

Compressibility Measures for Affinely Singular Random Vectors

Mohammad-Amin Charusaie, Arash Amini, *Senior, IEEE*, and Stefano Rini, *Senior, IEEE*

Abstract—There are several ways to measure the compressibility of a random measure; they include general approaches such as using the rate-distortion curve, as well as more specific notions, such as the Rényi information dimension (RID). The RID parameter indicates the concentration of the measure around lower-dimensional subsets of the space. While the evaluation of such compressibility parameters is well-studied for continuous and discrete measures, the case of discrete-continuous measures is quite subtle. In this paper, we focus on a class of multi-dimensional random measures that have singularities on affine lower-dimensional subsets. This class of distributions naturally arises when considering linear transformation of component-wise independent discrete-continuous random variables. To measure the compressibility of such distributions, we introduce the new notion of dimensional-rate bias (DRB) which is closely related to the entropy and differential entropy in discrete and continuous cases, respectively. Similar to entropy and differential entropy, DRB is useful in evaluating the mutual information between distributions of the aforementioned type. Besides the DRB, we also evaluate the RID of these distributions. We further provide an upper-bound for the RID of multi-dimensional random measures that are obtained by Lipschitz functions of component-wise independent discrete-continuous random variables (\mathbf{X}). The upper-bound is shown to be achievable when the Lipschitz function is $A\mathbf{X}$, where A satisfies $\text{SPARK}(A_{m \times n}) = m + 1$ (e.g., Vandermonde matrices). When considering discrete-domain moving-average processes with non-Gaussian excitation noise, the above results allow us to evaluate the block-average RID and DRB, as well as to determine a relationship between these parameters and other existing compressibility measures.

Index Terms—Discrete-Continuous Random Variables; Information Dimension; Moving-Average Processes; Rate-Distortion Function.

I. INTRODUCTION

Data compression has been widely utilized for cutting the storage and transmission costs for various sources of data. The Shannon entropy [1] is possibly the most fundamental notion of compressibility, which presents the minimum achievable rate to describe the outputs of a discrete source in bits using any lossless method. For continuous sources, the compressibility notion needs to be cautiously defined, in view of the fact that source realizations require an infinite number of bits to be described. A similar measure for this scenario is the differential entropy, in which a diverging term

is excluded from the entropy of the quantized source outputs. While the differential entropy is a natural extension of the entropy, it is not defined for singular or discrete-continuous sources. Further, its applicability as a compressibility measure has been challenged in the literature [2]. An early alternative of differential entropy is introduced by Rényi in [3], and studied for discrete-continuous distributions. A recent work [4] also studied an extension of differential entropy notion for rectifiable distributions.

Another notion of compressibility which also takes into account the lossy methods is the Rate-Distortion Function (RDF) [5]; the RDF represents the minimum bit-rate required to describe a source within some fidelity criterion. It is well known that when the distortion tends to zero ($D \rightarrow 0$), the limiting value of the RDF is closely related to the differential entropy (if it exists) [6]. The compressibility notions are not limited to discrete and continuous sources: there has been some recent efforts to define a notion of compressibility for sequences [7], [8], [9] and random processes [10], [11], [12], [13].

The Rényi Information Dimension (RID) defined in [3] measures the compressibility of a general random variable/vector (RV), beyond the discrete/continuous cases¹. For a mixture of discrete and continuous probability measures with real domain, the RID quantifies the fraction of the continuous part. The RID plays an important role in a number of applications such as signal quantization [14], sparse signal recovery [15], and chaos theory [16]. Despite the generality of its definition, Rényi evaluated the RID only for discrete-continuous RVs and absolutely continuous random vectors; a class of singular RVs with self-similar measures was later studied in [17]. Kawabata and Dembo in [18] showed that the RDF in the high-resolution case ($D \rightarrow 0$, where D is distortion) has an asymptotic log-scaling behavior with the rate equal to half the RID.

In this paper, we study the compressibility of n -dimensional random distributions that are composed of finitely or countably many components, each having an absolutely continuous distribution on an affine subset of \mathbb{R}^n . A typical example is an n -dimensional distribution that has singularities on a number of hyperplanes and points. This example is particularly helpful when studying linear transformations of independently distributed discrete-continuous RVs. More specifically, if X_i s are independent and have discrete-continuous measures, the random vector $A\mathbf{X}^n$, where A is an arbitrary matrix and $\mathbf{X}^n = [X_1, \dots, X_n]^T$, has singularities over affine subsets that are determined by A . For this class of measures, we investigate

M. Charusaie was with Sharif university of technology, Tehran, Iran, at the time of writing this manuscript and is now with Max Planck Institute for Intelligent Systems, Tübingen, Germany. (email: mcharusaie@tuebingen.mpg.de)

A. Amini is with the Advanced Communication Research Institute (ACRI), department of electrical engineering, Sharif university of technology, Tehran, Iran. (email: aamini@sharif.edu).

S. Rini is with the electrical and computer engineering department, National Chiao Tung university, Hsinchu, Taiwan. (email: stefano@nctu.edu.tw)

A part of this paper was presented in the International Symposium on Information Theory, 21-26 June, 2020.

¹For brevity, we use the same acronym for random variables and vectors.

the RDF for $D \rightarrow 0$, introduce a new compressibility notion accordingly and draw a link between this notion and mutual information between two RVs. We further study Lipschitz transformations –instead of linear mappings– of such RVs and derive a bound for the resulting RID. As an interesting application, we derive various compressibility measures for discrete-domain moving-average processes with discrete-continuous excitation noise. With this result, we establish a link between the studied compressibility measures (e.g., undersampling rate in the compressed sensing problem) and the RID of the corresponding excitation noise.

Related works

After the notion of information and entropy were introduced in [1], Kolmogorov studied the rate-distortion curve for continuous measures with ℓ_∞ -norm (and quadratic) distortion function in [2] under the name ϵ -entropy. Specifically, he calculated the ϵ -entropy for Gaussian processes. Again, Shannon returned to the rate-distortion problem in [5] and provided a general lower-bound, which is now known as the Shannon lower bound (SLB). For the case of the difference distortion function, Lin'kov provided a set of equations in [19] to evaluate the SLB. Under certain conditions, he further proved that SLB is asymptotically (vanishingly small distortion values) tight. The SLB for the more general expected ℓ_p -norm distortion functions was investigated in [20]. For these distortion functions, the tightness of the SLB was again confirmed in [6] in the low-distortion regime. The study of SLB for discrete-continuous probability measures appeared later in [21] and [22], for the one-dimensional and multi-dimensional random vectors, respectively.

In [3], instead of the previously common rate-distortion function, Rényi introduced the notions of information dimension (RID) and the dimensional entropy (RDE) to measure the compressibility of continuous-domain RVs (whether continuous or discrete-continuous). In simple words, RID corresponds to the asymptotic log-scaling of the entropy when the RV is uniformly quantized with a vanishing step size. For bounded RVs, Rényi observed that as $\epsilon \rightarrow 0$, the ϵ -entropy divided by $\log \frac{1}{\epsilon}$ has a limiting point that coincides with the RID. Interestingly, the case of multi-dimensional discrete-continuous random vectors is excluded from the Rényi's work (Rényi leaves this part as an open problem). While the RID of n -dimensional continuous RVs is shown to be n in [3], Csiszár in [23] proved the converse that the RID is strictly below n if the distribution is not continuous (e.g., contains singularities). The exact evaluation of the RID for a class of self-similar probability measures with singularity was carried out in [17].

In [18], a link between the RID and rate-distortion curve was found; it was shown that for a class of distortion functions, the asymptotic (vanishingly small distortion values) log-scaling of the rate-distortion function (called rate-distortion dimension or RDD) coincides with the RID.

More recently, RID was given an operational interpretation in almost lossless compression of analog memoryless sources in [10]. Specifically, it was shown that in a compressed sensing

problem where the high-dimensional vector is generated by a memoryless source, the minimum achievable undersampling rate is given by the RID of the source. The class of memoryless sources is extended to bounded Ψ^* -mixing processes in [12]. The compressed sensing problem is a typical example of projecting a high-dimensional source onto a lower dimensional subspace. Obviously, the RID of the projected source cannot exceed the RID of the original source. Interestingly, it is shown in [24] that RID remains constant with probability 1, if the projection is selected with Haar measure among all possible projections.

The concept of compressibility has also been generalized for discrete-domain stochastic processes. In particular, the notion of rate-distortion dimension (RDD) is defined in [18] using the log-scaling constant of the rate distortion function under vanishing distortion condition when asymptotically large number of samples are considered. The RDD notion is linked to some non-asymptotic concepts considered in the past. For instance, the results in [25] imply that memoryless processes (e.g., white noise) have the maximum RDD values among stationary processes. Besides, the results in [26] could be used to compute the RDD value for two special cases of discrete-domain autoregressive Gaussian processes.

The extension of RID to discrete-domain stochastic processes was considered in both [12] and [27]. In [12], the average RID of a block of samples with increasingly large block size is defined as the block-average information dimension (BID). It was later shown in [11] that BID coincides with RDD under certain conditions. The generalization in [27], however, relies on the log-scaling behavior of the entropy rate of the quantized samples. Unlike the BID, the latter notion always coincides with RDD.

For continuous-domain innovation processes (i.e., continuous-domain white noise), the notions of RID and RDE are defined in [13] by vanishingly fine quantization of the time axis and the amplitude range.

As for the rectifiable singular measures, a new compressibility measure based on Hausdorff density is introduced in [4].

Paper Organization

The remainder of the paper is organized as follows. We provide an overview of the results and notations of the paper in Section I. Preliminary notions related to this work are introduced in Section III. In Section IV we explain the main class of random variables studied in this work, the affinely singular random variables. Our study consist of multiple compressibility measures for these random variables and associated random processes. We describe our main results on random vectors in Section V. In Section VI, we investigate a new compressibility measure (i.e., DRB) for affinely singular RVs, and explain its connections with conventional mutual information between two RVs. Our results for random processes, specifically samples of moving average processes, are provided in Section III-B. Finally, Section VII concludes the paper.

II. OVERVIEW OF THE RESULTS AND NOTATIONS

Sequences of independent and identically distributed (i.i.d.) RVs (alternatively known as discrete-domain white noise) are widely used in stochastic modeling of physical phenomena. Most natural signals (such as images) have correlated structures, which enables us to compress them. It is therefore common to decorrelate a signal by means of a linear transformation so as to derive the most incompressible form of the signal without losing information. The decorrelated signal is oftentimes modeled by a discrete-domain white noise. As a result, the signals of interest are modeled by linear transformations of i.i.d. RVs. Because of the sparsity and compressibility properties, discrete-continuous RVs such as the Bernoulli-Gaussian law are of special interest. This in turn implies that we are dealing with linear transformations of independent discrete-continuous RVs in such models.

To measure the compressibility of the resulting linear transformations, we focus on the RDF of the outcome as $D \rightarrow 0$. While the RDF of absolutely continuous random vectors and independent collection of discrete-continuous RVs are studied in the past, there is not much to mention for the case of statistically dependent collection of discrete-continuous RVs. In this paper, we study the RDF of linear transformations of discrete-continuous RVs as a subclass of statistically dependent collection of discrete-continuous RVs.

Contributions

To describe the random vectors with singular distributions, we introduce *affinely singular* RVs. A central concept in this definition is a d -dimensional affine subset \mathcal{A} of \mathbb{R}^m , which is defined as a set that by a shift $\mathcal{A} - \mathbf{b}$ turns into a d -dimensional vector subspace of \mathbb{R}^m .

Definition 1: Let $\{\mu_i(\cdot)\}_i$ be a finite or countably infinite set of absolutely continuous probability measures on distinct e_i -dimensional affine subsets² \mathcal{A}_i of \mathbb{R}^m , for $e_i \in \{0, 1, \dots\}$; we interpret $e_i = 0$ (for which \mathcal{A}_i consists of a single point) as $\mu_i(\mathcal{B}) = \mathbb{1}_{\mathcal{A}_i \in \mathcal{B}}$. A measure $\mu(\cdot)$ is defined as *affinely singular*, if there exists a set $\{p_i\}$, where $p_i \in \mathbb{R}^+ \setminus \{0\}$, such that for every measurable set $\mathcal{B} \subseteq \mathbb{R}^m$ we have

$$\mu(\mathcal{B}) = \sum_i p_i \mu_i(\mathcal{B} \cap \mathcal{A}_i). \quad (1)$$

In Definition 1 we employ the term ‘‘absolute continuity’’ with the following acceptance: define a generic transformation f_i from an e_i -dimensional Euclidean space to the set \mathcal{A}_i as a combination of a rotation and shift. With this decomposition of f_i , we say that a measure $\mu_i(\cdot)$ is an absolutely continuous probability measures if it is absolutely continuous with respect to the push-forward measure $\ell_i(f_i^{-1}(\cdot))$, where $\ell_i(\cdot)$ is the Lebesgue measure on the e_i -dimensional Euclidean space.

In this paper, we derive the RID and DRB of affinely singular random vectors in a closed form. As a special application, we study these compressibility measures for linear transformation of a sub-class of affinely singular RVs (see Section IV), which we refer to as *orthogonally singular* RVs.

²A d -dimensional affine set in \mathbb{R}^m with $d \leq m$ is the image of the mapping $f : \mathbb{R}^d \rightarrow \mathbb{R}^m$, where f is an affine transformation $f(\mathbf{x}^d) = A\mathbf{x}^d + \mathbf{b}$.

Definition 2: Consider the RV $\mathbf{X}^n = [X_1, \dots, X_n]^\top$ comprised of discrete-continuous entries

$$X_i \stackrel{\text{d}}{=} \nu_i X_{c,i} + (1 - \nu_i) X_{d,i}, \quad (2)$$

where ν_i is a Bernoulli RV ($\mathbb{P}(\nu_i = 1) = \alpha_i$), $X_{c,i}$ is a RV with absolutely continuous distribution, and $X_{d,i}$ is a discrete RV. The RV \mathbf{X}^n is said to be orthogonally singular if $\{X_{c,i}\}_{i=1}^n$ form a set of jointly continuous RVs independent of $\mathbf{X}_d = [X_{d,1}, \dots, X_{d,2}]$ and $\boldsymbol{\nu} = [\nu_1, \dots, \nu_n]$, while \mathbf{X}_d and $\boldsymbol{\nu}_d$ could be dependent with the joint probability mass function $P_{\boldsymbol{\nu}, \mathbf{X}_d}(\cdot)$.

Note that if $\alpha_1 = \dots = \alpha_n = 1$, then, \mathbf{X}^n has an absolutely continuous distribution; otherwise, the distribution of \mathbf{X}^n contains singularities that are supported on hyper-planes aligned with some of the coordinate axes, which explains the name orthogonally singular.

Now, if we consider a linear transformation of \mathbf{X}^n such as

$$\mathbf{Y}^m = A_m \mathbf{X}^n, \quad (3)$$

then, \mathbf{Y}^m is likely not to be orthogonally singular as we show in Lemma 3. In this paper, besides finding the RDF of non-orthogonally singular random vectors \mathbf{Y}^m for limiting distortion $D \rightarrow 0$, we derive an expression for the RID of \mathbf{Y}^m that is determined by $P_{\boldsymbol{\nu}, \mathbf{X}_d}(\cdot)$ and the rank of some of the submatrices of A_m . Moreover, among all Lipschitz functions $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ of \mathbf{X}^n , we prove that the RID of $f(\mathbf{X}^n)$ is maximized when $f(\mathbf{X}^n) = A_m \mathbf{X}^n$, where A_m is a full-rank matrix with $\text{SPARK}(A_m) = m + 1$, where SPARK quantifies the minimum number of linearly dependent columns of a matrix. Interestingly, for \mathbf{X}^n vectors with equal marginal (i.e. one-dimensional) distributions, the RID of $A_m \mathbf{X}^n$ (with A_m satisfying $\text{SPARK}(A_m) = m + 1$) is neither minimized nor maximized when X_i s are independent.

Further, we derive a lower-bound on the RDF of affinely singular random vectors, and for every distortion D . We show that the lower-bound is tight for $D \rightarrow 0$.

Finally, we derive the formulation of mutual information between two affinely singular RVs. In fact, we show that

$$I(X; Y) = b(X) + b(Y) - b(X, Y), \quad (4)$$

where $b(\cdot)$ denotes the DRB.

Notations

Lower case and Boldface lower case letters denote fixed scalars and vectors, respectively; capital and boldface letters denote random variables and vectors, respectively. Matrices are also indicated with capital letters. Sets are indicated with calligraphic capital letters. Measures are indicated with Greek letters. Logarithms are taken in base 2 by default. Other notations are as follows:

- *Random variables and distributions:* the set of RVs $\{\mathbf{X}_m, \dots, \mathbf{X}_n\}$ is abbreviated as $\{\mathbf{X}_i\}_{i=m}^n$. For brevity, we define $\{\mathbf{X}_i\} = \{\mathbf{X}_i\}_{i=-\infty}^{\infty}$. When this set of random variables is used to construct a random vector, we employ the notation $\mathbf{X}_m^n = [X_m, X_{m+1}, \dots, X_n]$ with $n \geq m$. Again, when $m = 1$, the subscript is omitted, i.e. $\mathbf{X}_1^n = \mathbf{X}^n$. By abuse of notation, for a binary vector $\mathbf{s} \in \{0, 1\}^n$, $\mathbf{X}^{\mathbf{s}}$ denotes

a random vector formed by the elements X_i of \mathbf{X}^n , where $s_i = 1$. The absolute α -moment (around zero) of the RV X is denoted by $M_X(\alpha) = \mathbb{E}[|X|^\alpha]$ for $\alpha \in \mathbb{R}$. Further, by $M_X^0(\infty)$ we mean $\text{ess sup } |X|$. Equality in distribution is indicated as $\stackrel{d}{=}$. The discrete/continuous part of the RV X is indicated as X_d/X_c , respectively. The Bernoulli RV with success probability p is indicated as $\text{Bern}(p)$, the Gaussian distribution with parameters μ and σ^2 as $\text{Gauss}(\mu, \sigma^2)$, and the Bernoulli-Gaussian distribution as $\text{Bern} - \text{Gauss}(p, \mu, \sigma^2)$.

Shannon entropy function is shown by $H(\cdot)$, the differential entropy by $h(\cdot)$, the mutual information by $I(\cdot; \cdot)$ and the Kullback-Leibler divergence by $D(\cdot \parallel \cdot)$. For the sake of simplicity in expressing our results, we might define a *null* or 0-dimensional random vector \mathbf{X} . With an abuse of notation, we assume that $h(\mathbf{X}) = 0$.

The notation δ_x refers to the Dirac's measure, where

$$\delta_x(A) = \begin{cases} 1, & x \in A \\ 0, & \text{otherwise.} \end{cases}$$

- Set theory: Set subtraction is shown as $\mathcal{A} \setminus \mathcal{B} = \mathcal{A} \cap \mathcal{B}^c$. The span of a set \mathcal{A} of vectors is denoted as $\text{span}(\mathcal{A})$. Minkowski difference of two sets \mathcal{A} and \mathcal{B} is indicated as $\mathcal{A} - \mathcal{B} = \{\mathbf{a} - \mathbf{b} : \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}\}$. For an affine set \mathcal{A} , $\dim(\mathcal{A})$ stands for its Euclidean dimension. The sets $\{i, i+1, \dots, j\} \subseteq \mathbb{N}$ and $\{1, \dots, j\}$ are abbreviated as $[i : j]$ and $[j]$, respectively. A set \mathcal{M} of linearly dependent vectors is called minimally dependent, if all proper subsets of \mathcal{M} are linearly independent. The set of all minimally dependent subsets of a set \mathcal{A} of vectors is shown as $\Omega(\mathcal{A})$.

- Vectors and matrices: Given an $m \times n$ matrix A , we denote the i -th column of A by $A^{[i]}$, for $i \in [n]$. In addition, for a binary vector $\mathbf{s} \in \{0, 1\}^n$, $A^{[\mathbf{s}]}$ denotes the sub-matrix of A formed by columns $A^{[i]}$ of A for $i \in [n]$, where $s_i = 1$. The rank, spark and the span of the matrix A are represented by $\text{rank}(A)$, $\text{SPARK}(A)$ and $\text{span}(A)$, respectively. For an arbitrary matrix A (not necessarily square), $\det^+(A)$ refers to the product of the non-zero singular values of A . The conjugate transpose of the matrix A is indicated as A^\dagger . The α -vector-norm is represented by $\|\cdot\|_\alpha$. For $\mathbf{v}^n \in \{0, 1\}^n$, $\bar{\mathbf{v}}^n$ is the vector obtained by complementing all the elements in \mathbf{v} . The n -dimensional column vector of all zeros/ones is indicated as $\mathbf{0}_n/\mathbf{1}_n$. Similarly, the $n \times m$ all zeros/ones matrix is indicated as $\mathbf{0}_{n \times m}/\mathbf{1}_{n \times m}$.

We employ the notation $I_{\text{fcr}}(A)$ as a full-rank indicator function, i.e.,

$$I_{\text{fcr}}(A) = \begin{cases} 1 & \text{rank}(A) = n \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

- Other notations: For $\alpha \in [0, 1]$, define $\bar{\alpha} = 1 - \alpha$.

The uniform quantization of the RV \mathbf{X}^n with precision m is defined as

$$[\mathbf{X}^n]_m \triangleq \left[\left\lfloor \frac{mX_1}{m} \right\rfloor, \dots, \left\lfloor \frac{mX_n}{m} \right\rfloor \right], \quad (6)$$

with $[\mathbf{X}^n]_m \in (\mathbb{N}/m)^n$ and where $\lfloor x \rfloor$ is the floor of x .

III. PRELIMINARIES

Our main contribution in this paper revolves around singular probability measures. Therefore, in this section, we first define various types of probability measures (including the singular ones). Next, we review some of the known results regarding the compressibility of a sequence of RVs and stochastic processes.

In the following, we shall follow standard definitions of absolutely continuous, discrete-continuous, singular [28, Page 121], and k -regular measures.

Definition 3 (Types of measures): Let Σ be an abstract σ -algebra of \mathbb{R}^n . The RV \mathbf{X}^n with probability measure $\mu(\cdot)$ on Σ is called

- *absolutely continuous* if for every set $\mathcal{S} \in \Sigma$ with zero Lebesgue measure, we have $\mu(\mathcal{S}) = 0$.
- *discrete*, if there exists a finite or countable subset $\mathcal{S} \subset \mathbb{R}^n$ such that $\mu(\mathbb{R}^n \setminus \mathcal{S}) = 0$,
- *singular*, if there exists a subset $\mathcal{S} \subset \mathbb{R}^n$ with zero Lebesgue measure with $\mu(\mathbb{R}^n \setminus \mathcal{S}) = 0$.

