2^{n_0})-\epsilon 2^{n+1}} = 2^{(\delta-\epsilon)2^{n+1}-\delta 2^{n_0}}.$$

For $m \ge 0$, define

$$f_m(x) = \sum_{n_0=0}^{m}\sum_{n=n_0}^{m} d_{n_0,n}(x).$$

This is a uniform family of exact GapP-martingales. We have

$$f_m(\lambda) = \sum_{n_0=0}^{m}\sum_{n=n_0}^{m} d_{n_0,n}(\lambda) \le \sum_{n_0=0}^{m}\sum_{n=n_0}^{m} 2^{(\delta-\epsilon)2^{n+1}}.$$

There are $(m+1)^2$ terms in the double sum, each at most $2^{(\delta-\epsilon)2^{m+1}}$, so

$$f_m(\lambda) \le (m+1)^2 \cdot 2^{(\delta-\epsilon)2^{m+1}} = 2^{(\delta-\epsilon)2^{m+1}+2\log(m+1)}.$$

This makes $\sum\limits_{m=0}^{\infty} f_m(\lambda)$ P-convergent because $\epsilon > \delta$. Let

$$f(x) = \sum_{m=0}^{\infty} f_m(x).$$

By the Summation Lemma (Lemma 3.5), f is a GapP-martingale.

Let $B \in \mathsf{BQSIZE}(o(\frac{2^n}{n}))$ be arbitrary with small quantum circuits starting at some $n_0 \geq 0$. Let $\epsilon' > \epsilon$. We have

$$\begin{aligned} f(B_{\leq n}) &\geq f_n(B_{\leq n}) \\ &\geq d_{n_0,n}(B_{\leq n}) \\ &\geq \frac{\gamma 2^{2^{n+1}}}{2^{\epsilon 2^{n+1}}} \\ &= \gamma 2^{(1-\epsilon)2^{n+1}} \\ &\geq \gamma 2^{(1-\epsilon)(2^{n+1}-1)} \\ &\geq 2^{(1-\epsilon')(2^{n+1}-1)} \end{aligned}$$

for sufficiently large n. Therefore f ϵ'-strongly succeeds on B. Since $B \in \mathsf{BQSIZE}(o(\frac{2^n}{n}))$ and $\epsilon' > \epsilon$ are arbitrary, $\mathsf{BQSIZE}(o(\frac{2^n}{n}))$ has GapP-strong dimension at most ϵ. Since this holds for all $\epsilon > \delta$, the class has GapP-strong dimension at most $\delta = \frac{c}{b(c+1)}$. Since $b \geq 1$ is arbitrary, the class has GapP-strong dimension 0. □

Corollary 6.11. *$\mathsf{BQP/poly}$ has GapP-strong dimension 0.*

Lutz [57] showed that $\mathsf{SIZE}(\alpha\frac{2^n}{n})$ has PSPACE-dimension α and we improved this to $\#\mathsf{P}$-dimension α in Theorem 6.5. It remains open whether a similar result holds for quantum circuits in either PSPACE-dimension or GapP-dimension (or even Hausdorff dimension). Achieving this would refine the current dimension zero statement into an exact dimension classification for small quantum circuits, but it would apparently depend on the choice of universal quantum gate set.

Another interesting direction is determining the measure or dimension of $\mathsf{BQP/qpoly}$. While we know $\mathsf{BQP/poly}$ has GapP-dimension 0, extending this to quantum advice remains open. We note that Aaronson [2] has shown that $\mathsf{E}^{\#\mathsf{P}} \not\subseteq \mathsf{BQP/qpoly}$, so it would be consistent with Theorem 3.10 to show that $\mathsf{BQP/qpoly}$ has GapP-dimension 0.

A similar and simpler proof shows an infinitely-often version of Theorem 6.10, analogous to Theorem 6.7.

Theorem 6.12. $\dim_{\mathsf{GapP}}(\mathsf{BQSIZE}^{\mathrm{i.o.}}(o(\frac{2^n}{n}))) = \frac{1}{2}$.