It is easy to verify that discrete measures are special cases of singular measures. The well-known Lebesgue-Radon-Nikodym theorem mathematically formalized the fact that absolutely continuous and singular measures are the building blocks of all probability measures. More precisely, the Lebesgue-Radon-Nikodym theorem states that, for every probability measure μ on \mathbb{R}^n , there exist unique singular and absolutely continuous measures μ_s, μ_a , respectively, and $p \in [0, 1]$ such that $\mu = p\mu_a + \bar{p}\mu_s$ where μ_a, μ_s are absolutely continuous, and singular probability measures, respectively.

It is common to call a measure *discrete-continuous* if the singular component in the Lebesgue-Radon-Nikodym decomposition is purely discrete, and p is neither one nor zero.

Next, we define a *Lipschitz manifold*.

Definition 4 ([29], Definition 2.3): A set $\mathcal{X} \subset \mathbb{R}^n$ is called k -dimensional Lipschitz manifold, if for every $x \in \mathcal{X}$, there exists an open set \mathcal{U} containing x and a bi-Lipschitz surjective mapping $f : \mathcal{S} \rightarrow \mathcal{U}$, where $\mathcal{S} \subseteq \mathbb{R}^k$ is a bounded.

Using the notion of k -dimensional Lipschitz manifolds, we introduce k -regular measures.

Definition 5: A measure μ on \mathbb{R}^n is called k -regular, if it is absolutely continuous with respect to a finite or countably infinite union of k -dimensional Lipschitz sub-manifolds of \mathbb{R}^n .

In Definition 5, by absolute continuity of a measure μ with respect to a union of k -dimensional manifolds \mathcal{X}_i , we mean that for any measurable set $\mathcal{A} \subseteq \mathbb{R}^n$, there exists a function $g : \mathbb{R}^n \rightarrow \mathbb{R}$, such that

$$\mu(\mathcal{A}) = \sum_i \int_{\mathcal{X}_i \cap \mathcal{A}} g(\mathbf{x}) d\text{Vol}_k(\mathbf{x}), \quad (7)$$

where Vol_k is the natural volume of the k -dimensional Lipschitz manifold. The differential volume is found based on the Jacobian matrix $J(f(\mathbf{x}))$ as

$$d\text{Vol}_k(f(\mathbf{x})) = J(f(\mathbf{x})) d\ell_k(\mathbf{x}), \quad (8)$$

in which $f(\cdot)$ is defined in Definition 4 and $\ell_k(\cdot)$ is the k -dimensional Lebesgue measure. Note that the Jacobian matrix

exists almost everywhere due to Rademacher's theorem [30, Theorem 3.1] as $f(\cdot)$ is Lipschitz.

The above measures are sometimes called *rectifiable* in the literature (e.g., see [31, Definition 4.1]). However, to avoid the confusion with other definitions of rectifiable measures (e.g., see [10, Definition 13]), here we refer to such measures as k -regular.

A. Compressibility of random vectors

The classical notion of entropy is well-defined for discrete-valued RVs. For continuous-valued RVs, this notion could be defined via the limiting entropy of the quantized RV [32].

Definition 6 ([3]): For an RV \mathbf{X}^n , the *Rényi information dimension* (RID) is defined as

$$d(\mathbf{X}^n) = \lim_{m \rightarrow \infty} \frac{H([\mathbf{X}^n]_m)}{\log m}, \quad (9)$$

if the limit exists, where $H(\cdot)$ is the Shannon entropy function.

We recall that $[\mathbf{X}^n]_m$ stands for the uniform quantization of \mathbf{X}^n .

Definition 7 ([25]): The *quadratic rate-distortion function* (QRDF) of an RV \mathbf{X}^n is defined as

$$R_2(\mathbf{X}^n, D) = \inf_{\mu_{\widehat{\mathbf{X}}^n | \mathbf{X}^n}(\cdot, \cdot): \mathbb{E} \|\mathbf{X}^n - \widehat{\mathbf{X}}^n\|_2^2 < D} I(\mathbf{X}^n; \widehat{\mathbf{X}}^n), \quad (10)$$

where $\mu_{\widehat{\mathbf{X}}^n | \mathbf{X}^n}$ is the conditional probability measure of $\widehat{\mathbf{X}}^n$ given \mathbf{X}^n .

Definition 8 ([18]): For an RV \mathbf{X}^n , the *rate distortion dimension* is given by

$$d_R(\mathbf{X}^n) = 2 \lim_{D \rightarrow 0^+} \frac{R_2(\mathbf{X}^n, D)}{-\log D}, \quad (11)$$

if the limit exists.

The next definition follows naturally from Definition 8. To the best of our knowledge, this is the first time that such a measure is defined in this generality.

Definition 9: If there exists $b(\mathbf{X}^n) \in \mathbb{R}$ satisfying

$$\lim_{D \rightarrow 0} \left| R_2(\mathbf{X}^n, D) + \frac{d_R(\mathbf{X}^n)}{2} \log \left(\frac{2\pi e D}{d_R(\mathbf{X}^n)} \right) - b(\mathbf{X}^n) \right| = 0, \quad (12)$$

for $d_R(\mathbf{X}^n) \neq 0$, or

$$\lim_{D \rightarrow 0} \left| R_2(\mathbf{X}^n, D) - b(\mathbf{X}^n) \right| = 0, \quad (13)$$

for $d_R(\mathbf{X}^n) = 0$, then, it is called the *dimensional rate bias* (DRB) of \mathbf{X}^n . In simple words, DRB is the asymptotic value of the quadratic rate-distortion function at $D \rightarrow 0$ after removing the known diverging term (when $d_R(\mathbf{X}^n) \neq 0$).

The above definitions imply that the RDD characterizes the slope of rate-distortion function with respect to $\log \frac{1}{D}$ as $D \rightarrow 0$, while the DRB quantifies the bias of that limiting line. As an instance, for a one-dimensional continuous RV, the RDD is 1 which expresses that RDF diverges similar to $\log \frac{1}{D}$ as $D \rightarrow 0$, while the DRB, which in here is equal to differential entropy, determines the bias of the RDF limiting line with respect to that of uniform distribution $\mathcal{U}_{[0,1]}$.

Note that the term $\frac{d_R(\mathbf{X}^n)}{2} \log \left(\frac{2\pi e D}{d_R(\mathbf{X}^n)} \right)$ in (12) is the differential entropy of an isotropic Gaussian RV \mathbf{n} with bounded

norm $\mathbb{E}[\|\mathbf{n}\|^2] < D$ that is supported on a d_R -dimensional space. This RV is a model for the error of approximating \mathbf{X}^n with $\widehat{\mathbf{X}}$ that appears in the formulation of QRDF in (10).

The established link between the rate distortion dimension and the information dimension is as follows:

Theorem 1 (Prop. 3.3, [18]): For every RV \mathbf{X}^n in the metric space $(\mathbb{R}^n, \|\cdot\|_2)$, we have that

$$d(\mathbf{X}^n) = d_R(\mathbf{X}^n). \quad (14)$$

Theorem 2 ([6](Corollary 1), [33](Section 2.6)): For an absolutely continuous RV \mathbf{X}^n , if $h(\mathbf{X}^n) > -\infty$ and $\mathbb{E}\|\mathbf{X}^n\|_2^\alpha < \infty$ for some $\alpha > 0$, then

$$d(\mathbf{X}^n) = n, \quad b(\mathbf{X}^n) = h(\mathbf{X}^n).$$

Further, for a discrete RV \mathbf{Y}^n , if $H(\mathbf{Y}^n) < \infty$, then

$$d(\mathbf{Y}^n) = 0, \quad b(\mathbf{Y}^n) = H(\mathbf{Y}^n).$$

B. Compressibility of stochastic processes

Next, we describe three measures of compressibility for discrete-domain stochastic processes and explain their relationships. A summary of acronyms and notations of these measures (as well as those introduced in Section III-A) is provided in Table I.

Definition 10 ([12]): For a generic stationary process $\{\mathbf{X}_n\}$, the *block-average information dimension* (BID) is defined as

$$d_B(\{\mathbf{X}_n\}) = \lim_{n \rightarrow \infty} \frac{d(\mathbf{X}^n)}{n}. \quad (15)$$

Definition 11 ([27]): For a generic stochastic process $\{\mathbf{X}_n\}$, the *information dimension rate* (IDR) is defined as

$$d_I(\{\mathbf{X}_n\}) = \lim_{m \rightarrow \infty} \lim_{n \rightarrow \infty} \frac{H([\mathbf{X}^n]_m)}{n \log m}. \quad (16)$$

One can interpret the IDR as the average number of bits needed to transmit a source normalized by the maximum average number of bits in the high-resolution regime.

Definition 12 ([18]): For a generic stochastic process $\{\mathbf{X}_n\}$, the RDD is defined as

$$d_R(\{\mathbf{X}_n\}) = 2 \lim_{D \rightarrow 0^+} \lim_{n \rightarrow \infty} \frac{R_2(\mathbf{X}^n, nD)}{-n \log D}. \quad (17)$$

The existence of the above double limit for stationary processes is proved in [34, Theorem 9.8.1].

Theorem 3 ([27, Theorem 9]): For every stochastic process $\{\mathbf{X}_t\}$ we have

$$d_R(\{\mathbf{X}_t\}) = d_I(\{\mathbf{X}_t\}), \quad (18)$$

provided that $d_R(\{\mathbf{X}_t\})$ and $d_I(\{\mathbf{X}_t\})$ exist.

Definition 13: [10] Let $\{\mathbf{X}_n\}$ be a random process. For a given $n \in \mathbb{N}$, we call (f_n, g_n) an ϵ -encode-decode pair with rate R_n , if $f_n: \mathbb{R}^n \rightarrow \mathbb{R}^{\lfloor nR_n \rfloor}$, $g_n: \mathbb{R}^{\lfloor nR_n \rfloor} \rightarrow \mathbb{R}^n$, and

$$\mathbb{P}(g_n(f_n(\mathbf{X}^n)) \neq \mathbf{X}^n) \leq \epsilon. \quad (19)$$

Given the set of all achievable rates R_n (i.e., all values of R_n such an ϵ -encode-decode pair with rate R_n exists), we call $\liminf_{n \rightarrow \infty} R_n$ the minimum ϵ -achievable rate (or in short, ϵ -compression rate). If f_n is further restricted to be linear,

Measure	Acronym	Notation
Rényi information dimension	RID	$d(\mathbf{X}^n)$
Quadratic rate-distortion function	QRDF	$R_2(\mathbf{X}^n, D)$
Rate distortion dimension	RDD	$d_R(\mathbf{X}^n)$
Dimensional rate bias	DRB	$b(\mathbf{X}^n)$
Block-average information dimension	BID	$d_B(\{\mathbf{X}_n\})$
Information dimension rate	IDR	$d_I(\{\mathbf{X}_n\})$

TABLE I
A SUMMARY OF THE COMPRESSIBILITY MEASURES IN SECTION III-A AND SECTION III-B.

we call the result of \liminf the minimum linear-encode ϵ -achievable rate and denote it by $R^*(\epsilon)$. If g_n is restricted to be Lipschitz, then, we call the result of \liminf the minimum Lipschitz-decode ϵ -achievable rate and denote it by $R(\epsilon)$.

Lemma 1: [10, Lemma 10] The minimum linear-encode ϵ -achievable rate $R^*(\epsilon)$ coincides with the $\liminf_{n \rightarrow \infty} R_n$ given that there exists a Borel set $\mathcal{S}^n \subset \mathbb{R}^n$ and a subspace $\mathcal{H}^n \subset \mathbb{R}^n$ of the dimension at least $\lceil (1 - R_n)n \rceil$ such that

$$\mathbb{P}(\mathbf{X}^n \in \mathcal{S}^n) \geq 1 - \epsilon, \quad (20)$$

and

$$(\mathcal{S}^n - \mathcal{S}^n) \cap \mathcal{H}^n = \{0\}. \quad (21)$$

IV. AFFINELY SINGULAR RANDOM VECTORS

The definition of affinely singular RV in Definition 1 provides a measure-theoretical description of this random object. As we proceed, we often find it more convenient to describe an affinely singular RV through a *constructive* approach which sees the RV as a result of an affine transformation. This approach also shows that orthogonally singular RVs, as introduced in Definition 2, form a subclass of affinely singular RVs. In addition, we show that linear transformations of orthogonally singular RVs form affinely singular RVs.

Lemma 2: For $i \in \mathbb{N}$ let $e_i \in \{1, \dots, m\}$, and define the affine function $\mathbf{f}_i(\cdot) : \mathbb{R}^{e_i} \rightarrow \mathbb{R}^m$ as

$$\mathbf{f}_i(\mathbf{x}) = U_i \left[\mathbf{x}^\top, \underbrace{0, \dots, 0}_{m-e_i} \right]^\top + \mathbf{b}_i, \quad (22)$$

where U_i is an $m \times m$ unitary matrix and $\mathbf{b}_i \in \mathbb{R}^m$ is a fixed vector. We denote the image of \mathbf{f}_i by \mathcal{K}_i and assume that \mathcal{K}_i s are distinct. For an e_i -dimensional random column vector \mathbf{C}_i with an absolutely continuous distribution, define the RV $\mathbf{Z}^{(i)}$ as

$$\mathbf{Z}^{(i)} = \mathbf{f}_i(\mathbf{C}_i). \quad (23)$$

Further, let V_m be any RV supported on \mathbb{N} , and assume it is independent of $\mathbf{Z}^{(i)}$ s. Then,

$$\mathbf{Z}^m = \mathbf{Z}^{(V_m)}, \quad (24)$$

has an affinely singular probability measure as in Definition 1 with

$$p_i = \mathbb{P}(V_m = i) \quad (25a)$$

$$\mu_i(\cdot) = \mu_{\mathbf{C}_i}(\mathbf{f}_i^{-1}(\cdot)) \quad (25b)$$

$$\mathcal{A}_i = \mathcal{K}_i, \quad (25c)$$

for all i . Conversely, every affinely singular probability measure can be constructed as in (24) with a proper choice of $(\{\mathbf{f}_i\}, \{\mathbf{C}_i\}, V_m)$ that satisfy the conditions in (25).

Proof: First, we prove that (24) has an affinely singular probability measure. By the conditioning rule, we have

$$\mu_{\mathbf{Z}^m}(\mathcal{C}) = \sum_i \mathbb{P}(V_m = i) \mu_{\mathbf{Z}^{(i)}}(\mathcal{C}), \quad (26)$$

for any set $\mathcal{C} \subseteq \mathbb{R}^m$. Since $\mathbf{Z}^{(i)}$ is only supported on \mathcal{K}_i , we can rewrite (26) as

$$\mu_{\mathbf{Z}^m}(\mathcal{C}) = \sum_i \mathbb{P}(V_m = i) \mu_{\mathbf{Z}^{(i)}}(\mathcal{C} \cap \mathcal{K}_i). \quad (27)$$

Because of the 1-1 mapping from \mathbf{C}_i to $\mathbf{Z}^{(i)}$ and absolute continuity of \mathbf{C}_i with respect to the Lebesgue measure on \mathbb{R}^{e_i} , $\mathbf{Z}^{(i)}$ is also absolutely continuous with respect to the push-forward Lebesgue measure to \mathcal{K}_i . Therefore, we conclude that (27) is in accordance with the formulation of affinely singular RVs in Definition 1, as \mathcal{K}_i s are affine sets.

Conversely, for an affinely singular RV, we provide a representation as in (24). To do so, for every affine set \mathcal{A}_i in Definition 1, we find U_i and \mathbf{b}_i such that with $\mathbf{f}_i(\mathbf{x})$ as in (22), we have $\mathcal{A}_i = \{\mathbf{f}_i(\mathbf{x}) | \mathbf{x} \in \mathbb{R}^{e_i}\}$. Note that this is always possible, since \mathcal{A}_i is an affine set. Next, we generate RVs \mathbf{C}_i with push-forward measure $\mu_i(\mathbf{f}_i^{-1}(\cdot))$, which is by definition absolutely continuous. We also define V_m as a RV with probability p_i . Finally, we recall that if $\mathbf{Z}^{(i)}$ is defined as in (23), we have

$$\mu_{\mathbf{Z}^{(V_m)}}(\mathcal{C}) = \sum_i p_i \mu_i(\mathcal{C} \cap \mathcal{A}_i). \quad (28)$$

■

The next remark shows that orthogonally singular RVs form a subclass of affinely singular RVs.

Remark 1: According to Definition 2 of orthogonally singular RVs, one can rewrite (2) in the form of (24) as

$$\mathbf{X}^n = \mathbf{X}^{(\nu, \mathbf{x}_d^{\bar{\nu}})}, \quad (29)$$

where

$$\mathbf{X}^{(\mathbf{s}, \mathbf{x}_d^{\bar{\mathbf{s}}})} := I_n^{[\mathbf{s}]} \mathbf{X}_c^{\mathbf{s}} + I_n^{[\bar{\mathbf{s}}]} \mathbf{x}_d^{\bar{\mathbf{s}}}, \quad (30)$$

$\nu = [\nu_1, \dots, \nu_n]$ for ν_i in (2), and the realizations of this RV are indicated by $\nu = \mathbf{s}$. Since \mathbf{X}_c is absolutely continuous, its marginal probability measure $\mathbf{X}_c^{\mathbf{s}}$ is also absolutely continuous. Now, by comparing (30) and (22), we conclude that orthogonally singular RVs are also affinely singular. Moreover,

\mathbf{s}	$F_3(\mathbf{s})$
$[0, 1, 1]$	1
$[1, 1, 0]$	1
$[0, 1, 0]$	2

TABLE II
THE DEFINITION OF $F_3(\cdot)$ IN EXAMPLE OF FIGURE 1

i	$\mathbb{P}(\Upsilon_3 = i)$
1	$\mathbb{P}(\boldsymbol{\nu} = [0, 1, 1]) + \mathbb{P}(\boldsymbol{\nu} = [1, 1, 0])$
2	$\mathbb{P}(\boldsymbol{\nu} = [0, 1, 0])$

TABLE III
THE PROBABILITY MASS FUNCTION OF Υ_3 IN EXAMPLE OF FIGURE 1

\mathbf{s}	$\mathbb{P}(\Upsilon_3^{(1)} = \mathbf{s})$	$\mathbb{P}(\Upsilon_3^{(2)} = \mathbf{s})$
$[0, 1, 1]$	$\frac{\mathbb{P}(\boldsymbol{\nu}=[0,1,1])}{\mathbb{P}(\boldsymbol{\nu}=[0,1,1])+\mathbb{P}(\boldsymbol{\nu}=[1,1,0])}$	0
$[1, 0, 1]$	$\frac{\mathbb{P}(\boldsymbol{\nu}=[1,1,0])}{\mathbb{P}(\boldsymbol{\nu}=[0,1,1])+\mathbb{P}(\boldsymbol{\nu}=[1,1,0])}$	0
$[0, 1, 0]$	0	1

TABLE IV
THE PROBABILITY MASS FUNCTION OF $\Upsilon_3^{(1)}$ IN EXAMPLE OF FIGURE 1

since the affine subsets are formed by the functions

$$\mathbf{f}_i(\mathbf{x}) = (I_n^{[s]}, I_n^{[\bar{s}]}) \begin{bmatrix} \mathbf{x}^\top, \underbrace{0, \dots, 0}_{|\bar{s}|} \end{bmatrix}^\top + I_n^{[\bar{s}]} \mathbf{x}_d^{\bar{s}},$$

we see that such sets are parallel to the Euclidean axes.

Next, we investigate affinely singular RVs generated by linear transformations of orthogonally singular RVs.

A. Linear Transformation of Orthogonally Singular Random Vectors

Let us consider the linear transformation $\mathbf{Y}^m = A_m \mathbf{X}^n$ where \mathbf{X}^n is an orthogonally singular RV. Following Remark 1, \mathbf{X}^n is composed of absolutely continuous measures on affine sets that are specified by pairs $(\mathbf{s}, \mathbf{x}_d^{\bar{s}})$. The linear transformation $A_m \mathbf{x}^n$ of such affine sets forms a collection $\{\mathcal{K}_i\}_i$ of distinct e_i -dimensional affine sets. Further, let $\mathcal{T}_i^{(m)}$ be the set of all pairs of $(\mathbf{s}, \mathbf{x}_d^{\bar{s}})$ that generate the same affine subset \mathcal{K}_i (it is possible that after the linear transformation, some of the singular components of \mathbf{X}^n are mapped to the same affine sets). Besides, define $F_m : \bigcup \mathcal{T}_i^{(m)} \rightarrow \mathbb{N}$ as the function that identifies the index i for each pair $(\mathbf{s}, \mathbf{x}_d^{\bar{s}})$, i.e., if $(\mathbf{s}, \mathbf{x}_d^{\bar{s}}) \in \mathcal{T}_i^{(m)}$, then $F_m((\mathbf{s}, \mathbf{x}_d^{\bar{s}})) = i$. For this indices, we define the RV Υ_m as

$$\Upsilon_m = F_m((\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}})) \quad (31)$$

which implies that the total probability measure of \mathbf{Y}^m corresponding to $\mathcal{T}_i^{(m)}$ is $\mathbb{P}(\Upsilon_m = i)$.

Moreover, for each $i \in \mathbb{N}$ we define the RV $\Upsilon_m^{(i)}$ over $\mathcal{T}_i^{(m)}$ independent of $\Upsilon_m^{(j)}$ for $j \neq i$ such that

$$\forall (\mathbf{s}, \mathbf{x}_d^{\bar{s}}) \in \mathcal{T}_i^{(m)} : \quad \mathbb{P}(\Upsilon_m^{(i)} = (\mathbf{s}, \mathbf{x}_d^{\bar{s}})) = \frac{\mathbb{P}_{\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}}}(\mathbf{s}, \mathbf{x}_d^{\bar{s}})}{\mathbb{P}(\Upsilon_m = i)}. \quad (32)$$

Finally, for each pair $(\mathbf{s}, \mathbf{x}_d^{\bar{s}}) \in \bigcup_i \mathcal{T}_i^{(m)}$, we define a continuous random vector $\mathbf{W}_{\mathbf{s}, \mathbf{x}_d^{\bar{s}}}$ by

$$\mathbf{W}_{\mathbf{s}, \mathbf{x}_d^{\bar{s}}} = \tilde{D}_s \underline{U}_s^\dagger \mathbf{X}_c^{\mathbf{s}} + \tilde{U}_s^\dagger A_m^{[s]} \mathbf{x}_d^{\bar{s}}, \quad (33)$$

where \underline{U}_s , \tilde{D}_s , and \tilde{U}_s stand for the matrices of left-singular vectors of $A_m^{[s]}$, the upper $r_s^{(m)} \times m$ part of the diagonal matrix of the singular values of $A_m^{[s]}$ with $r_s^{(m)} = \text{rank}(A_m^{[s]})$, and the $m \times r_s^{(m)}$ matrix formed by the first $r_s^{(m)}$ columns of the right-singular vectors of $A_m^{[s]}$, respectively. Note that $\tilde{U}_s^\dagger A_m^{[s]}$ is a fixed term in the definition of $\mathbf{W}_{\mathbf{s}, \mathbf{x}_d^{\bar{s}}}$ in (33). The RVs $\mathbf{W}_{\mathbf{s}, \mathbf{x}_d^{\bar{s}}}$ essentially identify the continuous part of the \mathbf{Y}^m over lower-dimensional affine subsets for each specific discrete part of \mathbf{X}^n ; we should highlight that because of the rank of $A_m^{[s]}$ submatrices, the continuous part of \mathbf{X}^n does not necessarily generate a continuous component in \mathbf{Y}^m .

We are now equipped to state the result on the linear transformation of orthogonally singular RVs.

Lemma 3: For a matrix $A_m \in \mathbb{R}^{m \times n}$ and a vector $\mathbf{s} \in \{0, 1\}^n$, let \underline{U}_s stand for the $m \times m$ matrix of left-singular vectors of $A_m^{[s]}$. We form functions $\mathbf{f}_i(\cdot)$ as

$$\mathbf{f}_i(\mathbf{x}) = \underline{U}_i \left[\mathbf{x}^\top, \underbrace{0, \dots, 0}_{m-r_i} \right]^\top + \mathbf{b}_i, \quad (34)$$

where $\underline{U}_i = \underline{U}_s$, $r_i = \text{rank}(A_m^{[s]})$, and $\mathbf{b}_i = \underline{U}_s \tilde{U}_s^\dagger A_m^{[s]} \mathbf{x}_d^{\bar{s}}$ in which \tilde{U}_s is constructed by zeroing off the first $\text{rank}(A_m^{[s]})$ of left-singular vectors of $A_m^{[s]}$ and for $(\mathbf{s}, \mathbf{x}_d^{\bar{s}}) \in \mathcal{T}_i^{(m)}$ (we show that for all pairs in $\mathcal{T}_i^{(m)}$, these values are fixed and are therefore, indexed with i). Then, \mathbf{Y}^m in (3) is affinely singular as in Lemma 2 with the triplet $(\{\mathbf{f}_i\}, \{\mathbf{Y}_i\}, \Upsilon_m)$, where \mathbf{Y}_i is defined as

$$\tilde{\mathbf{Y}}_i = \mathbf{W}_{\Upsilon_m^{(i)}}. \quad (35)$$

Proof: See Appendix A. ■

For illustration of the above definitions, we have depicted a toy example of linear transformation of an orthogonally singular RV in Figure 1. In this example, the definition of $F_3(\cdot)$, the probability mass function of Υ_3 , and the RVs $\Upsilon_3^{(1)}$ and $\Upsilon_3^{(2)}$ are specified in Tables II, III, and IV, respectively. In this example, since the discrete component of the probability measure is $\mathbf{X}_d = [0, 0, 0]$ (see Definition 2), we omit its symbol in the notation of other parameters.

V. RESULTS ON RANDOM VARIABLES

Our main contribution in this paper is the derivation of the RDF for affinely singular RVs for $D \rightarrow 0$ through evaluating DRB and RID of such RVs. Through this result we are able to address the RDF of affinely transformed orthogonally singular RVs.

We begin by deriving the RID and the DRB of affinely singular RVs and the RID of linear transformations of orthogonally singular RVs. In Section V-B, using a simple example, we show how the dependence among elements of

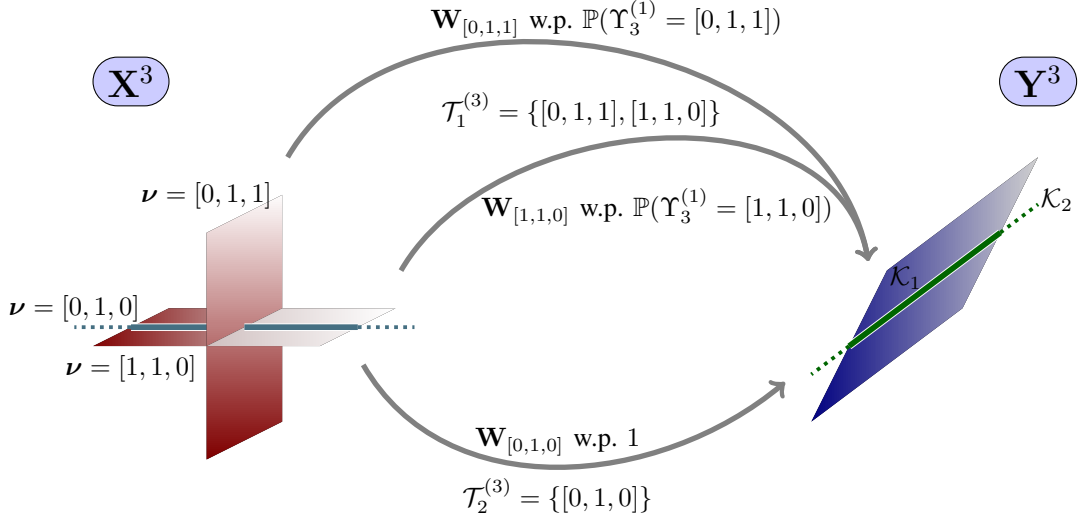


Fig. 1. A conceptual representation of a linear transformation of orthogonally singular RV into an affinely singular RV.

an orthogonally singular RV can maximize the information transfer in terms of RID, during the course of dimensionality reduction. Finally, in Section V-C we illustrate three examples of transforming orthogonally singular RVs.

A. RID and DRB of affinely singular RV

In this section, we derive an expression for the RID and DRB of the affinely singular RV \mathbf{Z}^m through its representation as in Lemma 2. As a reminder to the reader, the probability measure of \mathbf{Z}^m is formed by a union of absolutely continuous measures indexed by $i \in \mathbb{X} \subset \mathbb{N}$, where the i th measure is supported on an e_i -dimensional affine subset of \mathbb{R}^m and consists of $P(V_m = i)$ of the total probability measure.

Theorem 4: Let \mathbf{Z}^m be an affinely singular RV as per Definition 1, then, the RID of \mathbf{Z}^m is obtained as

$$d(\mathbf{Z}^m) = \mathbb{E}_{V_m} [e_{V_m}], \quad (36)$$

for V_m as in Lemma 2, provided that $H(V_m) < \infty$. Further, if $h(\mathbf{C}_i) > -\infty$ and $\mathbb{E}[\|\mathbf{Z}^m\|_\alpha^\beta] < \infty$ for some $\alpha, \beta \in \mathbb{R}^+$, then the DRB of \mathbf{Z}^m is obtained as

$$b(\mathbf{Z}^m) = \sum_{i=1}^{\infty} p_i h(\mathbf{C}_i) + H(V_m), \quad (37)$$

where $p_i = \mathbb{P}(V_m = i)$.

Proof: See Appendix B. \blacksquare

The proof of Theorem 4 heavily relies on the following lemma that is proved for a mixture of k_i -regular measures. Such measures, as stated in [31, Thm. 3.1] form the largest class of measures on which one could define probability density functions.

Lemma 4: Let μ be a probability measure on \mathbb{R}^m that can be written as a mixture of k_i -regular probability measures μ_i for $i \in \mathbb{N}$, as

$$\mu(\mathcal{A}) = \sum_i p_i \mu_i(\mathcal{A}), \quad (38)$$

for every set $\mathcal{A} \in \mathbb{R}^m$, and $p_i \in (0, 1]$, where $\sum_i -p_i \log p_i <$

∞ . Then, the RID of a random variable \mathbf{Z}^m with probability measure $\mu(\cdot)$ is given as

$$d(\mathbf{Z}^m) = \sum_i p_i k_i. \quad (39)$$

Proof: First, we show that the RID of a RV \mathbf{X}^m with k -regular measure $\tilde{\mu}(\cdot)$ is equal to k .

Based on [10, Equation 17], the RID of this \mathbf{X}^m can be obtained as

$$d(\mathbf{X}^m) = \lim_{\epsilon \rightarrow 0} \mathbb{E}_{\mathbf{x}^m \sim \mathbf{X}^m} \left[\frac{\log \tilde{\mu}(B_\epsilon(\mathbf{x}^m))}{\log \epsilon} \right], \quad (40)$$

where $B_\epsilon(\mathbf{x}^m)$ is a ball with radius ϵ around \mathbf{x}^m . Further, using [31, Theorem 1.1] and [35, 2.86], we know that if \mathbf{x}^m follows a k -regular measure $\tilde{\mu}(\cdot)$, the following limit is finite and non-zero almost surely

$$\lim_{\epsilon \rightarrow 0} \frac{\tilde{\mu}(B_\epsilon(\mathbf{x}^m))}{\epsilon^k}. \quad (41)$$

This is equivalent to the fact that

$$\lim_{\epsilon \rightarrow 0} \log \tilde{\mu}(B_\epsilon(\mathbf{x}^m)) - k \log \epsilon, \quad (42)$$

is finite almost surely, that leads to the fact that

$$\lim_{\epsilon} \frac{\log \tilde{\mu}(B_\epsilon(\mathbf{x}^m))}{\log \epsilon} = k, \quad (43)$$

almost surely. This, together with (40) shows that $d(\mathbf{X}^m) = k$.

We complete the proof by recalling [33, Theorem 5] to obtain $d(\mathbf{Z}^m) = \sum_i p_i k_i$; note that we assumed $\sum_i p_i \log \frac{1}{p_i} < \infty$. \blacksquare

So far, we have expressed the DRB as summation of the average differential entropy of absolutely continuous components of the measure and the uncertainty in the choice of affine subsets. Since V_m covers all possible choices of the discrete

components, we can express the DRB as

$$b(\mathbf{Z}^m) = \sum_{i=1}^{\infty} p_i h(\mathbf{C}_i) + H(\mathbf{Z}_D^m) \mathbb{P}(\mathbf{Z}^m \text{ is discrete}) \quad (44)$$

$$+ H(V_m | \mathbf{Z}^m \text{ is not discrete}) \mathbb{P}(\mathbf{Z}^m \text{ is not discrete}),$$

where \mathbf{Z}_D^m is the discrete component of \mathbf{Z}^m and $\mathbb{P}(\mathbf{Z}^m \text{ is not discrete})$ refers to the probability that the dimension of the corresponding set is $e_{V_m} = 0$.

The latter form is useful in studying the compressibility of discrete and continuous *mixed-pairs* as defined in [36].

Example 1: For a discrete random variable X taking values from $\mathcal{S} = \{x_1, x_2, \dots\}$ each with non-zero probability, and a continuous random variable Y supported on \mathbb{R} that have a joint probability measure $X, Y \sim \mu_{X,Y}$, the pair $\mathbf{Z} = (X, Y)$ is called a mixed-pair. We observe that the pair \mathbf{Z} has the probability measure

$$\mu_{\mathbf{Z}}(\mathcal{C}) = \sum_i \mu_i(\mathcal{C}) \cdot \mathbb{P}(X = x_i), \quad (45)$$

where $\mu_i(\cdot)$ denotes the conditional probability

$$\mu_i(\mathcal{C}) = \mathbb{P}((X, Y) \in \mathcal{C} | X = x_i). \quad (46)$$

Note that $\mu_i(\cdot)$ is absolutely continuous on the 1-dimensional affine set $\mathcal{A}'_i = \{x_i\} \times \mathbb{R}$; otherwise, if for some $x = x_i$ and a zero-Lebesgue measure $S \in \mathbb{R}$, we have $\mu_i(\{x_i\} \times S) > 0$, then, which implies that $\mu_Y(S) = \sum_i \mathbb{P}(X = x_i) \mu_i(\{x_i\} \times S) > 0$ that contradicts the absolute continuity of Y . As a result, \mathbf{Z} is affinely singular and using Lemma 2 it is described by the triplet $(\{f_i\}, \{C_i\}, V_m)$ where C_i is a RV with probability measure $\mu_{C_i} = \mu_{Y|X=x_i}$, $f_i(y) = (x_i, y)$, and $\mathbb{P}(V_m = i) = \mathbb{P}(X = x_i)$. Hence, using Theorem 4, we have

$$d(\mathbf{Z}) = \mathbb{E}_X[1] = 1,$$

$$b(\mathbf{Z}) = \sum_i \mathbb{P}(X = x_i) h(Y|X = x_i) + H(X) = \mathbb{H}(\mathbf{Z}),$$

where $\mathbb{H}(\mathbf{Z})$ is the *entropy of the mixed-pair* defined in [36].

This example reveals that the DRB coincides with the notion of entropy of mixed-pairs in this specific setting. In Section VI, we further show that $b(\mathbf{Z})$ for an affinely singular RV \mathbf{Z} coincides with the generalized entropy of its probability measure with respect to the mixture of Lebesgue measures on affine subsets.

Next, we evaluate the RID and DRB of linearly transformed orthogonally singular RVs.

Theorem 5: Let \mathbf{X}^n be an orthogonally singular RV as in Definition 2 such that $H(\boldsymbol{\nu}, \mathbf{X}_d) < \infty$. Then, the RID of $\mathbf{Y}^m = A_m \mathbf{X}^n$ satisfies

$$d(\mathbf{Y}^m) = \mathbb{E}_{\boldsymbol{\nu}}[\text{rank}(A_m^{[\boldsymbol{\nu}]})]. \quad (47)$$

Further, if $h(\mathbf{X}_c) > -\infty$ and $\mathbb{E}[\|\mathbf{X}_c\|_{\alpha}^{\beta}], \mathbb{E}[\|\mathbf{X}_d\|_{\alpha}^{\beta}] < \infty$ for some $\alpha, \beta \in \mathbb{R}^+$, then, the DRB of \mathbf{Y}^m is obtained as

$$b(\mathbf{Y}^m) = H(\Upsilon_m) + \sum_{i=1}^{\infty} p_i h(\tilde{\mathbf{Y}}_i), \quad (48)$$

where Υ_m is the discrete RV introduced in (31), and $\{\tilde{\mathbf{Y}}_i\}$ is

the set of absolutely continuous RVs mentioned in (35).

Proof: See Appendix C. \blacksquare

As a special case, Theorem 5 implies that if \mathbf{X}^n is absolutely continuous (i.e. $\alpha_i = 1$ for all i), then, $d(\mathbf{Y}^m) = \text{rank}(A_m)$. Further, in this case (48) reduces to

$$b(\mathbf{Y}^m) = \log \det^+(A_m) + h(\tilde{\mathbf{U}}^{\dagger} \mathbf{X}^n), \quad (49)$$

where $\tilde{\mathbf{U}}$ is composed of the first $r = \text{rank}(A_m)$ right singular vectors of A_m .

Another special case is when A_m is of full column-rank, i.e. $\text{rank}(A_m) = n$. In this case, $\text{rank}(A_m^{[s]}) = \sum_{i=1}^n s_i$, and the expectation in (47) simplifies to $d(\mathbf{Y}^m) = \sum_{i=1}^n \alpha_i$. This result is in agreement with a similar result for bi-Lipschitz transformations in [33, Theorem 2]. One can verify that in this case, $F_m(\cdot)$ is a one-to-one mapping. This fact, together with (31), (35), and (48) implies that

$$b(\mathbf{Y}^m) = H(\boldsymbol{\nu}, \mathbf{X}_d^{\boldsymbol{\nu}}) + m \psi_{m, \boldsymbol{\nu}}(A)$$

$$+ \sum_{\mathbf{s} \in \{0,1\}^n} \mathbb{P}(\boldsymbol{\nu} = \mathbf{s}) h(\mathbf{X}_c^{\mathbf{s}}), \quad (50)$$

where $h(\mathbf{X}_c^{\boldsymbol{\nu}})$ is the differential entropy of $\mathbf{X}_c^{\boldsymbol{\nu}}$, the sub-vector of \mathbf{X}_c associated with non-zero elements in $\boldsymbol{\nu}$, and $\psi_{m, \boldsymbol{\nu}}(A)$ is defined as

$$\psi_{m, \boldsymbol{\nu}}(A_m) := \frac{1}{m} \mathbb{E}_{\boldsymbol{\nu}} \left[\log \det^+(A_m^{[\boldsymbol{\nu}]}) \right]. \quad (51)$$

The subscript $\boldsymbol{\nu}$ in $\psi_{m, \boldsymbol{\nu}}(A_m)$ is to highlight that this value is a function of the probability distribution of $\boldsymbol{\nu}$ (but not its random value).

In the special case that \mathbf{Y}^m contains independent discrete-continuous elements (i.e., $m = n$, $A_m = I_n$ and \mathbf{X}^n is element-wise independent), formulation of RID and DRB in Theorem 5 reduces to

$$d(\mathbf{Y}^m) = \sum_{i=1}^m \mathbb{P}(\nu_i = 1), \quad (52)$$

and

$$b(\mathbf{Y}^m) = \sum_{i=1}^m H(\nu_i) + \mathbb{P}(\nu_i = 0) H(X_{d,i}) + \mathbb{P}(\nu_i = 1) h(X_{c,i}). \quad (53)$$

The latter identity is an extension of [21, Theorem 1] to RVs with bounded moment (instead of bounded variance).

Remark 2: A closer look at (47) reveals that $d(\mathbf{Y}^m)$, besides A_m , also depends on $\{\alpha_i = \mathbb{P}(\nu_i = 1)\}$. In other words, the choice of the continuous and discrete distributions of the elements of \mathbf{X}^n does not affect the RID: this quantity only depends on how much weight is assigned to the continuous components. Additionally, $d(\mathbf{Y}^m)$ is an increasing function of each α_i .

For fixed \mathbf{X}^n , the maximum value of $d(\mathbf{Y}^m)$ is achieved when

$$\text{rank}(A_m^{[s]}) = \min \left\{ m, \sum_{i=1}^n s_i \right\}, \quad \forall \mathbf{s} \in \{0,1\}^n. \quad (54)$$

Using the compressed-sensing terminology, the above condi-

tion is equivalent to $\text{SPARK}(A_m) = m + 1$. One can prove two directions for such equivalence as follows: (i) first, if we assume $\text{SPARK}(A_m) = m + 1$, it means that every d columns for $d \leq m$ are linearly independent. Hence, if $\sum_{i=1}^n s_i \leq m$, then, $\text{rank}(A_m^{[s]}) = \sum_{i=1}^n s_i = \min\{m, \sum_{i=1}^n s_i\}$. Further, (ii) if $\sum_{i=1}^n s_i \geq m$, then, there is at least m columns in $A_m^{[s]}$ which based on our assumption are linearly independent. As a result, $\text{rank}(A_m^{[s]}) \geq m$. Moreover, since the number of rows in $A_m^{[s]}$ is m , then we have $\text{rank}(A_m^{[s]}) \leq m$ which proves that $\text{rank}(A_m^{[s]}) = m = \min\{m, \sum_{i=1}^n s_i\}$. On the other hand, if $\text{rank}(A_m^{[s]}) = \min\{m, \sum_{i=1}^n s_i\}$, it means that if $\sum_{i=1}^n s_i \leq m$, then $\text{rank}(A_m^{[s]})$ is equal to its number of columns, which shows that the columns are linearly independent. As a result, $\text{SPARK}(A_m^{[s]}) \geq m + 1$ and using the property $\text{SPARK}(A_m^{[s]}) \leq m + 1$, one shows that $\text{SPARK}(A_m^{[s]}) = m + 1$.

The Vandermonde matrices are among the examples that satisfy the condition (54). Therefore, Vandermonde matrices can be considered among the transformations that maximally preserve the information measured by the RID.

As a special case of the above, the output RID of such linear transformations for independent discrete-continuous RVs is plotted in Figure 2.

This maximal behavior is even valid among Lipschitz functions, as shown by the next lemma.

Lemma 5: Let \mathbf{X}^n be an orthogonally singular RV as in Definition 2 with $H(X_{d,i}) < \infty$, $i \in [n]$, and A_m is an $m \times n$ matrix that satisfies $\text{SPARK}(A_m) = m + 1$. Then, for any Lipschitz function $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ we have that

$$\bar{d}(f(\mathbf{X}^n)) \leq d(A_m \mathbf{X}^n), \quad (55)$$

where $\bar{d}(f(\mathbf{X}^n))$ denotes the upper RID of $f(\mathbf{X}^n)$ (the RID itself might not exist for functions of \mathbf{X}^n).

Proof: See Appendix D. ■

As another application of Theorem 5, below we study the effect of a random matrix on the information dimension.

Proposition 1: Let the elements of the matrix $A = [a_{ij}]_{i,j=1}^{m,n}$ be distributed as $a_{ij} \sim f_a(a)$, where $f_a(\cdot)$ is a valid density function. For an n -dimensional truncation \mathbf{X}^n of an orthogonally singular random process with $\mathbb{P}(\nu_i = 1) = p$, and $m = \lceil rn \rceil$ where r is a fixed sampling rate, we have $\lim_{n \rightarrow \infty, m = \lceil rn \rceil} \frac{1}{m} d(A\mathbf{X}^n) = \min\{1, \frac{p}{r}\}$.

Proof: See Appendix E. ■

Sketch of proof: Since the set of roots of the determinant polynomial has zero Lebesgue measure, every sub-matrix of A is of full-rank with probability 1. Using (54), this results in $\frac{1}{m} d(A\mathbf{X}^n) = \mathbb{E}[\min\{1, \frac{\sum \nu_i}{m}\}]$. Finally, we make use of the concentration of $\frac{\sum \nu_i}{n}$ around $\frac{p}{r}$ to complete the proof. ■

B. A study of RID in RVs with dependent components

In this part, we present a simple example to examine the RID of a function of an orthogonally singular RV; in particular, we study the effect of dependence among the elements of an RV. If \mathbf{X}^n is an orthogonally singular RV, we know from Lemma 5 that among all Lipschitz functions of \mathbf{X}^n , linear matrix operators A_m with $\text{SPARK}(A_m) = m + 1$ maximize

TABLE V
JOINT PROBABILITY OF TWO SELECTION VARIABLES ν_1, ν_2 FOR THE EXAMPLE IN SECTION V-B.

$\nu_1 \backslash \nu_2$	0	1	$\nu_1 \backslash \nu_2$	0	1
0	0.18	0.12	0	0	0.3
1	0.42	0.28	1	0.6	0.1

$\nu_1 \backslash \nu_2$	0	1
0	0.3	0
1	0.3	0.4

the RID. However, the RID of $A_m \mathbf{X}^n$ is not the same if the elements of \mathbf{X}^n are dependent or independent. As we show here, the independent case corresponds to neither the maximum RID case nor the minimum RID case.

We consider a 2D RV with three dependency cases for ν_1 and ν_2 (defined in (2)) as shown in Table V:

- 1) the Q distribution corresponds to the case of independent ν_1 and ν_2 (equivalently, X_1 and X_2),
- 2) the Q' distribution in which X_1 and X_2 cannot take discrete values at the same time,
- 3) and the Q'' distribution in which a discrete value of X_1 never coincides with a continuous value of X_2 .