6.3 Density of Hard Sets

Investigations of the density of hard sets for complexity classes began with motivation from the Berman-Hartmanis Isomorphism Conjecture [12]. A language S is *sparse* if $|S_{\leq n}| \leq p(n)$ for some polynomial p and all n. A language S is *dense* if $|S_{\leq n}| > 2^{n^\epsilon}$ for some $\epsilon > 0$ and almost all n. Let SPARSE be the class of all sparse languages and DENSE be the class of all dense languages. Meyer [69] showed that every hard set for E is dense. A problem is in $\mathsf{P/poly}$ if and only if it is in $\mathsf{P_T}(\mathsf{SPARSE})$, the polynomial-time Turing closure of SPARSE [12, 45]. A line of subsequent work strengthened these results in multiple directions [14, 15, 27, 29, 34, 59, 63, 64, 73, 87]. The current best result for E is that the polynomial-time bounded-query Turing reduction closures $\mathsf{P}_{n^\alpha-\mathsf{T}}(\mathsf{DENSE}^c)$ and $\mathsf{P}_{o(n/\log n)-\mathsf{T}}(\mathsf{SPARSE})$ both have P-dimension 0, implying every hard language for E is dense or sparse, respectively, under these reductions [34]. Wilson [88] showed that there is an oracle relative to which E has sparse hard sets under $O(n)$-truth-table reductions. We now show that counting measure can handle polynomial-time Turing reductions to nondense sets, even if they are computed by $\mathsf{P/poly}$ circuits. Note that the following theorem extends Corollary 6.6.

Theorem 6.13. *The class $(\mathsf{P/poly})_\mathsf{T}(\mathsf{DENSE}^c)$ of problems that $\mathsf{P/poly}$-Turing reduce to nondense sets has $\#\mathsf{P}$-dimension 0.*

Proof. Let $A \in (\mathsf{P/poly})_{\mathsf{T}}(\mathsf{DENSE}^c)$ be in the class. Composing the reduction with a lookup table for the nondense set shows that for all $\epsilon > 0$ and infinitely many n, the polynomial-time bounded Kolmogorov of $A_{\leq n}$ is at most 2^{n^ϵ}. We then apply Theorem 5.8. □

Corollary 6.14. *Every problem that is* P/poly*-Turing hard for* Δ_3^{E} *is* dense.

Proof. This follows from Theorem 6.13, Proposition 3.2, and Corollary 3.13. □

7 Conclusion

We have introduced #P, GapP, and SpanP counting measures and dimensions. These are intermediate in power between polynomial-time measure and dimension and polynomial-space measure and dimension. We have shown that counting measures and dimensions are useful for classes where the space-bounded measure or dimension is known but the time-bounded measure or dimension is not known. This is the primary way to use counting measures and dimensions and we expect more results in this form.

1. If $\mu_{\mathsf{PSPACE}}(X) = 0$ and $\mu_{\mathsf{P}}(X)$ is unknown, investigate the counting measures $\mu_{\#\mathsf{P}}(X)$, $\mu_{\mathsf{SpanP}}(X)$, and $\mu_{\mathsf{GapP}}(X)$.
2. If $\mathsf{dim}_{\mathsf{PSPACE}}(X) = \alpha$ is known and $\mathsf{dim}_{\mathsf{P}}(X)$ is unknown, investigate the counting dimensions $\mathsf{dim}_{\#\mathsf{P}}(X)$, $\mathsf{dim}_{\mathsf{SpanP}}(X)$, and $\mathsf{dim}_{\mathsf{GapP}}(X)$.
3. If $\mathsf{Dim}_{\mathsf{PSPACE}}(X) = \alpha$ is known and $\mathsf{Dim}_{\mathsf{P}}(X)$ is unknown, investigate the counting strong dimensions $\mathsf{Dim}_{\#\mathsf{P}}(X)$, $\mathsf{Dim}_{\mathsf{SpanP}}(X)$, and $\mathsf{Dim}_{\mathsf{GapP}}(X)$.