We need to highlight that the marginal distribution of ν_i s are the same in all the three cases. Next, we evaluate the RID of $Y = [1, 2] \cdot \mathbf{X}^2$ (a linear transformation onto the one-dimensional space) for these cases. Obviously, $A_1 = [1, 2]$ is a Vandermonde matrix.

We first recall that the sum of a continuous RV and another (arbitrary) RV is always a continuous RV [13, Lemma 11]; hence, the discrete component in the distribution of Y is a result of both X_1 and X_2 taking discrete values. Furthermore, as Y is a scalar, the RID of Y equals to the total probability of the continuous component; i.e., 0.82, 1, and 0.7 for Q , Q' , and Q'' , respectively.

Since A_1 is a Vandermonde matrix, Lemma 5 guarantees that Y has the maximum possible RID among all Lipschitz functions $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ on \mathbf{X}^2 . Nevertheless, as the distribution of \mathbf{X}^2 changes, the RID of Y also changes. Surprisingly, the above example reveals that the RID of Y for the element-wise independent \mathbf{X}^2 and A_1 being a Vandermonde matrix does not necessarily provide a universal upper-bound.

For Lipschitz functions of a general RV (not necessarily orthogonally singular), the upper-bound

$$d(f(\mathbf{X}^n)) \leq \min\{d(\mathbf{X}^n), m\}. \quad (56)$$

is proved in [33, Theorem 2] and [3, Eq. (80)]. To compare this bound with our result in Theorem 5, we consider an input \mathbf{X}^n with i.i.d. elements that is mapped into \mathbf{Y}^2 (i.e., $m = 2$) using a Vandermonde matrix. Figure 3 depicts the upper-bound on the RID using both the general bound in (56) and our bound of the RID that is calculated in Theorem 5 by setting $\text{rank}(A_m^{[s]}) = \min\{m, \sum_{i=1}^n s_i\}$. This figure indicates that our result provides a tighter bound by restricting the input type.

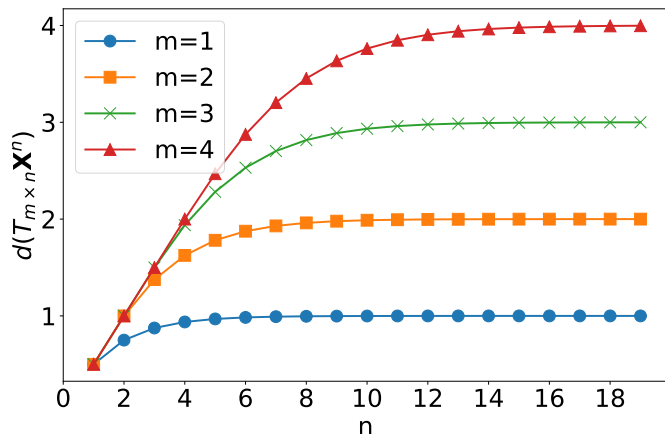
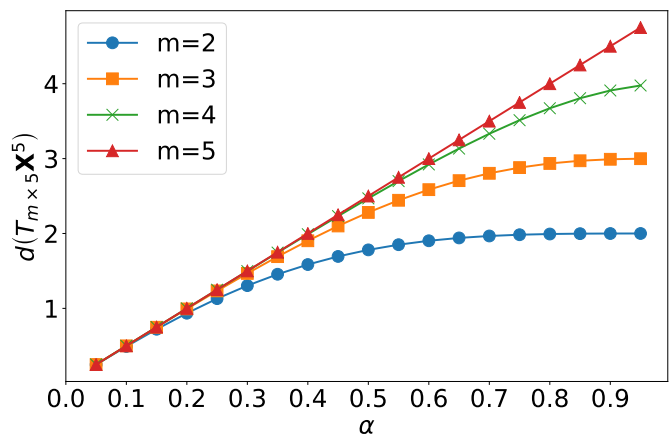
(a) $d(T_{m \times n} \mathbf{X}^n)$ vs. input dimension(b) $d(T_{m \times 5} \mathbf{X}^5)$ vs. input RID

Fig. 2. (a) The RID of $T_{m \times n} \mathbf{X}^n$ where $\text{SPARK}(T) = m + 1$, and $d(X_i) = 1/2$. One can see that for $n \leq m$ the curve is equal to $Y = n/2$ (linear) because $T_{m \times n}$ is full column rank and preserves the RID. Moreover, for large n 's the RID saturates to m . (b) Information dimension of $T_{m \times 5} \mathbf{X}^5$ for various values of $d(X_i) = \alpha$, where T is a Vandermonde matrix and the elements of \mathbf{X}^5 are independent discrete-continuous RVs. As one could conclude from Theorem 5, for $m > 5$, $d(T_{m \times 5} \mathbf{X}^5)$ has the same value as that of $m = 5$.

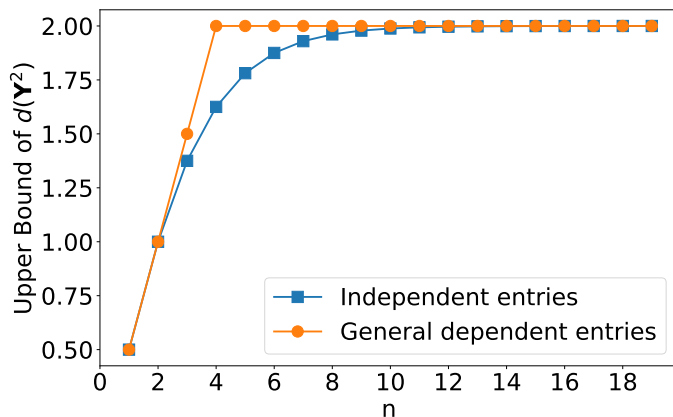


Fig. 3. Upper bounds of a two-dimensional Lipschitz function of element-wise dependent and independent discrete-continuous identically distributed RVs. Here, we portray the case in which $d(X_1) = 0.5$.

C. An illustrative example

As mentioned earlier, our goal in this paper is to derive the RID and DRB for linearly transformed random vectors in which entries have independent discrete-continuous distributions. To better clarify the problem formulation and our contributions, let us present in this section a rather simple but illustrative example. This example is illustrated in Fig. V-C.

Fig. 4(a) – Orthogonally singular RV: Let \mathbf{X}^3 be a three-dimensional random vector in which each entry has an independent Bernoulli-Gaussian distribution, that is

$$\mu_i^{\text{BG}}(\sigma_i, \alpha) = \alpha \mu_{\text{Gauss}}(0, \sigma_i^2) + \bar{\alpha} \delta_0, \quad (57)$$

for $i \in [3]$, with $\alpha = 1/2$, $\boldsymbol{\sigma} = [0.2, 0.4, 0.8]^T$ and where δ_x indicates the Dirac's measure distributed around x , and μ_{Gauss} is the Gaussian (normal) measure. Since each coordinate has a mass probability (of $\bar{\alpha} = 1/2$) at zero, the three-dimensional product measure has a mass probability in the origin. The singularity in zero in each dimension also yield one-dimensional singularities along the axes and two-

dimensional singularities on principal planes (i.e., $x - y$, $y - z$ and $x - z$ planes). Because of the structure of the singularities, we call \mathbf{X}^3 an *orthogonally singular RV*. As the singular parts of \mathbf{X}^3 belong to orthogonal planes, it is straightforward to check that $d(\mathbf{X}^3) = d(X_1) + d(X_2) + d(X_3) = 3/2$.

Fig. 4(b) – Affinely singular RV: Next, let us consider the RV \mathbf{Y}^3 obtained as the linear transformation $A \mathbf{X}^3$ for A full-rank. The full-rank linear transformation causes three-dimensional rotation on the singularity patterns. Therefore, it is no longer possible to decompose the singularities and derive the RID according to one-dimensional distributions. Our result – see Theorem 5 – characterizes the RID of this class of vectors, which we term *affinely singular RVs*. This theorem, asserting previous results on the RID of bi-Lipschitz functions of a RV, shows that for every invertible matrix A , we have $d(\mathbf{Y}^3) = 3/2$.

Fig. 4(c) – Degraded affinely singular RV: The case of most interest is the case of rank-deficient transformations. Let us consider the case in which $\tilde{\mathbf{Y}}^3 = \tilde{A} \mathbf{X}^3$, where

$$\tilde{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & -1 \end{bmatrix}. \quad (58)$$

Since $\text{rank}(\tilde{A}) = 2$, $\tilde{\mathbf{Y}}^3$ has a two-dimensional structure; i.e., the distribution of $\tilde{\mathbf{Y}}^3$ as a 3-dimensional vector is purely singular. See Figure 4(c). Besides, it consists of one dimensional singularities as well as a point mass. Quite interestingly, our results in this paper are general enough to even include this case – see Theorem 5. In particular, for the transformation in (58), we have that $d(\tilde{\mathbf{Y}}^3) = 11/8$.

VI. RESULTS ON MUTUAL INFORMATION

In this section, we apply the notion of DRB to evaluate the mutual information between two affinely singular random vectors. We first study the Kullback-Leibler (KL) divergence of two affinely singular random vectors \mathbf{X} and \mathbf{Y} , since their mutual information could be stated as the KL-divergence

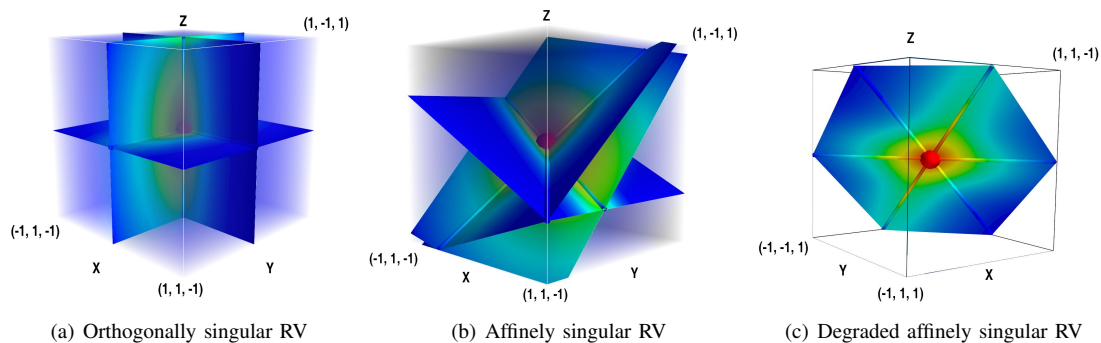


Fig. 4. A representation of orthogonally, affinely and degraded affinely singular random vectors (RVs).

divergence between the joint probability measure $\mu_{\mathbf{X}, \mathbf{Y}}(\cdot)$ and the product measure $\mu_{\mathbf{X}} \times \mu_{\mathbf{Y}}(\cdot)$.

Next, we show that if \mathbf{X} and \mathbf{Y} are affinely singular, such product and joint probability measures, in case of existence of the mutual information, must also be affinely singular. Employing these results, we show that

$$I(\mathbf{X}; \mathbf{Y}) = b(\mathbf{X}) + b(\mathbf{Y}) - b(\mathbf{X}, \mathbf{Y}). \quad (59)$$

Indeed, this is an extension of the classical results when \mathbf{X} and \mathbf{Y} are either both discrete or both continuous, where $b(\mathbf{X}) = H(\mathbf{X})$, $b(\mathbf{Y}) = H(\mathbf{Y})$ and $b(\mathbf{X}, \mathbf{Y}) = h(\mathbf{X}, \mathbf{Y})$, respectively.

We start by the following lemma that states absolutely continuous probability measures with respect to an affinely singular probability measure are affinely singular themselves with the same singularity subsets.

Lemma 6: Let $\mu_{\mathbf{X}}(\cdot)$ be an affinely singular probability measure according to Definition 1 on a collection of affine subsets $\mathcal{S}_{\mathbf{X}}$, and with measures $\mu_{\mathcal{A}}^{\mathbf{X}}(\cdot)$ on each set $\mathcal{A} \in \mathcal{S}_{\mathbf{X}}$. Then, $\mu_{\mathbf{Y}}(\cdot)$ is absolutely continuous with respect to $\mu_{\mathbf{X}}(\cdot)$, if and only if $\mu_{\mathbf{Y}}(\cdot)$ is affinely singular on a collection of affine subsets $\mathcal{S}_{\mathbf{Y}} \subseteq \mathcal{S}_{\mathbf{X}}$ and $\mu_{\mathcal{A}}^{\mathbf{Y}}(\cdot)$ is absolutely continuous with respect to $\mu_{\mathcal{A}}^{\mathbf{X}}(\cdot)$ for every $\mathcal{A} \in \mathcal{S}_{\mathbf{X}}$.

Proof: See Appendix F. ■

Using Radon-Nikodym theorem and the above lemma, we can evaluate the KL-divergence for a pair of affinely singular RVs.

Lemma 7: Let $\mu_{\mathbf{X}}(\cdot)$ and $\mu_{\mathbf{Y}}(\cdot)$ be two affinely singular probability measures according to Definition 1 on affine subsets $\mathcal{S}_{\mathbf{X}}$ and $\mathcal{S}_{\mathbf{Y}}$ with total probability $p_{\mathcal{A}}^{\mathbf{X}}$, $p_{\mathcal{B}}^{\mathbf{Y}}$ on each affine set $\mathcal{A} \in \mathcal{S}_{\mathbf{X}}$ and $\mathcal{B} \in \mathcal{S}_{\mathbf{Y}}$, and with measures $\mu_{\mathcal{A}}^{\mathbf{X}}(\cdot)$ and $\mu_{\mathcal{B}}^{\mathbf{Y}}(\cdot)$ on such sets, respectively. The KL-divergence $D(\mu_{\mathbf{X}} \parallel \mu_{\mathbf{Y}})$ is defined if and only if $\mathcal{S}_{\mathbf{X}} \subseteq \mathcal{S}_{\mathbf{Y}}$ and for every $\mathcal{A} \in \mathcal{S}_{\mathbf{X}}$, the measure $\mu_{\mathcal{A}}^{\mathbf{X}}$ is absolutely continuous with respect to the measure $\mu_{\mathcal{A}}^{\mathbf{Y}}$. In that case, we can evaluate the KL-divergence as

$$D(\mu_{\mathbf{X}} \parallel \mu_{\mathbf{Y}}) = \sum_{\mathcal{A} \in \mathcal{S}_{\mathbf{X}}} p_{\mathcal{A}}^{\mathbf{X}} D(\mu_{\mathcal{A}}^{\mathbf{X}} \parallel \mu_{\mathcal{A}}^{\mathbf{Y}}) + D(p_{\mathbf{X}} \parallel p_{\mathbf{Y}}), \quad (60)$$

where $D(p_{\mathbf{X}} \parallel p_{\mathbf{Y}}) := \sum_{\mathcal{A} \in \mathcal{S}_{\mathbf{X}}} p_{\mathcal{A}}^{\mathbf{X}} \log \frac{p_{\mathcal{A}}^{\mathbf{X}}}{p_{\mathcal{A}}^{\mathbf{Y}}}$.

Proof: See Appendix G. ■

Remark 3: One can check that the proof of Lemma 7 is not restricted to the case that $\mu_{\mathbf{Y}}$ is a probability measure. Using

Lemma 2, we know that there exists a triplet $(\{\mathbf{f}_i\}, \{\mathbf{C}_i\}, V_m)$, such that

$$\mu_{\mathbf{X}}(\mathcal{C}) = \sum_i \mathbb{P}(V_m = i) \mu_{\mathbf{C}_i}(\mathbf{f}_i^{-1}(\mathcal{C} \cap \mathcal{A}_i)). \quad (61)$$

Then, we can define $\mu_{\mathbf{Y}}(\cdot)$ as

$$\mu_{\mathbf{Y}}(\mathcal{C}) = \sum_i \ell_{e_i}(\mathbf{f}_i^{-1}(\mathcal{C} \cap \mathcal{A}_i)), \quad (62)$$

where e_i is the dimension of \mathbf{C}_i , and ℓ_{e_i} is the Lebesgue measure on \mathbb{R}^{e_i} . In that case, since $\mu_{\mathbf{Y}}(\cdot)$ is σ -finite, with the same line of proof as above, the generalized entropy of $\mu_{\mathbf{X}}$ with respect to $\mu_{\mathbf{Y}}$ can be obtained as

$$\begin{aligned} H_{\mu_{\mathbf{Y}}}(\mu_{\mathbf{X}}) & \\ & := - \int d\mu_{\mathbf{X}} \log \frac{d\mu_{\mathbf{X}}}{d\mu_{\mathbf{Y}}} \\ & = - \sum_i \mathbb{P}(V_m = i) \int_{\mathcal{A}_i} \frac{d\mathbf{f}_i^*(\mu_{\mathbf{C}_i})}{d\mathbf{f}_i^*(\ell_{e_i})} \log \frac{d\mathbf{f}_i^*(\mu_{\mathbf{C}_i})}{d\mathbf{f}_i^*(\ell_{e_i})} d\mathbf{f}_i^*(\ell_{e_i}) \\ & \quad - \sum_i \mathbb{P}(V_m = i) \log \mathbb{P}(V_m = i), \end{aligned} \quad (63)$$

where $\mathbf{f}_i^*(\mu)$ for a measure μ denotes the push-forward measure $\mu(\mathbf{f}_i^{-1}(\cdot))$.

With a change of variables, it is possible to rewrite (64) as

$$\begin{aligned} H_{\mu_{\mathbf{Y}}}(\mu_{\mathbf{X}}) & \\ & = - \sum_i \mathbb{P}(V_m = i) \int_{\mathbb{R}^{e_i}} \frac{d\mu_{\mathbf{C}_i}}{d\ell_{e_i}} \log \frac{d\mu_{\mathbf{C}_i}}{d\ell_{e_i}} d\ell_{e_i} + H(V_m) \\ & = \sum_i \mathbb{P}(V_m = i) h(\mathbf{C}_i) + H(V_m) \stackrel{(a)}{=} b(\mathbf{X}), \end{aligned} \quad (65)$$

in which (a) holds because of Theorem 4. This expresses the DRB of an affinely singular RV in terms of the generalized entropy of the probability measure with respect to a mixture of Lebesgue measures.

We now state the main result of this section which connects the notion of DRB to mutual information between two affinely singular RVs.

Theorem 6: Let $\mu_{\mathbf{X}}(\cdot)$ and $\mu_{\mathbf{Y}}(\cdot)$ be probability measures of two affinely singular RVs as in Lemma 7. The mutual information $I(\mathbf{X}; \mathbf{Y})$ exists only if the joint probability measure $\mu_{\mathbf{X}, \mathbf{Y}}(\cdot)$ is affinely singular on the collection of affine sets $\mathcal{S}_{\mathbf{X}} \otimes \mathcal{S}_{\mathbf{Y}} := \{\mathcal{A} \times \mathcal{B} : \mathcal{A} \in \mathcal{S}_{\mathbf{X}}, \mathcal{B} \in \mathcal{S}_{\mathbf{Y}}\}$. In this case, $I(\mathbf{X}; \mathbf{Y})$ can be calculated as (59).

Proof: Assume \mathbf{X} and \mathbf{Y} are m and n -dimensional RVs, respectively. Lemma 2 implies the existence of the triplets $(\{\mathbf{f}_i\}, \{\mathbf{C}_i\}, U_m)$ and $(\{\mathbf{g}_i\}, \{\mathbf{D}_i\}, V_n)$, such that

$$\mu_{\mathbf{X}}(\mathcal{C}) = \sum_i \mathbb{P}(U_m = i) \mu_{\mathbf{C}_i}(\mathbf{f}_i^{-1}(\mathcal{C} \cap \mathcal{K}_i)), \quad (66)$$

and

$$\mu_{\mathbf{Y}}(\mathcal{D}) = \sum \mathbb{P}(V_n = i) \mu_{\mathbf{D}_i}(\mathbf{g}_i^{-1}(\mathcal{D} \cap \mathcal{L}_i)), \quad (67)$$

for $\mathcal{C} \subseteq \mathbb{R}^m$ and $\mathcal{D} \subseteq \mathbb{R}^n$, where \mathcal{K}_i and \mathcal{L}_i are the images of $\mathbf{f}_i(\cdot)$ and $\mathbf{g}_i(\cdot)$, respectively, and where \mathbf{C}_i s and \mathbf{D}_i s are e_i - and e'_i -dimensional, respectively.

We construct the product measure

$$\mu_{\mathbf{X}} \times \mu_{\mathbf{Y}}(\mathcal{E}) = \int_{\mathbf{y} \in \mathbb{R}^n} \mu_{\mathbf{X}}(\mathcal{E}^{\mathbf{y}}) d\mu_{\mathbf{Y}}(\mathbf{y}), \quad (68)$$

where $\mathcal{E}^{\mathbf{y}} = \{(\mathbf{x}', \mathbf{y}') \in \mathcal{E} : \mathbf{y}' = \mathbf{y}\}$. Using Fubini's theorem and (66)-(68), we conclude that

$$\begin{aligned} \mu_{\mathbf{X}} \times \mu_{\mathbf{Y}}(\mathcal{E}) &= \sum_{i,j} p_{ij} \int_{\mathbf{y} \in \mathcal{L}_i} \mathbf{f}_i^*(\mu_{\mathbf{C}_i})(\mathcal{E}^{\mathbf{y}} \cap \mathcal{K}_i) d\mathbf{g}_i^*(\mu_{\mathbf{D}_i})(\mathbf{y}), \quad (69) \end{aligned}$$

where $\mathbf{f}_i^*(\mu_{\mathbf{C}_i})(\cdot)$ denotes the push-forward measure $\mu(\mathbf{f}_i^{-1}(\cdot))$, and p_{ij} indicates the product mass probability $p_{ij} = \mathbb{P}(U_m = i)\mathbb{P}(V_n = j)$. Hence, by the definition of the product measure, we have

$$\mu_{\mathbf{X}} \times \mu_{\mathbf{Y}}(\mathcal{E}) = \sum_{i,j} p_{ij} \mathbf{f}_i^*(\mu_{\mathbf{C}_i}) \times \mathbf{g}_i^*(\mu_{\mathbf{D}_j})(\mathcal{E} \cap \mathcal{K}_i \times \mathcal{L}_j). \quad (70)$$

Since the product of absolutely continuous measures is also absolutely continuous, $\mu_{\mathbf{X}} \times \mu_{\mathbf{Y}}$ is an affinely singular probability measure on the collection of affine sets $\mathcal{S}_{\mathbf{X}} \otimes \mathcal{S}_{\mathbf{Y}}$, as $\mathbf{f}_i^*(\mu_{\mathbf{C}_i})$ and $\mathbf{g}_j^*(\mu_{\mathbf{D}_j})$ are absolutely continuous on \mathcal{K}_i and \mathcal{L}_j . One can also see that $\mu_{\mathbf{X}} \times \mu_{\mathbf{Y}}$ is absolutely continuous with respect to the mixture measure

$$\ell_{\mathcal{C}} = \sum_{i,j} \ell_{e_i+e'_j}(h_{ij}^{-1}(\mathcal{C} \cap \mathcal{K}_i \times \mathcal{L}_j)), \quad (71)$$

where $h_{ij}([\mathbf{x}_1, \mathbf{x}_2]) = [\mathbf{f}_i(\mathbf{x}_1), \mathbf{g}_j(\mathbf{x}_2)]$, and e_i is the dimension of the domain of $h_{ij}(\cdot)$, and $\ell_{e_i+e'_j}(\cdot)$ is the Lebesgue measure on $\mathbb{R}^{e_i+e'_j}$. Since $\mathbf{f}_i(\cdot)$ and $\mathbf{g}_j(\cdot)$ are linear functions with images \mathcal{K}_i and \mathcal{L}_j , the inverse of the function $h_{ij}(\cdot)$ always exists.

Now, we recall the well-known identity

$$I(\mathbf{X}; \mathbf{Y}) = D(\mu_{\mathbf{X}, \mathbf{Y}} \| \mu_{\mathbf{X}} \times \mu_{\mathbf{Y}}).$$

With the help of Lemma 7, we conclude that $I(\mathbf{X}; \mathbf{Y})$ exists only if $\mu_{\mathbf{X}, \mathbf{Y}}$ is affinely singular on the collection of affine sets $\mathcal{S}_{\mathbf{X}} \otimes \mathcal{S}_{\mathbf{Y}}$. Hence, we can define $\mu_{\mathbf{X}, \mathbf{Y}}$ as

$$\mu_{\mathbf{X}, \mathbf{Y}}(\mathcal{E}) = \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} h_{ij}^*(\mu_{\mathbf{E}_{ij}})(\mathcal{E} \cap \mathcal{K}_i \times \mathcal{L}_j), \quad (72)$$

for $\mathcal{E} \subseteq \mathbb{R}^{m+n}$, where \mathbf{E}_{ij} is an absolutely continuous RV on $\mathbb{R}^{e_{ij}}$, in which e_{ij} is the dimension of the domain of $h_{ij}(\cdot)$. Further, since $\mu_{\mathbf{X}, \mathbf{Y}}(\mathcal{C} \times \mathbb{R}^n) = \mu_{\mathbf{X}}(\mathcal{C})$ for every $\mathcal{C} \subseteq \mathbb{R}^m$,

(66), implies that

$$\sum_j p_{i,j}^{\mathbf{X}, \mathbf{Y}} \mu_{\mathbf{E}_{ij}}(\mathcal{C} \times \mathbb{R}^n) = \mathbb{P}(U_m = i) \mu_{\mathbf{C}_i}(\mathcal{C}), \quad (73)$$

which yields

$$\sum_j p_{i,j}^{\mathbf{X}, \mathbf{Y}} = \mathbb{P}(U_m = i). \quad (74)$$

Similarly, one could prove that

$$\sum_j p_{i,j}^{\mathbf{X}, \mathbf{Y}} \mu_{\mathbf{E}_{ij}}(\mathbb{R}^m \times \mathcal{C}) = \mathbb{P}(V_n = j) \mu_{\mathbf{D}_j}(\mathcal{C}), \quad (75)$$

and

$$\sum_i p_{i,j}^{\mathbf{X}, \mathbf{Y}} = \mathbb{P}(V_n = j). \quad (76)$$

Again by using Lemma 7, we have that

$$\begin{aligned} I(\mathbf{X}; \mathbf{Y}) &= \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} D(h_{ij}^*(\mu_{ij}) \| \mathbf{f}_i^*(\mu_{\mathbf{C}_i}) \times \mathbf{g}_i^*(\mu_{\mathbf{D}_j})) \\ &\quad + \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} \log \frac{p_{i,j}^{\mathbf{X}, \mathbf{Y}}}{p_{ij}} \quad (77) \end{aligned}$$

$$\begin{aligned} &\stackrel{(a)}{=} \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} \int d h_{ij}^*(\mu_{\mathbf{E}_{ij}}) \log \frac{d h_{ij}^*(\mu_{\mathbf{E}_{ij}})}{d(\mathbf{f}_i^*(\mu_{\mathbf{C}_i}) \times \mathbf{g}_i^*(\mu_{\mathbf{D}_j}))} \\ &\quad + H(U_m) + H(V_n) + \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} \log p_{i,j}^{\mathbf{X}, \mathbf{Y}} \quad (78) \end{aligned}$$

$$\begin{aligned} &\stackrel{(b)}{=} \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} \int d \mu_{\mathbf{E}_{ij}} \log \frac{d \mu_{\mathbf{E}_{ij}}}{d(\mu_{\mathbf{C}_i} \times \mu_{\mathbf{D}_j})} \\ &\quad + H(U_m) + H(V_n) + \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} \log p_{i,j}^{\mathbf{X}, \mathbf{Y}} \quad (79) \end{aligned}$$

$$\begin{aligned} &\stackrel{(c)}{=} \sum_i \mathbb{P}(U_m = i) h(\mathbf{C}_i) + \sum_j \mathbb{P}(V_n = j) h(\mathbf{D}_j) \\ &\quad - \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} h(\mathbf{E}_{ij}) + H(U_m) + H(V_n) \\ &\quad + \sum_{i,j} p_{i,j}^{\mathbf{X}, \mathbf{Y}} \log p_{i,j}^{\mathbf{X}, \mathbf{Y}} \quad (80) \end{aligned}$$

$$= b(\mathbf{X}) + b(\mathbf{Y}) - b(\mathbf{X}, \mathbf{Y}), \quad (81)$$

where (a) holds because of (74) and (76), (b) follows from a change of variables, and (c) is validated through (73) and (75), and by chain rule $\frac{d \mu_{\mathbf{E}_{ij}}}{d(\mu_{\mathbf{C}_i} \times \mu_{\mathbf{D}_j})} = \frac{d \mu_{\mathbf{E}_{ij}}}{d h_{ij}^*(\ell_{e_i+e'_j})} \frac{d h_{ij}^*(\ell_{e_i+e'_j})}{d(\mu_{\mathbf{C}_i} \times \mu_{\mathbf{D}_j})}$. ■

VII. RESULTS ON RANDOM PROCESSES

In this section, we study the role of the DRB, BID, and IDR introduced in Section III-A and III-B in evaluating compressibility of stochastic processes. More specifically, in the following, we show that under certain conditions, the BID coincides with the ϵ -compression rates. In Section VII-B, we show that moving-average processes satisfy such conditions. Next, by finding the IDR and BID of moving-average processes, we evaluate the ϵ -compression rates for these cases. Finally, in Section VII-C, we quantify the DRB of a class of moving-average processes.

A. BID and ϵ -compression rates

For processes that have samples with affinely singular probability measures, we show that the ϵ -compression rate coincides with the BID under some conditions. This is our first result that makes a connection between information-theoretic and compressed-sensing notions of compressibility.

Theorem 7: Let $\{\mathbf{Z}_t\}_{t=-\infty}^{\infty}$ be a discrete-domain stochastic process for which the distribution of all finite subset of samples is affinely singular as in Lemma 2. Then, if the BID exists, it is achievable as

$$d_B(\{\mathbf{Z}_t\}) = \lim_{m \rightarrow \infty} \mathbb{E}\left[\frac{e_{V_m}}{m}\right]. \quad (82)$$

Moreover, if V_m has a finite sample space for all m and if for all $\epsilon \in (0, 1]$, $\delta \in \mathbb{R}^+$, there exists a finite integer $m(\epsilon, \delta) \in \mathbb{N}$ such that for all $m \geq m(\epsilon, \delta)$ we have

$$\mathbb{P}_V\left(i : \left|\frac{e_i}{m} - d_B(\{\mathbf{Z}_t\})\right| < \delta\right) > 1 - \epsilon, \quad (83)$$

then, for the process $\{\mathbf{Z}_t\}$ we know that

$$R^*(\epsilon) = R_B(\epsilon) = R(\epsilon) = d_B(\{\mathbf{Z}_t\}), \quad (84)$$

where $R_B(\epsilon)$ is the Minkowski dimension compression rate defined in [10, Definition 10].

Proof: See Appendix H. \blacksquare

Sketch of proof: The proof consists of three steps. In the first step, we show that $R(\epsilon) \leq d_B(\{\mathbf{Z}_t\}) + \delta$, for any value of $\delta \in (0, 1)$. For this purpose, we find a high-probability $\lfloor m(d_B(\{\mathbf{Z}_t\}) + \delta) \rfloor$ -rectifiable set \mathcal{R}_m by ignoring high-dimensional affine subsets and bounding \mathbf{Z}^m to a compact set.

In the second step, we prove $R^*(\epsilon) \geq d_B(\{\mathbf{Z}_t\})$ by contradiction; we show that if $d_B(\{\mathbf{Z}_t\}) - R^*(\epsilon) = \delta \in (0, 1)$, then, for every $m \geq M$, every $\lceil (1 - d_B(\{\mathbf{Z}_t\}) + \delta/2)m \rceil$ -dimensional subspace \mathcal{H}^m , and every high-probability set \mathcal{S}^m , the set $(\mathcal{S}_m - \mathcal{S}^m) \cap \mathcal{H}^m$ contains at least one non-zero vector. This coupled with Lemma 1 shows that $R^*(\epsilon) \geq d_B(\{\mathbf{Z}_t\}) - \delta/2$, which is a contradiction.

Finally, in the third step, using inequality $R^*(\epsilon) \leq R_B(\epsilon) \leq R(\epsilon)$ (see [10, Eqn. 75]), we complete the proof. \blacksquare

As an application of the above result, we study compression-rates of moving-average processes in the following subsection.

B. Compression rates and BID of moving-average processes

Using Theorem 5 and Theorem 7, we study a compressed sensing problem below: consider the moving average (MA) process

$$Y_i = \sum_{j=-l_1}^{l_2} c_j W_{i-j}, \quad (85)$$

where the excitation noise $\{W_j\}_{j \in \mathbb{Z}}$ is a set of i.i.d. RVs with discrete-continuous distribution. We further assume that $d(W_j) = \alpha$, and $\{c_j\}_{j \in [-l_1, l_2]}$ are constants with $c_{-l_1}, c_{l_2} \neq 0$. Let us consider the problem of recovering a truncated version of the process $\{Y_t\}$ (e.g., Y_1, \dots, Y_m) from noisy random projections onto lower dimensional sub-spaces. The

goal is to determine the minimum dimension of such sub-spaces in terms of the truncated length (i.e., m). More formally, we would like to find the minimum value of k such that $\mathbf{Y}^m = (Y_1, \dots, Y_m)^\top$ could be fairly recovered from $H_{k \times m} \mathbf{Y}^m + \mathbf{N}^k$ where $H_{k \times m}$ is a random projection matrix and \mathbf{N}^k stands for the noise vector.

Theorem 7 suggests that $k = m\alpha$ if (83) is fulfilled; below we show that, if the sample space of the discrete part of W_i s is finite in the moving-average process, then, this inequality holds. Leveraging this result, we are able to evaluate $R(\epsilon)$ in such cases.

Lemma 8: If we generate an m -dimensional realization of a moving-average process as in (85), the probability of that realization being on an at least $(k+1)$ -dimensional affine singularity for $\frac{k+l_1+l_2}{m+l_1+l_2} < \alpha$, can be bounded as

$$\mathbb{P}_{V_m}(e_{V_m} > k) \geq 1 - \exp\left\{- (m + l_1 + l_2) \mathbb{D}\left(\frac{k+l_2+l_1}{m+l_1+l_2} \parallel \alpha\right)\right\}, \quad (86)$$

and the probability of being on an at most $(k-1)$ -dimensional affine singularity in the case $\frac{k}{m} > \alpha$, is bounded as

$$\mathbb{P}_{V_m}(e_{V_m} < k) \geq 1 - \exp\left\{- m \mathbb{D}\left(\frac{k}{m} \parallel \alpha\right)\right\}, \quad (87)$$

where $\mathbb{D}(p \parallel q)$ is the Kullback-Leibler divergence between $\text{Bern}(p)$ and $\text{Bern}(q)$.

Proof: See Appendix I. \blacksquare

Corollary 8: For each pair $(\epsilon, \delta) \in (0, 1]^2$, there exists a large enough m such that $\mathbb{P}_{V_m}(|\frac{e_{V_m}}{m} - \alpha| > \delta) < \epsilon$.

Proof: To show this, let $\epsilon, \delta \in \mathbb{R}^+$ and define $k_m = m(\alpha - \delta)$. If

$$m \geq \max\left\{\frac{2(l_1+l_2)(1-\alpha+\delta)}{\delta}, \frac{-\log \epsilon}{\mathbb{D}(\alpha-\delta/2 \parallel \alpha)} - l_1 - l_2\right\}, \quad (88)$$

then, we have that

$$\frac{k_m+l_1+l_2}{m+l_1+l_2} = \alpha - \delta + \frac{(l_1+l_2)(1-\alpha+\delta)}{m+l_1+l_2} \leq \alpha - \frac{\delta}{2} \quad (89a)$$

$$< \alpha. \quad (89b)$$

Now, using Lemma 8 we conclude that

$$\begin{aligned} \mathbb{P}_{V_m}(e_{V_m} > k_m) &\geq 1 - \exp\left\{- (m + l_1 + l_2) \mathbb{D}\left(\frac{k_m+l_2+l_1}{m+l_1+l_2} \parallel \alpha\right)\right\} \\ &\stackrel{(a)}{\geq} 1 - \exp\left\{- (m + l_1 + l_2) \mathbb{D}(\alpha - \delta/2 \parallel \alpha)\right\} \\ &\stackrel{(b)}{\geq} 1 - \epsilon, \end{aligned} \quad (90)$$

where (a) is due to (89a) and (b) is because of (88).

To upper-bound e_{V_m} , let $k'_m = m(\alpha + \delta)$. Thus,

$$\frac{k'_m}{m} = \alpha + \delta > \alpha. \quad (91)$$

Now, if

$$m \geq \frac{-\log \epsilon}{\mathbb{D}(\alpha+\delta \parallel \alpha)}, \quad (92)$$

we can conclude

$$\begin{aligned} \mathbb{P}_{V_m}(e_{V_m} < k'_m) &\geq 1 - \exp\left\{- m \mathbb{D}\left(\frac{k'_m}{m} \parallel \alpha\right)\right\} \\ &\stackrel{(a)}{\geq} 1 - \exp(-m \mathbb{D}(\alpha + \delta \parallel \alpha)) \end{aligned}$$

$$\stackrel{(b)}{\geq} 1 - \epsilon, \quad (93)$$

using (87). Here, (a) is because of (91) and (b) is due to (92). ■

Next, we find the IDR and BID of MA processes in the general case; here, the alphabet of the discrete component is not necessarily restricted to be finite as opposed to the result in Theorem 7.

Theorem 9: Let $\{Y_i\}$ be a MA process as in (85) with $d(W_j) = \alpha$. Then, we have

$$d_B(\{\mathbf{Y}_t\}) = d_I(\{\mathbf{Y}_t\}) = \alpha. \quad (94)$$

Proof: For a better explanation of the linear transformation in (85), we can express the truncated process $\{\mathbf{Y}_t\}$ as

$$\mathbf{Y}^m = \underbrace{\begin{bmatrix} c_{-l_1} & \dots & c_{l_2} & 0 & \dots & 0 \\ 0 & c_{-l_1} & \dots & c_{l_2} & \dots & 0 \\ \vdots & \dots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & c_{-l_1} & \dots & c_{l_2} \end{bmatrix}}_{A_m} \mathbf{W}^{m+l_1+l_2}, \quad (95)$$

where c_j s are the constants introduced in (85). Due to the Lipschitz dependence of \mathbf{Y}^m on $\mathbf{W}^{m+l_1+l_2}$, we know that

$$d(\mathbf{Y}^m) \leq (m + l_1 + l_2)\alpha, \quad (96)$$

where α stands for the probability of W_i s being drawn from the continuous component (α_i in (2)). To lowerbound $d(\mathbf{Y}^m)$, let us consider W_i s separately and assume each has its own α_i (i.e., α_i s could be different). From Remark 2, we know that $d(\mathbf{Y}^m)$ does not depend on the choice of the discrete component of W_i s; thus, if we assume W_i takes the value 0 with probability $1 - \alpha_i$ (and is drawn from a continuous distribution with probability α_i), $d(\mathbf{Y}^m)$ remains unchanged. Furthermore, if we decrease any α_i , then, $d(\mathbf{Y}^m)$ decreases or remains unchanged. Therefore, a lower-bound for $d(\mathbf{Y}^m)$ can be achieved by setting the first $l_1 + l_2$ terms $W_1 = \dots = W_{l_1+l_2} \equiv 0$ which corresponds to $\alpha_1 = \dots = \alpha_{l_1+l_2} = 0$. This implies that

$$\begin{aligned} d(\mathbf{Y}^m) &\geq d\left(Q_m [W_{l_1+l_2+1}, \dots, W_{l_1+l_2+m}]^\top\right) \\ &= \sum_{\mathbf{s} \in \{0,1\}^m} \text{rank}(Q_m^{[\mathbf{s}]}) \alpha^{\|\mathbf{s}\|_1} (1 - \alpha)^{(1 - \|\mathbf{s}\|_1)}, \end{aligned} \quad (97)$$

where Q_m is the matrix formed by columns with index $[l_1 + l_2 + 1 : l_1 + l_2 + m]$ of A_m . Since Q_m is a lower triangular matrix with non-zero diagonal elements, we conclude that it is full-rank. Hence, we have

$$\begin{aligned} d(\mathbf{Y}^m) &\geq \sum_{\mathbf{s} \in \{0,1\}^m} \left(\sum_{i=1}^m s_i \right) \alpha^{(\sum_{i=1}^m s_i)} (1 - \alpha)^{(1 - \sum_{i=1}^m s_i)} \\ &= \sum_{i=0}^m i \alpha^i (1 - \alpha)^{1-i} = m\alpha. \end{aligned} \quad (98)$$

By combining (96) and (98) as $m \rightarrow \infty$, we have that

$$d_B(\{\mathbf{Y}_t\}) = \lim_{m \rightarrow \infty} \frac{d(\mathbf{Y}^m)}{m} = \alpha. \quad (99)$$

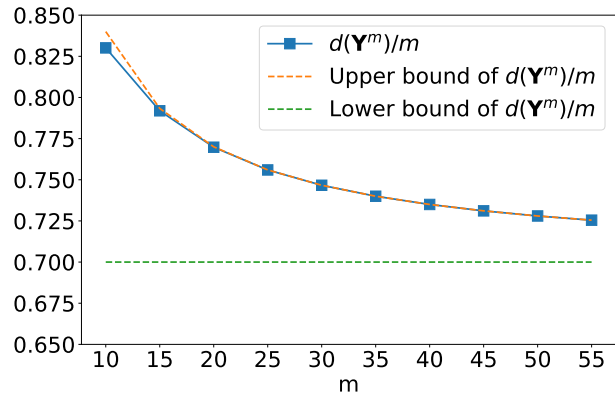


Fig. 5. Block-average information dimension of a moving-average process samples and its bounds as in (96) and (98), in the special case in which $\mathbf{a} = [-2, 0.5, 1]$ and $\alpha = 0.7$.

Moreover, since MA processes are ψ^* -mixing according to the definition in [12], due to [27, Corollary 15] we know that the IDR and BID for such processes are equal, which together with (99) concludes

$$d_I(\{\mathbf{Y}_t\}) = \alpha. \quad (100)$$

To better visualize Theorem 9, we consider the MA process associated with $\mathbf{c} = [-2, 0.5, 1]$ and $\alpha = 0.7$; Figure 5 depicts the evolution of $\frac{d(\mathbf{Y}^m)}{m}$, as well as the upper and lower-bounds in (96) and (98).

Note that Theorem 9 is an improvement over [12, Theorem 5] wherein the proved equality in this work is presented only as an upper-bound. Nevertheless, [12, Theorem 9] implies that if a bounded MA process is sampled using an $m \times n$ random matrix with independent standard normal entries, then, the Lagrangian-minimum entropy pursuit (MEP) algorithm reconstructs the realization of MA process with no asymptotic loss as n grows to infinity.

C. DRB of moving-average processes

As an application of the result in Theorem 5 and the evaluation of the value of DRB therein, we consider the samples of a moving-average process with discrete-continuous excitation. Indeed, we truncate the samples into an m -dimensional vector and evaluate the DRB of the vector normalized by m as $m \rightarrow \infty$. This measure is useful for comparing the compressibility of processes with the same BID (e.g., two MA processes with discrete-continuous excitation that have the same information dimension).

To express our results on the DRB of a process, we introduce the following notations

$$\Psi_\alpha(c_{-l_1}, \dots, c_{l_2}) = \Psi_\alpha(A_m) := \lim_{m \rightarrow \infty} \psi_{m,\nu}(A_m), \quad (101)$$

where $\psi_{m,\nu}(\cdot)$ is defined in (51). Note that A_m is determined by moving-average process coefficients $(c_{-l_1}, \dots, c_{l_2})$.

Proposition 2: For the MA process in (85), if $h(W_{c,1}) > -\infty$, $M_{W_{c,1}}(\beta) < \infty$ for some $\beta \in \mathbb{R}^+$, and the support of $W_{d,1}$ is a finite set, then, with Ψ_α defined as (101) we have that

- $\lim_{m \rightarrow \infty} \frac{b(\mathbf{Y}^m)}{m} = b(W_1) + \Psi_\alpha(c_{-l_1}, \dots, c_{l_2})$, given $\alpha \in (0, \frac{1}{l_1+l_2})$, and
- $\lim_{m \rightarrow \infty} \frac{b(\mathbf{Y}^m)}{m} = b(W_1)$, given $\alpha = 0$, and $\mathbb{P}(W_{d,1} \neq 0) \in (0, \frac{1}{l_1+l_2})$.

Before we proceed to the proof of Proposition 2, we provide the below lemma that considers a general linear transformation of discrete-continuous RVs (i.e., not necessarily samples of an MA process).