We strengthened Lutz's PSPACE-measure result by showing that the class of languages with circuit size $\frac{2^n}{n}(1 + \frac{\alpha \log n}{n})$ has SpanP-measure zero for all $\alpha < 1$. This improvement utilizes the Minimum Circuit Size Problem (MCSP) to bridge the gap between PSPACE-measure and SpanP-measure. As a consequence, we showed that this measure-theoretic circuit size lower bound holds in the third level of the exponential-time hierarchy, $\Delta_3^{\mathsf{E}} = \mathsf{E}^{\Sigma_2^{\mathsf{P}}}$. Previously this was only known to hold in the exponential-space class ESPACE. We also noted that recent work [51] on exponential circuit lower bounds for the symmetric alternation class S_2^{E} extends to this tighter $\frac{2^n}{n}(1 + \frac{\alpha \log n}{n})$ bound. Under derandomization assumptions, our results further improve to the second level, $\Delta_2^{\mathsf{E}} = \mathsf{E}^{\mathsf{NP}}$. We showed that BQP and more generally, the class of problems with $o\left(\frac{2^n}{n}\right)$-size quantum circuits, has GapP-strong dimension 0. This is the first work in resource-bounded measure or dimension to address quantum complexity. Our results on circuit-size complexity are summarized in Figure 1.3.

We conclude with several open questions. The relationships between counting dimensions and other dimension notions, entropy rates, and Kolmogorov complexity rates are summarized in Figure 5.1.

Question 7.1. *Can any of the relationships in Figure 5.1 be improved?*

Arvind and Köbler [8] showed that for each $\mathcal{C} \in \{\oplus\mathsf{P}, \mathsf{PP}\}$, $\mu_{\mathsf{P}}(\mathcal{C}) \neq 0$ implies $\mathsf{PH} \subseteq \mathcal{C}$. Hitchcock [32] showed that if SPP does not have P-measure 0, then $\mathsf{PH} \subseteq \mathsf{SPP}$. All of these classes have PSPACE-measure 0 and their P-measures are unknown, so the above paradigm applies:

Question 7.2. *What are the counting measures and dimensions of counting complexity classes including* PP*,* $\oplus$P*, and* SPP*?*

In particular, we know from Corollary 4.8 that GapP-random languages are not in SPP. It is known that SPP is low for GapP [20], meaning that an SPP oracle provides no additional power to GapP: $\mathsf{GapP}^{\mathsf{SPP}} = \mathsf{GapP}$. We do not know if SPP languages can be shown to uniformly have GapP-measure 0.

Question 7.3. *Does* SPP *have* GapP*-measure 0?*

We showed in Theorem 3.12 that SpanP-measure is dominated by Δ_3^{P}-measure, which implies Δ_3^{E} does not have SpanP-measure 0 or $\#\mathsf{P}$-measure 0. For GapP-measure, we only know that $\mathsf{E}^{\mathsf{GapP}} = \mathsf{E}^{\#\mathsf{P}}$ does not have GapP-measure 0.

Question 7.4. *What is the smallest complexity class that does not have* GapP*-measure 0?*

We also know that NP and UP have PSPACE-measure 0, but we do not know their P-measures. From Corollary 4.8, we know that SpanP-random languages are not in NP and $\#\mathsf{P}$-random languages are not in UP. As with SPP, it is not clear how to extend these proofs to show that the classes NP or UP have counting measure 0.

Question 7.5. *Does* NP *have* SpanP*-measure 0?*

Question 7.6. *Does* UP *have* $\#\mathsf{P}$*-measure 0?*

The measure hypothesis $\mu_{\mathsf{P}}(\mathsf{NP}) \neq 0$ is known to have many plausible consequences [38, 56, 60, 61]. Hypotheses that complexity classes do not have counting measure 0 could be interesting to study. For example:

$$\begin{array}{ccccc} \mu_{\mathsf{SpanP}}(\mathsf{NP}) \neq 0 & \Rightarrow & \mu_{\#\mathsf{P}}(\mathsf{NP}) \neq 0 & \Rightarrow & \mu_{\mathsf{P}}(\mathsf{NP}) \neq 0 \\ \Downarrow & & \Downarrow & & \Downarrow \\ \mu_{\mathsf{SpanP}}(\mathsf{PP}) \neq 0 & \Rightarrow & \mu_{\#\mathsf{P}}(\mathsf{PP}) \neq 0 & \Rightarrow & \mu_{\mathsf{P}}(\mathsf{PP}) \neq 0. \end{array}$$