Lemma 9: Let $\{\mathbf{X}_t\}$ be an i.i.d. process with discrete-continuous elements as (2). We denote the continuous and discrete components of X_i by $X_{c,i}$ and $X_{d,i}$, respectively; α_i also stands for the probability that X_i takes a value from the corresponding continuous measure. Further, assume $h(X_{c,1}) > -\infty$, $M_{X_{c,1}}(\beta) < \infty$ for some $\beta \in \mathbb{R}^+$, and $X_{d,i}$ takes values in a finite set. Let $g : \mathbb{N} \rightarrow \mathbb{N}$ be a function that satisfies $g(m) > \beta e$ for large enough m , and let $G(m) = \max(g(1), \dots, g(m))$. For each $m = 1, 2, \dots$, we define $Y_m = \mathbf{c}_m^T \mathbf{X}^{g(m)}$ where $\mathbf{c}_m \in \mathbb{R}^{g(m)}$ is an arbitrary but known vector. Hence, $\{\mathbf{Y}_t\}$ is a random process that linearly depends on $\{\mathbf{X}_t\}$. Besides, we form $m \times G(m)$ matrices A_m by zero-padding each \mathbf{c}_i^T in the range $i = 1, \dots, m$ with enough zeros to increase the length of the vector to $G(m)$ and stacking all of them as the rows of the matrix A_m . Now, there exist fixed values $C_i \in \mathbb{R}$ (or $\tilde{C}_i \in \mathbb{R}$) for $i \in [2]$ such that

- if $\alpha_1 \neq 0$, then, for sufficiently large m ,

$$\begin{aligned} & \left| \frac{b(\mathbf{Y}^m)}{m} - \frac{G(m)}{m} b(X_1) - \psi_{m,\nu}(A_m) \right| \\ & \leq \frac{G(m)}{m} \rho_m(A_m, \alpha) (C_1 G(m) + C_2 \log \rho_m(A_m, \alpha)), \end{aligned} \quad (102)$$

where

$$\rho_m(A_m, \alpha) := \mathbb{P}_\nu(I_{\text{fcr}}(A_m^\nu) = 0), \quad (103)$$

provided that $G(m)\rho_m(A_m, \alpha) \leq \frac{1}{2e}$ for such m ,

- if X_1 is discrete (i.e., $\alpha_1 = 0$), then, for sufficiently large m ,

$$\begin{aligned} & \left| \frac{b(\mathbf{Y}^m)}{m} - \frac{G(m)}{m} b(X_1) \right| \\ & \leq \frac{G(m)}{m} \tilde{\rho}_m(A_m, \xi) (\tilde{C}_1 G(m) + \tilde{C}_2 \log \tilde{\rho}_m(A_m, \xi)), \end{aligned} \quad (104)$$

where

$$\tilde{\rho}_m(A_m, \xi) = \mathbb{P}_\xi(I_{\text{fcr}}(A_m^\xi) = 0), \quad (105)$$

provided that $G(m)\tilde{\rho}_m(A_m, \xi) \leq \frac{1}{2e}$ for such m . Here, $\xi = [\xi_1, \dots, \xi_{G(m)}]$ and $\{\xi_i\}$ is a set of i.i.d. Bernoulli RVs with $\mathbb{P}(\xi_i = 0) = \mathbb{P}(X_{d,1} = 0)$, where $\psi_{m,\nu}(A_m)$ is defined as in (51) and ν is the selection RV defined in (2).

Proof: See Appendix J.

Corollary 10: Provided that the conditions in Lemma 9 are satisfied, one can now verify that

- if $\alpha_1 \neq 0$, $G(m) - m \sim o(m)$, and $\rho_m(A_m, \alpha) \sim o(1/m)$, then

$$\lim_{m \rightarrow \infty} \frac{b(\mathbf{Y}^m)}{m} = b(X_1) + \Psi_\alpha(A_m), \quad (106)$$

where $\Psi_\alpha(A_m)$ in (101) is well-defined.

- if $\alpha_1 = 0$, $G(m) - m \sim o(m)$, and $\tilde{\rho}_m(A_m, \xi) \sim o(1/m)$, then

$$\lim_{m \rightarrow \infty} \frac{b(\mathbf{Y}^m)}{m} = b(X_1), \quad (107)$$

Proof of Proposition 2: Since c_{-l_1} and c_{l_2} are non-zero, for $m \geq l_1 + l_2$, A_m cannot have a zero column (each column includes at least one of c_{-l_1} and c_{l_2}). We further check when $I_{\text{fcr}}(A_m^{[s]})$ can be zero (linear dependence among columns of A_m for which $s_i \neq 0$). Let $1 \leq i_1 < \dots < i_t \leq n$ be such that $s_{i_j} = 1$ and a linear combination of columns $\{i_1, \dots, i_t\}$ of A_m with non-zero coefficients is zero. We claim that $i_{j+1} - i_j \leq l_1 + l_2$ for all $1 \leq j \leq t-1$. Indeed, if $i_{j+1} - i_j > l_1 + l_2$, then, the $(i_{j+1} - l_1 - l_2)$ th element in any linear combination of $A_m^{[i_1]}, \dots, A_m^{[i_t]}$ with non-zero coefficients, is non-zero. Note that the $(i_{j+1} - l_1 - l_2)$ th element of all $A_m^{[i_k]}$ is zero for all $k \in [t]$ except for $k = j+1$. A similar argument shows that $i_1 \leq l_1 + l_2$; otherwise, the $(i_1 - l_1 - l_2)$ th element in any linear combination with non-zero coefficients shall be non-zero. Thus, we conclude that $t \geq \lfloor \frac{n-1}{l_1+l_2} \rfloor$, or equivalently, $\sum_{i=1}^n s_i \geq \lfloor \frac{n-1}{l_1+l_2} \rfloor$. Using this fact, [37, Theorem 1], and the definition of $\rho_m(A_m, \alpha)$ in (103), we have that

$$\begin{aligned} \rho_m(A_m, \alpha) & \leq \exp(-nD(\frac{n-1}{n(l_1+l_2)} \parallel \alpha)) \\ & < \exp(-nD(\frac{1}{l_1+l_2} \parallel \alpha)), \end{aligned} \quad (108)$$

provided that $\alpha < \frac{n-1}{n(l_1+l_2)}$. Note that $D(p \parallel q)$ is the KL-divergence between $\text{Bern}(p)$ and $\text{Bern}(q)$. Since we assumed $\alpha \in (0, \frac{1}{l_1+l_2})$, this condition is satisfied for large enough n .

Similarly, if we let $\alpha' = \mathbb{P}(W_{d,1} \neq 0)$, we can bound $\tilde{\rho}_m(A_m, \xi)$ as

$$\tilde{\rho}_m(A_m, \xi) < \exp\left(-nD\left(\frac{1}{l_1+l_2} \parallel \alpha'\right)\right). \quad (109)$$

Finally, (108) and (109) together with Corollary 10 yield the results in Proposition 2. ■

Proposition 3: $\Psi_\alpha(c_1, c_2)$ as defined in (101) exists, is bounded and is equal to

$$\Psi_\alpha(c_1, c_2) = \frac{1-\alpha}{2} \mathbb{E}_Y[\log E_Y], \quad (110)$$

in which Y is an α -geometric RV (defined in (284)), and E_k is defined as

$$E_k := \begin{cases} \frac{c_1^{2k+2} - c_2^{2k+2}}{c_1^2 - c_2^2}, & c_1^2 \neq c_2^2 \\ c_1^{2k}(1+k), & c_1^2 = c_2^2 \end{cases}. \quad (111)$$

Proof: See Appendix K. ■

For the visual illustration of the results, we consider three examples in Figure 6, namely

- Case 1) a Bernoulli-Gaussian excitation noise with $\alpha = 0.6$, and Gaussian variance $\sigma^2 = 1$, passed through the MA system $Y_m = 1.5X_{m-1} + X_m$,
- Case 2) a Bernoulli-Laplace excitation noise with $\alpha = 0.6$, and Laplace parameter $b = 1$, passed through the MA system $Y_m = 1.5X_{m-1} + X_m$, and
- Case 3) a Bernoulli-Laplace excitation noise with $\alpha = 0.4$, and Laplace parameter $b = 1$, passed through the MA system $Y_m = X_{m-2} + 1.2X_{m-1} + X_m$.

For these cases, we have plotted the Monte-Carlo evaluation of $\psi_{m,\nu}(\cdot)$ via Prop. 2, and its convergence to the average information loss $\lim_{m \rightarrow \infty} \frac{b(\mathbf{Y}^m)}{m} - \lim_{n \rightarrow \infty} \frac{b(\mathbf{X}^n)}{n}$ based on Proposition 3. The Monte-Carlo simulation of $\psi_{m,\nu}(\cdot)$ is done by forming a set of randomly generated binary selection variables \mathcal{S}_M from the distribution $\text{Bern}(\alpha)$, and finding $\hat{\psi}_m = \frac{1}{mM} \sum_{s \in \mathcal{S}_M} \log \det^+(A_m^{[s]})$. Next, we can estimate the variance of $\log \det^+(A_m^{[s]})$ via an unbiased variance estimator. Since the terms $\log \det^+(A_m^{[s]})$ are bounded, as M grows, $\hat{\psi}_M$ converges in distribution to a Gaussian random variable. Hence, using error function (erf) we can approximate the interval in which $\hat{\psi}_M$ falls with 95% probability. Further, using (102), we can find an upper- and lower-bound on $\frac{b(\mathbf{Y}^m)}{m} - b(X_1)$ by $\psi_{m,\nu}(A_m)$ and a diminishing term. This, coupled with the previous Monte-Carlo analysis, could give us a 95% confidence interval on $\frac{b(\mathbf{Y}^m)}{m} - b(X_1)$. In all the three cases, we observe that the 95% confidence interval shrinks as n increases.

VIII. CONCLUSION

In this paper, we defined a new class of probability measures that have singularities over affine subsets. This is a high-dimensional extension of a sparse random variable that includes a mass probability at the origin. We studied the compressibility of this new class using conventional notions such as RID and also the new notion of DRB. Specifically, we found the analytical value of the RID and DRB of a linear functions of i.i.d. vectors with element-wise discrete-continuous RV. Furthermore, we provided an upper-bound for Lipschitz functions of this class of RVs. Next, we established a connection between the notions of DRB and mutual information between two affinely singular RVs. Studying this connection for two general RVs (not necessarily affinely singular) is a potential research direction. We evaluated the BID, IDR, and DRB of a discrete-domain moving-average process with discrete-continuous excitation noise. The RID was shown to be closely related to the notion of ϵ -compression rates in such cases. Overall, the results show that the RID plays a fundamental role in evaluating the compressibility of sequences with dependent components in compressed-sensing scenarios. Furthermore, our results show that instead of sparsity, it is affine singularity that determine the extent to which we could smoothly compress and robustly reconstruct a sequence. Indeed, although the samples of a moving-average process are less sparse than their excitation noise, they could be equally compressed. Such phenomenon could be further investigated for more general processes, such as auto-regressive moving-average processes. Our results on the DRB, its application in evaluating mutual information, and its equality with Shannon's entropy and differential entropy in discrete and continuous cases nominate DRB as a useful replacement for compressibility measures such as RDE in comparing the compressibility of sources with the same RID.

REFERENCES

[1] C. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[2] A. Kolmogorov, "On the Shannon theory of information transmission in the case of continuous signals," *IRE Transactions on Information Theory*, vol. 2, no. 4, pp. 102–108, 1956.

[3] A. Rényi, "On the dimension and entropy of probability distributions," *Acta Mathematica Hungarica*, vol. 10, no. 1-2, pp. 193–215, 1959.

[4] G. Koliander, G. Pichler, E. Riegler, and F. Hlawatsch, "Entropy and source coding for integer-dimensional singular random variables," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6124–6154, 2016.

[5] C. Shannon, "Coding theorems for a discrete source with a fidelity criterion," *Institute of Radio Engineers, International Convention Records*, vol. 7, pp. 325–350, 1959.

[6] T. Linder and R. Zamir, "On the asymptotic tightness of the Shannon lower bound," *IEEE Transactions on Information Theory*, vol. 40, no. 6, pp. 2026–2031, 1994.

[7] A. Amini, M. Unser, and F. Marvasti, "Compressibility of deterministic and random infinite sequences," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5193–5201, 2011.

[8] J. F. Silva and M. S. Derpich, "Precise best k-term approximation error analysis of ergodic processes," in *2014 IEEE International Symposium on Information Theory*, June 2014, pp. 2654–2658.

[9] —, "On the characterization of ℓ_p -compressible ergodic sequences," *IEEE Transactions on Signal Processing*, vol. 63, no. 11, pp. 2915–2928, June 2015.

[10] Y. Wu and S. Verdú, "Rényi information dimension: Fundamental limits of almost lossless analog compression," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3721–3748, 2010.

[11] F. E. Rezagah, S. Jalali, E. Erkip, and H. V. Poor, "Compression-based compressed sensing," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6735–6752, 2017.

[12] S. Jalali and H. V. Poor, "Universal compressed sensing for almost lossless recovery," *IEEE Transactions on Information Theory*, vol. 63, no. 5, pp. 2933–2953, May 2017.

[13] H. Ghourchian, A. Amini, and A. Gohari, "How compressible are innovation processes?" *IEEE Transactions on Information Theory*, vol. 64, no. 7, pp. 4843–4871, July 2018.

[14] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[15] D. L. Donoho, A. Javanmard, and A. Montanari, "Information-theoretically optimal compressed sensing via spatial coupling and approximate message passing," *IEEE transactions on information theory*, vol. 59, no. 11, pp. 7434–7464, 2013.

[16] J. D. Farmer, "Information dimension and the probabilistic structure of chaos," *Zeitschrift für Naturforschung A*, vol. 37, no. 11, pp. 1304–1326, 1982.

[17] J. Geronimo and D. Hardin, "An exact formula for the measure dimensions associated with a class of piecewise linear maps," *Constructive Approximation*, vol. 5, no. 1, pp. 89–98, 1989.

[18] T. Kawabata and A. Dembo, "The rate-distortion dimension of sets and measures," *IEEE transactions on information theory*, vol. 40, no. 5, pp. 1564–1572, 1994.

[19] Y. Lin'kov, "Evaluation of ϵ -entropy of random variables for small ϵ ," *Problemy Peredachi Informatsii*, vol. 1, no. 2, pp. 18–26, 1965.

[20] T. Yamada, S. Tazaki, and G. R., "Asymptotic performance of block quantizers with difference distortion measures," *IEEE Transactions on Information Theory*, vol. 26, no. 1, pp. 6–14, 1980.

[21] H. Rosenthal and J. Biniai, "On the epsilon entropy of mixed random variables," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1110–1114, 1988.

[22] A. Gyorgy, T. Linder, and K. Zeger, "On the rate-distortion function of random vectors and stationary sources with mixed distributions," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2110–2115, 1999.

[23] I. Csiszár, "Some remarks on the dimension and entropy of random variables," *Acta Mathematica Hungarica*, vol. 12, no. 3-4, pp. 399–408, 1961.

[24] B. Hunt and V. Kaloshin, "How projections affect the dimension spectrum of fractal measures," *IEEE Transactions on Information Theory*, vol. 10, no. 5, pp. 1031–1046, 1997.

[25] T. Berger, *Rate distortion theory*. Englewood Cliffs, N.J., Prentice-Hall, 1971.

[26] R. Gray, "Information rates of autoregressive processes," *IEEE transactions on information theory*, vol. 16, no. 4, pp. 412–421, 1970.

[27] B. C. Geiger and T. Koch, "On the information dimension of stochastic processes," *EEE Transactions on Information Theory*, 2019.

[28] W. Rudin, *Real and complex analysis*. Tata McGraw-hill education, 2006.

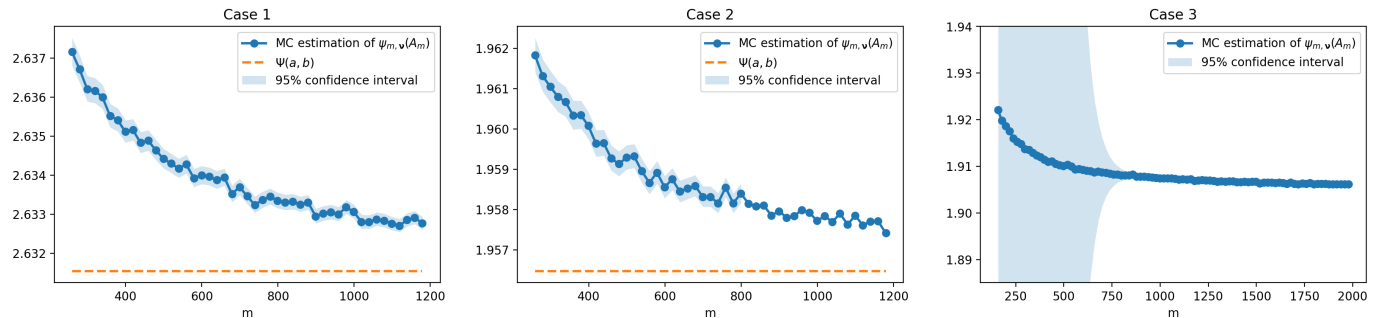


Fig. 6. Monte-Carlo estimation of $\psi_{m,\nu}(A_m)$, the 95% confidence interval of the difference $\frac{b(\mathbf{Y}^m)}{m} - b(X_1)$, and the value of Ψ for the three cases mentioned in Section VII-C.

- [29] J. Naumann and C. G. Simader, *Measure and integration on Lipschitz-manifolds*. Humboldt-Universität zu Berlin, Mathematisch-Naturwissenschaftliche Fakultät, 2011.
- [30] J. Heinonen, *Lectures on Lipschitz analysis*. University of Jyväskylä, 2005, no. 100.
- [31] C. De Lellis, "Lecture notes on rectifiable sets, densities, and tangent measures," *Preprint*, vol. 23, 2006.
- [32] J. Balatoni and A. Rényi, "Remarks on entropy," *Publ. Math. Inst. Hung. Acad. Sci.*, vol. 1, pp. 9–40, 1956.
- [33] Y. Wu, "Shannon theory for compressed sensing," Ph.D. dissertation, Princeton University, 2011.
- [34] R. Gallager, *Information theory and reliable communication*. New York: Wiley, 1968.
- [35] L. Ambrosio, N. Fusco, and D. Pallara, *Functions of bounded variation and free discontinuity problems*. Courier Corporation, 2000.
- [36] C. Nair, B. Prabhakar, and D. Shah, "On entropy for mixtures of discrete and continuous variables," *arXiv preprint cs/0607075*, 2006.
- [37] R. Arratia and L. Gordon, "Tutorial on large deviations for the binomial distribution," *Bulletin of mathematical biology*, vol. 51, no. 1, pp. 125–131, 1989.
- [38] S. J. Axler, *Linear algebra done right*. Springer, 1997, vol. 2.
- [39] U. Kirmaci, M. K. Bakula, M. Özdemir, and J. E. Pecaric, "On some inequalities for p-norms," *Journal of Inequalities in Pure and Applied Mathematics*, vol. 9, no. 1, 2008.
- [40] D. Shanbhag and M. Sreehari, "On certain self-decomposable distributions," *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, vol. 38, no. 3, pp. 217–222, 1977.
- [41] Y. Polyanskiy and Y. Wu, *Lecture notes on information theory*. Lecture Notes for ECE563 (UIUC), 2017.
- [42] S. Foucart and H. Rauhut, "An invitation to compressive sensing," in *A mathematical introduction to compressive sensing*. Springer, 2013, pp. 1–39.
- [43] H. Federer, *Geometric measure theory*, ser. Grundlehren der mathematischen Wissenschaften. Springer, 1969. [Online]. Available: <https://books.google.ae/books?id=TALvAAAAMAAJ>
- [44] H. Steinhaus, "Sur les distances des points dans les ensembles de mesure positive," *Fundamenta Mathematicae*, vol. 1, no. 1, pp. 93–104, 1920. [Online]. Available: <http://eudml.org/doc/212590>
- [45] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.
- [46] C. C. Pugh, *Real mathematical analysis*. Springer, 2015.

APPENDIX A PROOF OF LEMMA 3

In this section, we first prove the following lemma, which expresses that a full-row-rank matrix preserves absolute continuity of a random vector. By means of this lemma, then we prove Lemma 3.

Lemma 10: Let \mathbf{X}^n be an absolutely continuous RV and let $\mathbf{Y}^m = A_m \mathbf{X}^n$. If $\text{rank}(A_m) = m$, then, \mathbf{Y}^m is also an absolutely continuous RV.

Proof: Since A_m has full row rank, the rows of A_m are linearly independent. Therefore, it is possible to extend these m rows to a set of n linearly independent row vector ([38, Theorem 2.12]). We can now form the $n \times n$ matrix A_{aug} by

using this linearly independent set as the rows. Obviously, A_{aug} is invertible. Since \mathbf{X}^n is absolutely continuous and A_{aug} is invertible, we conclude that $\mathbf{Y}_{\text{aug}} = A_{\text{aug}} \mathbf{X}^n$ is also absolutely continuous (A_{aug}^{-1} is a linear operator and maps sets with zero-Lebesgue-measure into sets with zero-Lebesgue-measure [28, Theorem 2.20]). Finally, note that the probability distribution of $\mathbf{Y} = A_m \mathbf{X}^n$ is a marginal distribution of \mathbf{Y}_{aug} ; hence, it is also absolutely continuous. ■

Now we get back to the proof of Lemma 3. We can represent $A_m \mathbf{X}^n$ as

$$\begin{aligned} A_m \mathbf{X}^n &= \sum_{\mathbf{s} \in \{0,1\}^n} \mathbb{1}_{\nu=\mathbf{s}} A_m \mathbf{X}^n \\ &= \sum_{\mathbf{s} \in \{0,1\}^n} \mathbb{1}_{\nu=\mathbf{s}} (A_m^{[\mathbf{s}]} \mathbf{X}_c^{\mathbf{s}} + A_m^{[\bar{\mathbf{s}}]} \mathbf{X}_d^{\bar{\mathbf{s}}}) \\ &= \sum_{\mathbf{s} \in \{0,1\}^n} \sum_{\mathbf{x}_d^{\bar{\mathbf{s}}} \in \mathcal{X}_{\bar{\mathbf{s}}}} \mathbb{1}_{\nu=\mathbf{s}, \mathbf{x}_d^{\bar{\mathbf{s}}}=\mathbf{x}} (A_m^{[\mathbf{s}]} \mathbf{X}_c^{\mathbf{s}} + A_m^{[\bar{\mathbf{s}}]} \mathbf{x}_d^{\bar{\mathbf{s}}}). \end{aligned} \quad (112)$$

The definition of $\mathcal{T}_i^{(m)}$ for $i \in \mathbb{N}$ (before (33)) implies that $\bigcup_{i \in \mathbb{N}} \mathcal{T}_i^{(m)} = \{(\mathbf{s}, \mathbf{x}_d^{\bar{\mathbf{s}}}) : \mathbf{s} \in \{0,1\}^n, \mathbf{x}_d^{\bar{\mathbf{s}}} \in \mathcal{X}_{\bar{\mathbf{s}}}\}$. As a result, one can rewrite (112) as

$$A_m \mathbf{X}^n = \sum_{i \in \mathbb{N}} \sum_{(\mathbf{s}, \mathbf{x}_d^{\bar{\mathbf{s}}}) \in \mathcal{T}_i^{(m)}} \mathbb{1}_{\nu=\mathbf{s}, \mathbf{x}_d^{\bar{\mathbf{s}}}=\mathbf{x}} (A_m^{[\mathbf{s}]} \mathbf{X}_c^{\mathbf{s}} + A_m^{[\bar{\mathbf{s}}]} \mathbf{x}_d^{\bar{\mathbf{s}}}). \quad (113)$$

Next, we deploy the singular value decomposition for $A_m^{[\mathbf{s}]}$ as

$$A_m^{[\mathbf{s}]} = \underline{U}_s D_s \underline{U}_s^\dagger, \quad (114)$$

where D_s , \underline{U}_s and \underline{U}_s indicate the diagonal $m \times k$ matrix of the singular values, the $k \times k$ matrix of right-singular vectors and the $m \times m$ matrix of left-singular vectors of $A_m^{[\mathbf{s}]}$; here, k represents the number of non-zero elements in \mathbf{s} . Hence, we see that

$$A_m^{[\mathbf{s}]} \mathbf{X}_c^{\mathbf{s}} + A_m^{[\bar{\mathbf{s}}]} \mathbf{x}_d^{\bar{\mathbf{s}}} = \underline{U}_s (\mathbf{Y}_s^\top, \underbrace{0, \dots, 0}_{m - \text{rank}(A^{[\mathbf{s}]})})^\top + A_m^{[\bar{\mathbf{s}}]} \mathbf{x}_d^{\bar{\mathbf{s}}}, \quad (115)$$

where using Lemma 10, \mathbf{Y}_s is an absolutely continuous RV defined as

$$\mathbf{Y}_s = \tilde{D}_s \underline{U}_s^\dagger \mathbf{X}_c^{\mathbf{s}}, \quad (116)$$

with \tilde{D}_s being a $\text{rank}(A_m^{[\mathbf{s}]}) \times k$ matrix formed by the first

$\text{rank}(A_m^{[s]})$ rows of D_s . If the columns of \underline{U}_s are shown by $\{\mathbf{u}_i^s\}_{i \in [n]}$, (115) reveals that $A_m^{[s]}\mathbf{X}_c^s + A_m^{[s]}\mathbf{x}_d^s$ is supported on the affine subset $\mathcal{A}(s, \mathbf{x}_d^s)$ of \mathbb{R}^m , defined via

$$\mathcal{A}(s, \mathbf{x}_d^s) = \left\{ \sum_{i=1}^{\text{rank}(A_m^{[s]})} a_i \mathbf{u}_i^s + \mathbf{b}^\perp(s, \mathbf{x}_d^s) : \mathbf{a} \in \mathbb{R}^{\text{rank}(A_m^{[s]})} \right\}, \quad (117)$$

where

$$\mathbf{b}^\perp(s, \mathbf{x}_d^s) = \underline{U}_s \widehat{U}_s^\dagger A_m^{[s]} \mathbf{x}_d^s, \quad (118)$$

is perpendicular to $\text{span}(\{\mathbf{u}_i^s\}_{i \in [\text{rank}(A_m^{[s]})]})$; \widehat{U}_s is the $m \times m$ matrix formed by zeroing off the first $\text{rank}(A_m^{[s]})$ columns of \underline{U}_s . We should highlight that for all $(s, \mathbf{x}_d^s) \in \mathcal{T}_i^{(m)}$, $A_m^{[s]}$ shall span the same space; therefore, without loss of generality, we use $\text{rank}(A_m^{[s]}) = r_i$, $\underline{U}_s = U_i$, and $\mathbf{b}^\perp(s, \mathbf{x}_d^s) = \mathbf{b}_i$; i.e., only the index i for $\mathcal{T}_i^{(m)}$ is important, and not the specific vector of s (as long as $(s, \mathbf{x}_d^s) \in \mathcal{T}_i^{(m)}$). We can now rewrite (115) as

$$A_m^{[s]}\mathbf{X}_c^s + A_m^{[s]}\mathbf{x}_d^s = \underline{U}_i (\mathbf{W}_{s, \mathbf{x}_d^s}^\top, \underbrace{0, \dots, 0}_{m-r_i})^\top + \mathbf{b}_i, \quad (119)$$

in which $\mathbf{W}_{s, \mathbf{x}_d^s}$ is defined in (33). For the sake of simplicity, we define the RV $\Upsilon_m^{(i)}$ for $i \in \mathbb{N}$ as

$$\Upsilon_m^{(i)} = \begin{cases} (\boldsymbol{\nu}, \mathbf{X}_d^s) & \Upsilon_m = i, \\ T_i & \text{otherwise,} \end{cases} \quad (120)$$

where T_i is a RV independent of Υ_m and supported on $\mathcal{T}_i^{(m)}$, with probability mass function

$$\forall (s, \mathbf{x}_d^s) \in \mathcal{T}_i^{(m)} : \quad \mathbb{P}(T_i = (s, \mathbf{x}_d^s)) = \frac{\mathbb{P}_{\boldsymbol{\nu}, \mathbf{X}_d^s}(\mathbf{s}, \mathbf{x}_d^s)}{\mathbb{P}(\Upsilon_m = i)}. \quad (121)$$

The definition of T_i is such that $\mathbb{P}(\Upsilon_m^{(i)} | \Upsilon_m = j)$ for all j is the same (whether $j = i$ or $j \neq i$); consequently, $\Upsilon_m^{(i)}$ and Υ_m are independent. Furthermore, the probability mass function of $\Upsilon_m^{(i)}$ coincides with (32).

With these notations in hand, we combine (113) and (119) to rewrite $A_m \mathbf{X}^n$ as

$$A_m \mathbf{X}^n = \sum_{i \in \mathbb{N}} \mathbb{1}_{\Upsilon_m = i} \left[\underline{U}_i (\widetilde{\mathbf{Y}}_i^\top, \underbrace{0, \dots, 0}_{m-r_i})^\top + \mathbf{b}_i \right], \quad (122)$$

where $\widetilde{\mathbf{Y}}_i$ is defined in (35). This representation coupled with (34) proves

$$\mathbf{Y}^m = \mathbf{f}_{\Upsilon_m}(\widetilde{\mathbf{Y}}_{\Upsilon_m}). \quad (123)$$

The definitions of \mathbf{X}^n and $\mathbf{W}_{s, \mathbf{x}_d^s}$ in (2) and (33), respectively, show that $\mathbf{W}_{s, \mathbf{x}_d^s}$ is independent of $(\boldsymbol{\nu}, \mathbf{X}_d^s)$. Since $\widetilde{\mathbf{Y}}_i$ is a function of $\mathbf{W}_{s, \mathbf{x}_d^s}$ and $\Upsilon_m^{(i)}$, it is independent of Υ_m . This point implies that (123) has a similar representation as (24).

APPENDIX B PROOF OF THEOREM 4

We calculate RID and DRB of the affinely singular random vectors as follows.

A. RID of affinely singular RVs

By comparing Definition 1 and 5, and making use of Lemma 2, one can see that the probability measure of the affinely singular RV \mathbf{Z}^m is a mixture of e_i -regular measures with set of probabilities $\{\mathbb{P}(V_m = i)\}_i$. Since $H(V_m) < \infty$ and using Lemma 4, one can show that

$$d(\mathbf{Z}^m) = \mathbb{E}_{V_m}[e_{V_m}]. \quad (124)$$

B. DRB of affinely singular RVs

The proof of this part of the theorem is an extension of [22, Theorem 1] to the affinely singular RVs with a bounded moment and differential entropy. To prove this part, we first show in the following Lemma that differential entropy is continuous in terms of additive Gaussian random vectors with infinitesimal Frobenious norm of covariance matrix.

Lemma 11: Let \mathbf{X} be an absolutely continuous RV with finite moment $\mathbb{E}[\|\mathbf{X}\|_\alpha^\beta]$ for some $\alpha, \beta \in \mathbb{R}^+$, and differential entropy $h(\mathbf{X}) > -\infty$. Also let $\{\mathbf{N}_i\}_i \in \mathbb{N}$ be a sequence of normal RVs with covariance matrices $\{\Sigma_i\}_i$. If

$$\lim_{i \rightarrow \infty} \|\Sigma_i\|_F = 0, \quad (125)$$

we have that

$$\lim_{i \rightarrow \infty} h(\mathbf{X} + \mathbf{N}_i) = h(\mathbf{X}). \quad (126)$$

Proof: Let $q = \min\{1, \beta\}$. One can bound $\mathbb{E}[\|\mathbf{X}\|_\alpha^q]$ as $\mathbb{E}[\|\mathbf{X}\|_\alpha^q] = \mathbb{E}[\|\mathbf{X}\|_\alpha^q | \|\mathbf{X}\|_\alpha \leq 1] \mathbb{P}(\|\mathbf{X}\|_\alpha \leq 1) + \mathbb{E}[\|\mathbf{X}\|_\alpha^q | \|\mathbf{X}\|_\alpha > 1] \mathbb{P}(\|\mathbf{X}\|_\alpha > 1)$ (127) $\leq 1 + \mathbb{E}[\|\mathbf{X}\|_\alpha^\beta | \|\mathbf{X}\|_\alpha > 1] \mathbb{P}(\|\mathbf{X}\|_\alpha > 1)$ (128) $\leq 1 + \mathbb{E}[\|\mathbf{X}\|_\alpha^\beta] < \infty$, (129)

where the last inequality holds because $\mathbb{E}[\|\mathbf{X}\|_\alpha^\beta] < \infty$. By setting $\tilde{d} = \max\{1, \alpha\}$, the norm inequality in [39, Lemma 2.1] shows that

$$\|\mathbf{v}\|_{\tilde{d}} \leq \|\mathbf{v}\|_\alpha, \quad (130)$$

for every vector \mathbf{v} , which concludes that

$$\mathbb{E}[\|\mathbf{X}\|_{\tilde{d}}^q] \leq \mathbb{E}[\|\mathbf{X}\|_\alpha^q] < \infty. \quad (131)$$

Further, for two-dimensional vectors $\mathbf{v}_1 = (\|\mathbf{X} + \mathbf{N}(D)\|_{\tilde{d}}, \|\mathbf{N}(D)\|_{\tilde{d}})^\top$, and $\mathbf{v}_2 = (\|\mathbf{X}\|_{\tilde{d}}, \|\mathbf{N}(D)\|_{\tilde{d}})^\top$, we have

$$\begin{aligned} \|\mathbf{X}\|_{\tilde{d}} &\stackrel{(a)}{\leq} \|\mathbf{X} + \mathbf{N}(D)\|_{\tilde{d}} + \|\mathbf{N}(D)\|_{\tilde{d}} \\ &\leq (\|\mathbf{X} + \mathbf{N}(D)\|_{\tilde{d}}^q + \|\mathbf{N}(D)\|_{\tilde{d}}^q)^{\frac{1}{q}}, \end{aligned} \quad (132)$$

and

$$\|\mathbf{X} + \mathbf{N}(D)\|_{\tilde{d}} \stackrel{(b)}{\leq} \|\mathbf{X}\|_{\tilde{d}} + \|\mathbf{N}(D)\|_{\tilde{d}}$$

$$\leq (\|\mathbf{X}\|_d^q + \|\mathbf{N}(D)\|_d^q)^{\frac{1}{q}}, \quad (133)$$

where (a) and (b) are followed by the triangle inequality for $\hat{d} \geq 1$, and the fact that $\|\cdot\|_1 \leq \|\cdot\|_q$ for $q = \min\{1, \beta\} \leq 1$ (again, see [39, Lemma 2.1]). Combining (132) and (133), we arrive at

$$-\|\mathbf{N}(D)\|_d^q \leq \|\mathbf{X} + \mathbf{N}(D)\|_d^q - \|\mathbf{X}\|_d^q \leq \|\mathbf{N}(D)\|_d^q, \quad (134)$$

and

$$\begin{aligned} & \mathbb{E}[\|\mathbf{X} + \mathbf{N}(D)\|_d^q] - \mathbb{E}[\|\mathbf{X}\|_d^q] \leq \mathbb{E}[\|\mathbf{N}(D)\|_d^q] \\ & \leq \mathbb{E}[\|\mathbf{N}(D)\|_1^q] \leq \mathbb{E}[\|\mathbf{N}(D)\|_q^q] = \sum_{i=1}^n \mathbb{E}[|N^i(D)|^q]. \end{aligned} \quad (135)$$

As $\mathbf{N}(D)$ is a normal random vector, each $N^i(D)$ is also a normal RV with standard deviation σ_i that satisfy

$$\sigma_i \leq \left(\sum_i \sigma_i^2 \right)^{1/2} \leq \|\Sigma(D)\|_F. \quad (136)$$

Using the bound in [40, Theorem 3] for the moments of a normal RV, we have

$$\mathbb{E}[|N^i(D)|^q] \leq \sigma_i^q \frac{2^{q/2} \Gamma(\frac{q+1}{2})}{\sqrt{\pi}} \leq \|\Sigma(D)\|_F^q \frac{2^{q/2} \Gamma(\frac{q+1}{2})}{\sqrt{\pi}}, \quad (137)$$

where $\Gamma(\cdot)$ is the Gamma function.

As a result of (135) and (137), and the assumption that $\lim_{D \rightarrow 0} \|\Sigma(D)\|_F = 0$, we have that

$$\lim_{D \rightarrow 0} \mathbb{E}[\|\mathbf{X} + \mathbf{N}(D)\|_d^q] = \mathbb{E}[\|\mathbf{X}\|_d^q]. \quad (138)$$

Finally, [6, Theorem 1] results in the desired claim as $h(\mathbf{X}) > -\infty$ (other requirements of this theorem are fulfilled due to (131) and (138)). ■

Now, we prove the second part of Theorem 4 in two parts: (i) first we find a lower bound for the \liminf and then (ii) we find an upper bound for the \limsup . The proof of the second part of Theorem 4 follows from the equality of the two bounds.

- **Step (i):** Using the definition of rate-distortion function, there exists a sequence $\{\hat{\mathbf{Z}}_{k,D}^m\}_{k \in \mathbb{N}}$ of m -dimensional RVs that

$$\lim_{k \rightarrow \infty} I(\mathbf{Z}^m; \hat{\mathbf{Z}}_{k,D}^m) = R_2(\mathbf{Z}^m, D), \quad (139)$$

and

$$\mathbb{E}[\|\mathbf{Z}^m - \hat{\mathbf{Z}}_{k,D}^m\|_2^2] \leq D. \quad (140)$$

Next, because $\mathbf{Z}^{(i)}$'s are mutually singular, V_m is a function of \mathbf{Z}^m with probability 1. As a result, one has

$$I(\mathbf{Z}^m; \hat{\mathbf{Z}}_{k,D}^m) = I(\mathbf{Z}^m, V_m; \hat{\mathbf{Z}}_{k,D}^m) \quad (141)$$

$$= I(V_m; \hat{\mathbf{Z}}_{k,D}^m) + I(\mathbf{Z}^m; \hat{\mathbf{Z}}_{k,D}^m | V_m) \quad (142)$$

$$= I(V_m; \hat{\mathbf{Z}}_{k,D}^m) + \sum_{i=1}^{\infty} p_i I(\mathbf{Z}^{(i)}; \hat{\mathbf{Z}}_{k,D}^{(i)}), \quad (143)$$

where $\hat{\mathbf{Z}}_{k,D}^{(i)}$ is a RV with the probability measure equal to the conditional probability measure of $\hat{\mathbf{Z}}_{k,D}^m$ given $V_m = i$.

If $e_i = 0$ for a selection $V_m = i$, then we have

$$0 \leq I(\mathbf{Z}^{(i)}; \hat{\mathbf{Z}}_{k,D}^{(i)}) \leq H(\mathbf{Z}^{(i)}) = 0. \quad (144)$$

Next, by assuming $e_i \neq 0$ we bound each expression in (143). First, we claim that

$$\liminf_{D \rightarrow 0} \liminf_{k \rightarrow \infty} I(V_m; \hat{\mathbf{Z}}_{k,D}^m) \geq H(V_m). \quad (145)$$

The reason is that for every $\epsilon \in \mathbb{R}^+$, there exists $\tilde{k}(D, \epsilon) \in \mathbb{N}$ such that

$$\liminf_{k \rightarrow \infty} I(V_m; \hat{\mathbf{Z}}_{k,D}^m) \geq I(V_m; \hat{\mathbf{Z}}_{\tilde{k}(D, \epsilon), D}^m) - \epsilon. \quad (146)$$

As for any $D > 0$ we know that $\mathbb{E}[\|\mathbf{Z}^m - \hat{\mathbf{Z}}_{\tilde{k}(D, \epsilon), D}^m\|^2] \leq D$, we conclude that $(V_m; \hat{\mathbf{Z}}_{\tilde{k}(D, \epsilon), D}^m)$ converges to $(V_m; \mathbf{Z}^m)$ in mean (also in distribution) for any sequence $\{D_t\}_{t \in \mathbb{N}}$ with $D_t \xrightarrow{t \rightarrow \infty} 0$. Recalling the lower semi-continuity property of the mutual information (see [41, Eqn. 3.13]), we can write

$$\liminf_{t \rightarrow \infty} I(V_m; \hat{\mathbf{Z}}_{\tilde{k}(D_t, \epsilon), D_t}^m) \geq I(V_m; \mathbf{Z}^m). \quad (147)$$

Now, by combining (146) and (147), we conclude that

$$\liminf_{D \rightarrow 0} \liminf_{k \rightarrow \infty} I(V_m; \hat{\mathbf{Z}}_{k,D}^m) \geq I(V_m; \mathbf{Z}^m) - \epsilon \quad (148)$$

$$= H(V_m) - \epsilon. \quad (149)$$

As (149) holds for all $\epsilon > 0$, we can use $\epsilon \rightarrow 0$ and (145) is immediate.

Second, using the fact that an invertible function preserves the mutual information, we have

$$I(\mathbf{Z}^{(i)}; \hat{\mathbf{Z}}_{k,D}^{(i)}) = I(\mathbf{C}_i; U^\dagger(\hat{\mathbf{Z}}_{k,D}^{(i)} - \mathbf{b}_i)). \quad (150)$$

By defining the first e_i elements of $U^\dagger(\hat{\mathbf{Z}}_{k,D}^{(i)} - \mathbf{b}_i)$ as $\tilde{\mathbf{Z}}_{k,D}^{(i)}$ and, we can rewrite (150) as

$$\begin{aligned} I(\mathbf{Z}^{(i)}; \hat{\mathbf{Z}}_{k,D}^{(i)}) & \stackrel{(a)}{\geq} I(\mathbf{C}_i; \tilde{\mathbf{Z}}_{k,D}^{(i)}) \\ & = h(\mathbf{C}_i) - h(\mathbf{C}_i | \tilde{\mathbf{Z}}_{k,D}^{(i)}) \\ & = h(\mathbf{C}_i) - h(\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)} | \tilde{\mathbf{Z}}_{k,D}^{(i)}) \\ & \stackrel{(b)}{\geq} h(\mathbf{C}_i) - \frac{e_i}{2} \log \frac{2\pi e \mathbb{E}[\|\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)}\|_2^2]}{e_i}, \end{aligned} \quad (151)$$

where (a) holds due to the fact that dropping a RV from one side of the mutual information, decrease its value. The validity of (b) is also because of the decreasing property of differential entropy with conditioning; besides, the Gaussian RV with i.i.d. components maximizes the differential entropy among all RVs with the second-order moment constraint.

Moreover, we know that

$$\begin{aligned} \|\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)}\|_2^2 & \leq \|(\mathbf{C}_i^\top, \underbrace{0, \dots, 0}_{m-e_i})^\top - U^\dagger(\hat{\mathbf{Z}}_{k,D}^{(i)} - \mathbf{b}_i)\|_2^2 \\ & \stackrel{(a)}{=} \|\mathbf{Z}^{(i)} - \hat{\mathbf{Z}}_{k,D}^{(i)}\|_2^2, \end{aligned} \quad (152)$$

where (a) is correct because multiplication by a unitary matrix preserves the Euclidean norm of a vector. Using this inequality,

we have

$$\sum_{i=1}^{\infty} p_i \mathbb{E}[\|\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)}\|_2^2] \leq \sum_{i=1}^{\infty} p_i \mathbb{E}[\|\mathbf{Z}^{(i)} - \hat{\mathbf{Z}}_{k,D}^{(i)}\|_2^2] \leq D, \quad (153)$$

where the last inequality follows from (140), and the definition of $\mathbf{Z}^{(i)}$ and $\hat{\mathbf{Z}}_{k,D}^{(i)}$. We recall the log-sum inequality as

$$\sum_i a_i \log \frac{b_i}{a_i} \leq a \log \frac{b}{a}, \quad (154)$$

where a_i, b_i are arbitrary non-negative reals, $a = \sum_i a_i$ and $b = \sum_i b_i$. Thus, if we set $a_i = p_i e_i$ and $b_i = 2\pi e p_i \mathbb{E}[\|\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)}\|_2^2]$, the log-sum inequality (154) implies that

$$\begin{aligned} & \sum_{i=1, e_i \neq 0}^{\infty} \frac{p_i e_i}{2} \log \frac{2\pi e \mathbb{E}[\|\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)}\|_2^2]}{e_i} \\ & \leq \frac{\sum_{i=1, e_i \neq 0}^{\infty} p_i e_i}{2} \log \frac{2\pi e \sum_{i=1}^{\infty} p_i \mathbb{E}[\|\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)}\|_2^2]}{\sum_{i=1, e_i \neq 0}^{\infty} p_i e_i} \\ & \leq \frac{d(\mathbf{Z}^m)}{2} \log \frac{2\pi e \sum_{i=1}^{\infty} p_i \mathbb{E}[\|\mathbf{C}_i - \tilde{\mathbf{Z}}_{k,D}^{(i)}\|_2^2]}{d(\mathbf{Z}^m)} \\ & \stackrel{(a)}{\leq} \frac{d(\mathbf{Z}^m)}{2} \log \frac{2\pi e D}{d(\mathbf{Z}^m)}, \end{aligned} \quad (155)$$

where $d(\mathbf{Z}^m) = \sum_i p_i e_i$ and (a) is due to (153). As a result of (139), (143), (151), and (155) one has

$$\begin{aligned} & R_2(\mathbf{Z}^m, D) \\ & \geq \liminf_{k \rightarrow \infty} I(V_m; \hat{\mathbf{Z}}_{k,D}^m) + \sum_{i=1}^{\infty} p_i h(\mathbf{C}_i) \\ & \quad - \frac{d(\mathbf{Z}^m)}{2} \log \frac{2\pi e D}{d(\mathbf{Z}^m)}. \end{aligned} \quad (156)$$

Finally, by combining (145) and (156) we conclude that

$$\begin{aligned} & \liminf_{D \rightarrow 0} \left(R_2(\mathbf{Y}^m, D) + \frac{d(\mathbf{Z}^m)}{2} \log \frac{2\pi e D}{d(\mathbf{Z}^m)} \right) \\ & \geq H(V_m) + \sum_{i=1}^{\infty} p_i h(\mathbf{C}_i). \end{aligned} \quad (157)$$