Our results imply that if $\mu_{\#\mathsf{P}}(\mathsf{NP}) \neq 0$, then strong consequences hold for NP:

1. NP has problems with circuit-size complexity at least $\frac{2^n}{n}$ (Theorem 6.5).

2. The $\leq_{\mathsf{T}}^{\mathsf{P/poly}}$-hard languages for NP are dense (Theorem 6.13).

Question 7.7. *What else does* $\mu_{\#\mathsf{P}}(\mathsf{NP}) \neq 0$ *imply? How does it compare with the standard measure hypothesis* $\mu_{\mathsf{P}}(\mathsf{NP}) \neq 0$*?*

We were able to show in Theorem 6.5 that $\mathsf{SIZE}\left(\alpha \frac{2^n}{n}\right)$ has $\#\mathsf{P}$-dimension α, but in Theorem 6.10 we only showed that $\mathsf{BQSIZE}\left(o\left(\frac{2^n}{n}\right)\right)$ has GapP-strong dimension 0.

Question 7.8. *Is it possible to determine the* GapP*-dimension for the class of problems with* $\alpha\frac{2^n}{n}$*-size quantum circuits, for an appropriate choice of universal gate set?*

While $\mathsf{BQP/poly}$ has GapP-strong dimension 0, we do not know if this can be extended to quantum advice, even for GapP-measure.

Question 7.9. *Does* $\mathsf{BQP/qpoly}$ *have* GapP*-measure 0?*

Aaronson [2] has shown that $\mathsf{E}^{\#\mathsf{P}} \not\subseteq \mathsf{BQP/qpoly}$, so a positive answer to Question 7.9 is consistent with Theorem 3.10.

Acknowledgments. We thank Morgan Sinclaire and Saint Wesonga for helpful discussions.

References

[1] S. Aaronson, B. Aydinlioglu, H. Buhrman, J. Hitchcock, and D. van Melkebeek. A note on exponential circuit lower bounds from derandomizing Arthur-Merlin games. Technical Report TR10-174, Electronic Colloquium on Computational Complexity, 2010. 34

[2] Scott Aaronson. Oracles are subtle but not malicious. In *21st Annual IEEE Conference on Computational Complexity (CCC 2006), 16-20 July 2006, Prague, Czech Republic*, pages 340–354. IEEE Computer Society, 2006. `arXiv:0504048`, `doi:10.1109/CCC.2006.32`. 38, 40

[3] E. Allender and R. Rubinstein. P-printable sets. *SIAM Journal on Computing*, 17:1193–1202, 1988. `doi:10.1137/0217075`. 4

[4] K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In A. Sorbi, editor, *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics, pages 1–47. Marcel Dekker, New York, N.Y., 1997. `doi:10.1201/9780429187490-1`. 3, 4, 9

[5] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn. Genericity and measure for exponential time. *Theoretical Computer Science*, 168(1):3–19, 1996. `doi:10.1016/0304-3975(96)89424-2`. 10

[6] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009. 9

[7] Srinivasan Arunachalam, Alex B. Grilo, Tom Gur, Igor C. Oliveira, and Aarthi Sundaram. Quantum learning algorithms imply circuit lower bounds. In *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*, pages 562–573. IEEE, 2021. `doi:10.1109/FOCS52979.2021.00062`. 24

[8] V. Arvind and J. Köbler. On pseudorandomness and resource-bounded measure. *Theoretical Computer Science*, 255(1–2):205–221, 2001. `doi:10.1016/s0304-3975(99)00164-4`. 39

[9] K. B. Athreya, J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. Effective strong dimension in algorithmic information and computational complexity. *SIAM Journal on Computing*, 37(3):671–705, 2007. `arXiv:cs.CC/0211025`, `doi:10.1137/s0097539703446912`. 3, 4, 5, 9, 13, 25, 34

[10] B. Aydinlioglu, D. Gutfreund, J. M. Hitchcock, and A. Kawachi. Derandomizing Arthur-Merlin games and approximate counting implies exponential-size lower bounds. *Computational Complexity*, 20(2):329–366, 2011. `doi:10.1007/s00037-011-0010-8`. 34

[11] Saugata Basu and Laxmi Parida. Quantum analog of Shannon's lower bound theorem. Technical Report 2308.13091, arXiv, 2023. `arXiv:2308.13091`. 36

[12] L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing*, 6(2):305–322, 1977. `doi:10.1137/0206023`. 38, 45

[13] R. V. Book. Tally languages and complexity classes. *Information and Control*, 26:186–193, 1974. `doi:10.1016/s0019-9958(74)90473-2`. 16

[14] H. Buhrman, L. Fortnow, J. M. Hitchcock, and B. Loff. Learning reductions to sparse sets. In *Proceedings of the 38th International Symposium on Mathematical Foundations of Computer Science*, pages 243–253. Springer-Verlag, 2013. `doi:10.1007/978-3-642-40313-2_23`. 38

[15] H. Buhrman and S. Homer. Superpolynomial circuits, almost sparse oracles and the exponential hierarchy. In *Proceedings of the 12th Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 116–127. Springer, 1992. doi:10.1007/3-540-56287-7_99. 38

[16] Lijie Chen, Shuichi Hirahara, and Hanlin Ren. Symmetric exponential time requires near-maximum circuit size. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, page 1990–1999, New York, NY, USA, 2024. Association for Computing Machinery. doi:10.1145/3618260.3649624. 7, 36

[17] Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang. Quantum meets the minimum circuit size problem. Technical Report 2108.03171, arXiv, 2021. arXiv:2108.03171. 36

[18] Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang. Quantum Meets the Minimum Circuit Size Problem. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 47:1–47:16, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2022.47. 24, 36, 37

[19] R. Downey and D. Hirschfeldt. *Algorithmic Randomness and Complexity.* Springer-Verlag, 2010. doi:10.1007/978-0-387-68441-3. 4

[20] S. A. Fenner, L. Fortnow, and S. A. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994. doi:10.1016/s0022-0000(05)80024-8. 3, 6, 11, 24, 40

[21] Stephen Fenner, Lance Fortnow, Stuart A Kurtz, and Lide Li. An oracle builder's toolkit. *Information and Computation*, 182(2):95–136, 2003. doi:10.1016/S0890-5401(03)00018-X. 24

[22] Stephen A. Fenner. PP-lowness and a simple definition of AWPP. *Theory of Computing Systems*, 36(3):199–212, 2003. doi:10.1007/s00224-002-1089-8. 24

[23] L. Fortnow. Counting complexity. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 81–107. Springer-Verlag, 1997. doi:10.1007/978-1-4612-1872-2_4. 3

[24] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999. doi:10.1006/jcss.1999.1651. 22, 24

[25] Lance Fortnow. One complexity theorist's view of quantum computing. *Theoretical Computer Science*, 292(3):597–610, 2003. doi:10.1016/S0304-3975(01)00377-2. 22

[26] Gudmund Skovbjerg Frandsen and Peter Bro Miltersen. Reviewing bounds on the circuit size of the hardest functions. *Information Processing Letters*, 95(2):354–357, 2005. doi:10.1016/j.ipl.2005.03.009. 7, 35

[27] B. Fu. With quasilinear queries EXP is not polynomial time Turing reducible to sparse sets. *SIAM Journal on Computing*, 24(5):1082–1090, 1995. doi:10.1137/s0097539792237188. 8, 38

[28] X. Gu. A note on dimensions of polynomial size circuits. *Theoretical Computer Science*, 359(1–3):176–187, 2006. doi:10.1016/j.tcs.2006.02.022. 36

[29] Ryan C. Harkins and John M. Hitchcock. Dimension, halfspaces, and the density of hard sets. *Theory of Computing Systems*, 49(3):601–614, 2011. doi:10.1007/S00224-010-9288-1. 38

[30] F. Hausdorff. Dimension und äußeres Maß. *Mathematische Annalen*, 79:157–179, 1919. doi:10.1007/BF01457179. 4, 12

[31] J. M. Hitchcock. *Effective Fractal Dimension: Foundations and Applications*. PhD thesis, Iowa State University, 2003. URL: https://www.proquest.com/dissertations-theses/effective-fractal-dimension-foundations/docview/305335849/se-2. 7, 27, 28, 31

[32] J. M. Hitchcock. The size of SPP. *Theoretical Computer Science*, 320(2–3):495–503, 2004. doi:10.1016/s0304-3975(04)00128-8. 39

[33] J. M. Hitchcock. Correspondence principles for effective dimensions. *Theory of Computing Systems*, 38(5):559–571, 2005. doi:10.1007/s00224-004-1122-1. 27, 28

[34] J. M. Hitchcock. Online learning and resource-bounded dimension: Winnow yields new lower bounds for hard sets. *SIAM Journal on Computing*, 36(6):1696–1708, 2007. arXiv:cs/0512053, doi:10.1137/050647517. 8, 38

[35] J. M. Hitchcock, M. López-Valdés, and E. Mayordomo. Scaled dimension and the Kolmogorov complexity of Turing-hard sets. *Theory of Computing Systems*, 43(3-4):471–497, 2008. doi:10.1007/s00224-007-9013-x. 4

[36] J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. Scaled dimension and nonuniform complexity. *Journal of Computer and System Sciences*, 69(2):97–122, 2004. doi:10.1016/j.jcss.2003.09.001. 32

[37] J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. The fractal geometry of complexity classes. *SIGACT News*, 36(3):24–38, September 2005. doi:10.1145/1086649.1086662. 3, 4, 9

[38] J. M. Hitchcock and A. Pavan. Hardness hypotheses, derandomization, and circuit complexity. *Computational Complexity*, 17(1):119–146, 2008. doi:10.1007/s00037-008-0241-5. 40

[39] J. M. Hitchcock and A. Pavan. On the NP-completeness of the minimum circuit size problem. In *Proceedings of the 35th IARCS Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 236–245. Leibniz International Proceedings in Informatics, 2015. doi:10.4230/LIPICS.FSTTCS.2015.236. 33

[40] J. M. Hitchcock and N. V. Vinodchandran. Dimension, entropy rates, and compression. *Journal of Computer and System Sciences*, 72(4):760–782, 2006. doi:10.1016/j.jcss.2005.10.002. 4, 7, 8, 9, 10, 11, 27, 28, 31, 34, 35, 36

[41] R. Impagliazzo and A. Wigderson. Randomness vs. time: Derandomization under a uniform assumption. *Journal of Computer and System Sciences*, 63:672–688, 2001. doi:10.1006/jcss.2001.1780. 22

[42] D. W. Juedes and J. H. Lutz. Weak completeness in E and E_2. *Theoretical Computer Science*, 143(1):149–158, 1995. doi:10.1016/0304-3975(95)80030-D. 13

[43] D. W. Juedes and J. H. Lutz. Completeness and weak completeness under polynomial-size circuits. *Information and Computation*, 125(1):13–31, 1996. doi:10.1006/inco.1996.0017. 4

[44] V. Kabanets and J.-Y. Cai. Circuit minimization problem. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 73–79. ACM, 2000. doi:10.1145/335305.335314. 7, 33

[45] R. M. Karp and R. J. Lipton. Turing machines that take advice. *L'Enseignement Mathématique*, 28:191–201, 1982. doi:10.5169/seals-52237. 38

[46] J. Köbler, U. Schöning, and J. Toran. On counting and approximation. *Acta Informatica*, 26(4):363–379, 1989. doi:10.1007/BF00276023. 3, 10

[47] Oliver Korten. The hardest explicit construction. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 433–444. IEEE, 2022. doi:10.1109/FOCS52979.2021.00051. 7, 36

[48] W. Kuich. On the entropy of context-free languages. *Information and Control*, 16:173–200, 1970. doi:10.1016/s0019-9958(70)90105-1. 27

[49] Henri Lebesgue. Intégrale, longueur, aire. *Annali di Matematica Pura ed Applicata*, 7(1):231–359, 1902. doi:10.1007/BF02420592. 4, 12

[50] Lide Li. *On the counting functions*. PhD thesis, University of Chicago, 1993. URL: https://www.proquest.com/dissertations-theses/on-counting-functions/docview/304080357/se-2. 3, 11

[51] Zeyong Li. Symmetric exponential time requires near-maximum circuit size: Simplified, truly uniform. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, page 2000–2007, New York, NY, USA, 2024. Association for Computing Machinery. doi:10.1145/3618260.3649615. 7, 36, 39

[52] O. B. Lupanov. On the synthesis of contact networks. *Doklady Akademii Nauk SSSR*, 119(1):23–26, 1958. 3, 7

[53] J. H. Lutz. *Resource-Bounded Category and Measure in Exponential Complexity Classes*. PhD thesis, California Institute of Technology, 1987. doi:10.7907/qny92-v6h14. 3

[54] J. H. Lutz. Category and measure in complexity classes. *SIAM Journal on Computing*, 19(6):1100–1131, 1990. doi:10.1137/0219076.

[55] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44(2):220–258, 1992. doi:10.1016/0022-0000(92)90020-j. 3, 4, 5, 7, 9, 12, 15, 16, 29, 33, 34, 36

[56] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 225–254. Springer-Verlag, 1997. doi:10.1007/978-1-4612-1872-2_10. 3, 4, 9, 22, 40

[57] J. H. Lutz. Dimension in complexity classes. *SIAM Journal on Computing*, 32(5):1236–1259, 2003. arXiv:cs/0203016, doi:10.1137/S0097539701417723. 3, 4, 5, 8, 9, 12, 13, 15, 34, 35, 38

[58] J. H. Lutz. Effective fractal dimensions. *Mathematical Logic Quarterly*, 51(1):62–72, 2005. doi:10.1002/malq.200310127. 4, 9

[59] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23(4):762–779, 1994. doi:10.1137/s0097539792237498. 8, 38

[60] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*, 164(1–2):141–163, 1996. doi:10.1016/0304-3975(95)00189-1. 40

[61] J. H. Lutz and E. Mayordomo. Twelve problems in resource-bounded measure. *Bulletin of the European Association for Theoretical Computer Science*, 68:64–80, 1999. Also appears as [62]. 3, 4, 9, 40

[62] J. H. Lutz and E. Mayordomo. Twelve problems in resource-bounded measure. In G. Păun, G. Rozenberg, and A. Salomaa, editors, *Current Trends in Theoretical Computer Science: Entering the 21st Century*, pages 83–101. World Scientific Publishing, 2001. doi:10.1142/9789812810403_0001. 45

[63] J. H. Lutz and Y. Zhao. The density of weakly complete problems under adaptive reductions. *SIAM Journal on Computing*, 30(4):1197–1210, 2000. doi:10.1137/s0097539797321547. 8, 38

[64] S. R. Mahaney. Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis. *Journal of Computer and System Sciences*, 25(2):130–143, 1982. doi:10.1016/0022-0000(82)90002-2. 38

[65] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science*, 136(2):487–506, 1994. doi:10.1016/0304-3975(94)00023-c. 7, 25, 26

[66] E. Mayordomo. *Contributions to the study of resource-bounded measure*. PhD thesis, Universitat Politècnica de Catalunya, 1994. URL: https://eccc.weizmann.ac.il/static/books/Contributions_to_the_Study_of_Resource_Bounded_Measure/. 4, 9, 33

[67] E. Mayordomo. Effective Hausdorff dimension. In B. Löwe, B. Piwinger, and T. Räsch, editors, *Classical and New Paradigms of Computation and their Complexity Hierarchies*, volume 23 of *Trends in Logic*, pages 171–186. Kluwer Academic Press, 2004. doi:10.1007/978-1-4020-2776-5_10. 4, 9

[68] E. Mayordomo. Effective fractal dimension in algorithmic information theory. In S. B. Cooper, B. Löwe, and A. Sorbi, editors, *New Computational Paradigms: Changing Conceptions of What is Computable*, pages 259–285. Springer-Verlag, 2008. doi:10.1007/978-0-387-68546-5_12. 4, 9

[69] A. R. Meyer, 1977. Reported in [12]. 38

[70] P. B. Miltersen, N. V. Vinodchandran, and O. Watanabe. Superpolynomial versus subexponential circuit size in the exponential hierarchy. In *Proceedings of the Fifth Annual International Computing and Combinatorics Conference*, pages 210–220, 1999. doi:10.1007/3-540-48686-0_21. 7

[71] Cody D. Murray and R. Ryan Williams. On the (non) NP-hardness of computing circuit complexity. *Theory of Computing*, 13(4):1–22, 2017. doi:10.4086/toc.2017.v013a004. 33

[72] Satyadev Nandakumar, Subin Pulari, Akhil S, and Suronjona Sarma. One-way functions and polynomial time dimension. Technical Report 2411.02392, arXiv, 2025. arXiv:2411.02392. 7, 32

[73] M. Ogiwara and O. Watanabe. On polynomial-time bounded truth-table reducibility of NP sets to sparse sets. *SIAM Journal on Computing*, 20(3):471–483, 1991. doi:10.1137/0220030. 38

[74] K. W. Regan, D. Sivakumar, and J. Cai. Pseudorandom generators, measure theory, and natural proofs. In *Proceedings of the 36th Symposium on Foundations of Computer Science*, pages 26–35. IEEE Computer Society, 1995. doi:10.1109/SFCS.1995.492459. 22

[75] C. A. Rogers. *Hausdorff Measures*. Cambridge University Press, 1998. Originally published in 1970. 28

[76] Uwe Schöning. The power of counting. In Alan L. Selman, editor, *Complexity Theory Retrospective*, pages 204–223. Springer, 1990. doi:10.1007/978-1-4612-4478-3_9. 3

[77] R. Shaltiel and C. Umans. Pseudorandomness for approximate counting and sampling. In *Proceedings of the 20th IEEE Conference on Computational Complexity*, pages 212–226. IEEE Computer Society, 2005. doi:10.1007/s00037-007-0218-9. 10, 11

[78] C. E. Shannon. The synthesis of two-terminal switching circuits. *Bell System Technical Journal*, 28(1):59–98, 1949. doi:10.1002/j.1538-7305.1949.tb03624.x. 3, 7

[79] L. Staiger. Recursive automata on infinite words. In *Proceedings of the 10th Annual Symposium on Theoretical Aspects of Computer Science*, pages 629–639. Springer-Verlag, 1993. doi:10.1007/3-540-56503-5_62. 28

[80] L. J. Stockmeyer. On approximation algorithms for #P. *SIAM Journal on Computing*, 14:849–861, 1985. doi:10.1137/0214060. 4, 10, 33

[81] Donald M. Stull. Resource bounded randomness and its applications. In Johanna N. Y. Franklin and Christopher P. Porter, editors, *Algorithmic Randomness: Progress and Prospects*, volume 50 of *Lecture Notes in Logic*, page 301–348. Cambridge University Press, Cambridge, 2020. doi:10.1017/9781108781718.010. 4, 9

[82] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991. doi:10.1137/0220053. 16, 18

[83] C. Tricot. Two definitions of fractional dimension. *Mathematical Proceedings of the Cambridge Philosophical Society*, 91:57–74, 1982. 12

[84] Leslie G Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979. doi:10.1016/0304-3975(79)90044-6. 3, 10

[85] D. van Melkebeek. The zero-one law holds for BPP. *Theoretical Computer Science*, 244(1–2):283–288, 2000. doi:10.1016/s0304-3975(00)00191-2. 22

[86] J. Ville. *Étude Critique de la Notion de Collectif*. Gauthier–Villars, Paris, 1939. 4, 13

[87] O. Watanabe. Polynomial time reducibility to a set of small density. In *Proceedings of the Second Structure in Complexity Theory Conference*, pages 138–146. IEEE Computer Society, 1987. doi:10.1109/PSCT.1987.10319263. 38

[88] C. B. Wilson. Relativized circuit complexity. *Journal of Computer and System Sciences*, 31(2):169–181, 1985. doi:10.1016/0022-0000(85)90040-6. 38

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il