- **Step (ii):** To upper-bound the QRDF of \mathbf{Z}^m , if $e_i \neq 0$, we perturb the RV with a Gaussian noise of (vector) variance D . Then, we upper-bound the mutual information between the original and the perturbed versions. More specifically, assume that

$$\hat{\mathbf{Z}}^{(i)} = \mathbf{Z}^{(i)} + U_i(\mathbf{N}_i^T, \underbrace{0, \dots, 0}_{m-e_i})^T, \quad (158)$$

where \mathbf{N}_i is an e_i -dimensional Gaussian RV with zero-mean i.i.d. elements and element-wise variance $\frac{D}{d(\mathbf{Z}^m)}$. Besides, \mathbf{N}_i and \mathbf{N}_j are independent of each other for $i \neq j$. We further define $\hat{\mathbf{Z}}^m$ as

$$\hat{\mathbf{Z}}^m = \sum_{i=1}^{\infty} \mathbb{1}_{V_m=i} \hat{\mathbf{Z}}^{(i)}. \quad (159)$$

Now, we have

$$\begin{aligned} \mathbb{E}[\|\mathbf{Z}^m - \hat{\mathbf{Z}}^m\|_2^2] &= \sum_{i=1}^{\infty} p_i \mathbb{E}[\|\mathbf{Z}^{(i)} - \hat{\mathbf{Z}}^{(i)}\|_2^2] \\ &= \sum_{i=1, e_i \neq 0}^{\infty} p_i \mathbb{E}[\|\mathbf{N}_i\|_2^2] = \sum_{i=1}^{\infty} p_i \frac{e_i D}{d(\mathbf{Z}^m)} = D, \end{aligned} \quad (160)$$

where the last identity holds because

$$d(\mathbf{Z}^m) = \sum_{i=1, e_i \neq 0}^{\infty} p_i e_i = \sum_{i=1}^{\infty} p_i e_i. \quad (162)$$

Hence, we shall have that

$$R(\mathbf{Z}^m, D) \leq I(\mathbf{Z}^m; \hat{\mathbf{Z}}^m). \quad (163)$$

Using the same steps as in (143), we have that

$$I(\mathbf{Z}^m; \hat{\mathbf{Z}}^m) = I(V_m; \hat{\mathbf{Z}}^m) + \sum_{i=1}^{\infty} p_i I(\mathbf{Z}^{(i)}; \hat{\mathbf{Z}}^{(i)}). \quad (164)$$

For the first term, using (161) and [22, Lemma 3], we can write that

$$\lim_{D \rightarrow 0} I(V_m; \hat{\mathbf{Z}}^m) = H(V_m). \quad (165)$$

For the second term in (164), using the fact that an invertible function preserves the value of mutual information, we have that

$$\begin{aligned} I(\mathbf{Z}^{(i)}; \hat{\mathbf{Z}}^{(i)}) &= I(\mathbf{C}_i; \mathbf{C}_i + \mathbf{N}_i) \\ &= h(\mathbf{C}_i + \mathbf{N}_i) - h(\mathbf{C}_i + \mathbf{N}_i | \mathbf{C}_i) \\ &= h(\mathbf{C}_i + \mathbf{N}_i) - h(\mathbf{N}_i | \mathbf{C}_i) \\ &\stackrel{(a)}{=} h(\mathbf{C}_i + \mathbf{N}_i) - h(\mathbf{N}_i), \\ &= h(\mathbf{C}_i + \mathbf{N}_i) - \frac{e_i}{2} \log \frac{2\pi e D}{d(\mathbf{Z}^m)} \end{aligned} \quad (166)$$

where (a) is true because \mathbf{C}_i is independent of \mathbf{N}_i . Now, using the assumption that $h(\mathbf{C}_i) > -\infty$ and the fact that $\mathbb{E}[\|\mathbf{C}_i\|_{\alpha}^{\beta}] < \infty$ (otherwise, $\mathbb{E}[\|\mathbf{Z}^m\|_{\alpha}^{\beta}] = \infty$), we conclude from Lemma 11 that

$$\lim_{D \rightarrow 0} h(\mathbf{C}_i + \mathbf{N}_i) = h(\mathbf{C}_i). \quad (167)$$

Finally, by combining (161)-(167), we prove that

$$\begin{aligned} & \limsup_{D \rightarrow 0} \left(R_2(\mathbf{Z}^m, D) + \frac{d(\mathbf{Z}^m)}{2} \log \frac{2\pi e D}{d(\mathbf{Z}^m)} \right) \\ & \leq H(V_m) + \sum_{i=1}^{\infty} p_i h(\mathbf{C}_i). \end{aligned} \quad (168)$$

Since the lower and upper-bounds in (157) and (168), respectively, coincide, the proof is complete.

APPENDIX C PROOF OF THEOREM 5

We obtain the RID and DRB of a linear transformation of orthogonally singular RVs in the following sections, respectively.

A. RID of linear transformations of orthogonally singular RVs

Using Lemma 3 (which shall be proved later), we know that \mathbf{Y}^m has an affinely singular measure as in (24) with $V_m = \Upsilon_m$, and $\mathbf{Z}^{(i)} = \tilde{\mathbf{Y}}^{(i)}$ for $i \in \mathbb{N}$. In particular, for each

$$\boldsymbol{\nu}_0 \in \bigcup_{(\boldsymbol{\nu}, \mathbf{x}_d) \in \mathcal{T}_i^{(m)}} \boldsymbol{\nu},$$

the support of \mathbf{Y}^m contains an affine subspace with dimension $e_0 = \text{rank}(A_m^{[\boldsymbol{\nu}_0]})$; the set $\mathcal{T}_i^{(m)}$ was defined in Section VII-C.

Let Υ_m be the RV defined in (31). We first show that $H(\Upsilon_m) < \infty$. Using the definition of $\Upsilon_m^{(i)}$ defined in (32) we have that

$$\begin{aligned} & -\mathbb{P}(\Upsilon_m = i) \log \mathbb{P}(\Upsilon_m = i) \\ & \leq -\mathbb{P}(\Upsilon_m = i) \log \mathbb{P}(\Upsilon_m = i) + \mathbb{P}(\Upsilon_m = i) H(\Upsilon_m^{(i)}) \\ & = - \sum_{(\mathbf{s}, \mathbf{x}_d^{\bar{s}}) \in \mathcal{T}_i^{(m)}} \mathbb{P}_{\boldsymbol{\nu}, \mathbf{x}_d^{\bar{s}}}(\mathbf{s}, \mathbf{x}_d^{\bar{s}}) \log \mathbb{P}_{\boldsymbol{\nu}, \mathbf{x}_d^{\bar{s}}}(\mathbf{s}, \mathbf{x}_d^{\bar{s}}). \end{aligned}$$

As a result, we can write that

$$\begin{aligned} H(V) & \leq H(\boldsymbol{\nu}) + \sum_{\mathbf{s} \in \{0,1\}^d} H(\mathbf{X}_d^{\bar{s}} | \boldsymbol{\nu} = \mathbf{s}) \mathbb{P}(\boldsymbol{\nu} = \mathbf{s}) \\ & \leq H(\boldsymbol{\nu}) + \sum_{\mathbf{s} \in \{0,1\}^d} H(\mathbf{X}_d | \boldsymbol{\nu} = \mathbf{s}) \mathbb{P}(\boldsymbol{\nu} = \mathbf{s}) \\ & = H(\boldsymbol{\nu}, \mathbf{X}_d). \end{aligned}$$

Since $H(\boldsymbol{\nu}, \mathbf{X}_d) < \infty$ by assumption, we conclude that $H(\Upsilon_m) < \infty$. We now recall Theorem 4 to conclude the claim that

$$d(\mathbf{Y}^m) = \mathbb{E}_{\boldsymbol{\nu}}[\text{rank}(A_m^{[\boldsymbol{\nu}]})]. \quad (169)$$

B. DRB of linear transformations of orthogonally singular RVs

Here, we first prove the following Lemma that states the conditions by means of which $h(A_m \mathbf{X}^n)$ is lower bounded.

Lemma 12: Let \mathbf{X}^n for $n \in \mathbb{N}$ be an RV with $\mathbb{E}[\|\mathbf{X}^n\|_{\alpha}^{\beta}] < \infty$. If A_m is a full-rank $k \times n$ matrix, and \mathbf{X}^n is an absolutely continuous RV with $h(\mathbf{X}^n) > -\infty$, then $h(A_m \mathbf{X}^n) > -\infty$.

Proof: We use the singular value decomposition A_m as

$$A_m = U D V_k^{\dagger}, \quad (170)$$

where U is a unitary $k \times k$ matrix, D is $k \times k$ diagonal matrix and V_k is a $n \times k$ matrix (incomplete unitary matrix). Indeed, V_k is formed by the first columns of the unitary matrix V

$$V = [V_k, V_{k+1,n}]. \quad (171)$$

Using the properties of the differential entropy we know that

$$h(A_m \mathbf{X}^n) = h(V_k^{\dagger} \mathbf{X}^n) + \sum_{i=1}^k \log \sigma_i, \quad (172)$$

where σ_i s are the singular values, and due to the full-rank property of A_m , they are strictly positive. Hence, $h(A_m \mathbf{X}^n) > -\infty$ is equivalent to

$$h(V_k^{\dagger} \mathbf{X}^n) > -\infty. \quad (173)$$

By employing the rotation-invariance property of the differential entropy, we know that

$$\begin{aligned} h(\mathbf{X}^n) & = h(V^{\dagger} \mathbf{X}^n) = h(V_{k+1,n}^{\dagger} \mathbf{X}^n, V_k^{\dagger} \mathbf{X}^n) \\ & \leq h(V_{k+1,n}^{\dagger} \mathbf{X}^n) + h(V_k^{\dagger} \mathbf{X}^n). \end{aligned} \quad (174)$$

Moreover, we have that

$$\mathbb{E}[\|V_{k+1,n}^{\dagger} \mathbf{X}^n\|_{\alpha}^{\beta}] \leq \|V_{k+1,n}\|_{\alpha}^{\beta} \mathbb{E}[\|\mathbf{X}^n\|_{\alpha}^{\beta}] \quad (176)$$

$$\stackrel{(a)}{\leq} n \frac{\beta(1+\alpha)}{\alpha} \mathbb{E}[\|\mathbf{X}^n\|_{\alpha}^{\beta}], \quad (177)$$

where $\|V_{k+1,n}\|_{\alpha}$ is the operator norm of matrix $V_{k+1,n}$ induced by vector α -norm, and (a) is due to (190). Using [6, Corollary 1], we conclude that

$$h(V_{k+1,n}^{\dagger} \mathbf{X}^n) \leq \log M, \quad (178)$$

where

$$M = V_{\alpha, n-k} \cdot \left(\frac{\alpha \cdot e \cdot n^{\frac{\beta(1+\alpha)}{\alpha}} \mathbb{E}[\|\mathbf{X}^n\|_{\alpha}^{\beta}]}{n-k} \right)^{\frac{n-k}{\beta}} \cdot \Gamma\left(1 + \frac{n-k}{\beta}\right), \quad (179)$$

$V_{\alpha, n-k}$ is the volume of the α -norm unit-ball in $(n-k)$ dimensions, and $\Gamma(\cdot)$ is the Gamma function.

Since $h(\mathbf{X}^n) > -\infty$, (178) induces a lower-bound on $h(V_k^{\dagger} \mathbf{X}^n)$ via (175), which completes the proof. ■

Now, we divide the proof of the second part of Theorem 5 in three steps: (i) we first show that $h(\tilde{\mathbf{Y}}_i) > -\infty$, (ii) then, we prove that $\mathbb{E}[\|\mathbf{Y}^m\|_{\alpha}^{\beta}] < \infty$, and (iii) finally, we utilize Theorem 4 to complete the proof.

- **Step (i):** Using (33) and (35) one can see that

$$h(\tilde{\mathbf{Y}}_i | \Upsilon_m^{(i)} = (\mathbf{s}, \mathbf{x}_d^{\bar{s}})) = h(B_{\mathbf{s}} \mathbf{X}_c^{\bar{s}}). \quad (180)$$

Here, $B_{\mathbf{s}} = \tilde{D}_{\mathbf{s}} U_{\mathbf{s}}^{\dagger}$, and $U_{\mathbf{s}}^{\dagger}$ and $\tilde{D}_{\mathbf{s}}$ were previously defined in Section VII-C. It is not difficult to verify that $B_{\mathbf{s}}$ is a full row rank matrix. Besides, the RHS in (180) is invariant to $\mathbf{x}_d^{\bar{s}}$. As a result, we have

$$h(\tilde{\mathbf{Y}}_i) \geq h(\tilde{\mathbf{Y}}_i | \Upsilon_m^{(i)}) \quad (181)$$

$$= \sum_{(\mathbf{s}, \mathbf{x}_d^{\bar{s}}) \in \mathcal{T}_i^{(m)}} \mathbb{P}(\Upsilon_m^{(i)} = (\mathbf{s}, \mathbf{x}_d^{\bar{s}})) h(\tilde{\mathbf{Y}}_i | \Upsilon_m^{(i)} = (\mathbf{s}, \mathbf{x}_d^{\bar{s}})) \quad (182)$$

$$= \sum_{\mathbf{s} \in \{0,1\}^n} \mathbb{P}(\boldsymbol{\nu} = \mathbf{s}) h(B_{\mathbf{s}} \mathbf{X}_c^{\bar{s}}). \quad (183)$$

Next, we form $B_{\mathbf{s}, \text{aug}}$ with n columns by including the columns of $B_{\mathbf{s}}$ in places where \mathbf{s} is equal to 1; the rest of the columns are zero (corresponding to zero locations in \mathbf{s}). In this way, we are able to write

$$B_{\mathbf{s}} \mathbf{X}_c^{\bar{s}} = B_{\mathbf{s}, \text{aug}} \mathbf{X}_c. \quad (184)$$

Since $B_{\mathbf{s}}$ is of full row rank, $B_{\mathbf{s}, \text{aug}}$ has also full row rank (some zeros with fixed pattern are inserted within the rows). Hence, by using Lemma 12, $h(\mathbf{X}_c) > -\infty$, and $\mathbb{E}[\|\mathbf{X}_c\|_{\alpha}^{\beta}] < \infty$ we have that

$$h(B_{\mathbf{s}} \mathbf{X}_c^{\bar{s}}) = h(B_{\mathbf{s}, \text{aug}} \mathbf{X}_c) > -\infty. \quad (185)$$

In addition, \mathbf{s} is a discrete RV with at most 2^n possible values, hence

$$h(\tilde{\mathbf{Y}}_i) \geq \min_{\mathbf{s}} h(B_{\mathbf{s}} \mathbf{X}_c^{\mathbf{s}}) > -\infty. \quad (186)$$

• **Step (ii):** We can bound $\|\mathbf{X}\|_{\alpha}^{\beta}$ as

$$\begin{aligned} \|\mathbf{X}^n\|_{\alpha}^{\beta} &= \left(\sum_{i=1}^n |X_i|^{\alpha} \right)^{\beta/\alpha} \\ &\stackrel{(a)}{=} \left(\sum_{i=1}^n \nu_i |X_{c,i}|^{\alpha} + (1 - \nu_i) |X_{d,i}|^{\alpha} \right)^{\beta/\alpha} \\ &\leq (\|\mathbf{X}_c\|_{\alpha}^{\alpha} + \|\mathbf{X}_d\|_{\alpha}^{\alpha})^{\beta/\alpha}. \end{aligned} \quad (187)$$

where (a) is because of the definition of \mathbf{X}^n in (2).

Further, general equivalence of norms in finite-dimensional spaces (e.g., see [42, pp. 517]) deduces that

$$\|\mathbf{v}\|_1 \leq C_q \|\mathbf{v}\|_q, \quad (188)$$

for a scalar $C_q \in \mathbb{R}^+$. Hence, by setting $q = \frac{\beta}{\alpha}$ and $\mathbf{v}_{2 \times 1} = (\|\mathbf{X}_c\|_{\alpha}^{\alpha}, \|\mathbf{X}_d\|_{\alpha}^{\alpha})^{\top}$, (187) and (188) imply that

$$\begin{aligned} \|\mathbf{X}^n\|_{\alpha}^{\beta} &\leq C_{\beta/\alpha} (\|\mathbf{X}_c\|_{\alpha}^{\beta} + \|\mathbf{X}_d\|_{\alpha}^{\beta}) \\ \Rightarrow \mathbb{E}[\|\mathbf{X}^n\|_{\alpha}^{\beta}] &\leq C_{\beta/\alpha} (\mathbb{E}[\|\mathbf{X}_c\|_{\alpha}^{\beta}] + \mathbb{E}[\|\mathbf{X}_d\|_{\alpha}^{\beta}]). \end{aligned} \quad (189)$$

Hence, since $\mathbb{E}[\|\mathbf{X}_d\|_{\alpha}^{\beta}], \mathbb{E}[\|\mathbf{X}_c\|_{\alpha}^{\beta}] < \infty$, we have $\mathbb{E}[\|\mathbf{X}^n\|_{\alpha}^{\beta}] < \infty$. Thus, with $\mathbf{Y}^m = A_m \mathbf{X}^n$, we know that $\mathbb{E}[\|\mathbf{Y}^m\|_{\alpha}^{\beta}] < \|A_m\|_{\alpha}^{\beta} \mathbb{E}[\|\mathbf{X}^n\|_{\alpha}^{\beta}] < \infty$, where $\|A_m\|_{\alpha}$ is an operator norm of matrix A_m induced by vector α -norm. This inequality is followed by the fact that

$$\|A_m\|_{\alpha} \leq \|A_m\|_{\alpha, \infty} \leq m^{1/\alpha} n \max_{i,j} |a_{ij}|, \quad (190)$$

for $A_m = [a_{ij}]$, where $\|A_m\|_{\alpha, \infty}$ denotes (α, ∞) -subordinate norm defined as

$$\|A_m\|_{\alpha, \infty} = \max_{\mathbf{x}^n \neq \mathbf{0}} \frac{\|A_m \mathbf{x}^n\|_{\alpha}}{\|\mathbf{x}\|_{\infty}}. \quad (191)$$

• **Step (iii):** The claim easily follows from Theorem 4 if we substitute $\mathbf{Y}^m \rightarrow \mathbf{Z}^m$, $\tilde{\mathbf{Y}}_i \rightarrow \mathbf{C}_i$, and $V \rightarrow V_m$, where $\tilde{\mathbf{Y}}_i$ and V are defined in (35) and (31), respectively.

APPENDIX D PROOF OF LEMMA 5

Since f is a Lipschitz function, $g_{\mathbf{x}_{\bar{v}}}(\cdot)$ defined via

$$g_{\mathbf{x}_{\bar{v}}}(\mathbf{X}_{\nu}) = f(\mathbf{X}_{\nu}, \mathbf{x}_{\bar{v}}) \quad (192)$$

is also a Lipschitz function. Thus, by using [33, Theorem 2], we achieve³

$$\bar{d}(f(\mathbf{X}_{\nu}, \mathbf{x}_{\bar{v}})) \leq \sum_{i=1}^n \nu_i. \quad (193)$$

Alternatively, [3, Eqn. 80] shows that

$$\bar{d}(f(\mathbf{X}_{\nu}, \mathbf{x}_{\bar{v}})) \leq m. \quad (194)$$

Now, by combining [33, Theorem 5], (193), and (194) we conclude that

$$\begin{aligned} \bar{d}(f(\mathbf{X}^n)) &\leq \mathbb{E}_{\nu} \left[\min \left\{ \sum_{i=1}^n \nu_i, m \right\} \right] \\ &= d(A_m \mathbf{X}^n), \end{aligned} \quad (195)$$

where the last equality follows from Theorem 5 and equation (54).

APPENDIX E PROOF OF PROPOSITION 1

To prove this proposition, first we show that for a binary vector \mathbf{s} , we have $\text{rank}(A^{[\mathbf{s}]}) = \min\{m, \sum_{i=1}^n s_i\}$ with probability 1. The reason is twofold. First, it is proved that a polynomial is either trivial (i.e., $p(x) = 0$ everywhere) or the set of its roots is zero Lebesgue measure. As a result, the determinant of a square matrix with i.i.d continuous random variables is zero with probability 0, because joint probability measure of i.i.d continuous random variables is absolutely continuous w.r.t the Lebesgue measure, and the determinant is a polynomial function of the matrix elements. In other words, every k number of m -dimensional vectors with i.i.d continuous random variables are linearly independent with probability 1, if we have $k \leq m$. As a result, in the case that $\sum_{i=1}^n s_i \leq m$, we have $\text{rank}(A^{[\mathbf{s}]}) = \sum_{i=1}^n s_i$ with probability 1. On the other hand, if $\sum_{i=1}^n s_i > m$, the above discussion shows that every sub-matrix of $A^{[\mathbf{s}]}$ with m number of columns is full-rank with probability 1. Finally, since $\text{rank}(A^{[\mathbf{s}]})$ is bounded by its number of rows m , one sees that $\text{rank}(A^{[\mathbf{s}]}) = m$ with probability 1. This proves the claim $\text{rank}(A^{[\mathbf{s}]}) = \min\{m, \sum_{i=1}^n s_i\}$.

Next, we show that $\frac{1}{m} d(A \mathbf{X}^n) \rightarrow \min\{1, \frac{p}{r}\}$. Firstly, Theorem 5 shows that

$$\frac{1}{m} d(A \mathbf{X}^n) = \mathbb{E}_{\nu} \left[\frac{1}{m} \text{rank}(A^{[\nu]}) \right] = \mathbb{E}_{\nu} \left[\min \left\{ 1, \frac{\sum_{i=1}^n \nu_i}{m} \right\} \right], \quad (196)$$

where the last equality is followed by the above discussion. By conditioning on whether $\sum_{i=1}^n \nu_i \leq m$ or not, we have

$$\begin{aligned} \frac{1}{m} d(A \mathbf{X}^n) &= \mathbb{P} \left(\sum_{i=1}^n \nu_i > m \right) \\ &\quad + \mathbb{E}_{\nu} \left[\frac{\sum_{i=1}^n \nu_i}{m} \mid \sum_{i=1}^n \nu_i \leq m \right] \mathbb{P} \left(\sum_{i=1}^n \nu_i \leq m \right), \end{aligned} \quad (197)$$

In the case that $p \geq r$, the proportion $\frac{\sum_{i=1}^n \nu_i}{m}$ concentrates around $\frac{p}{r} \geq 1$, which concludes that $\mathbb{P}(\sum_{i=1}^n \nu_i \leq m) \rightarrow 0$. Furthermore, $\mathbb{E}_{\nu} \left[\frac{\sum_{i=1}^n \nu_i}{m} \mid \sum_{i=1}^n \nu_i \leq m \right]$ is bounded by $\frac{1}{r}$. As a result, asymptotically we have $\frac{1}{m} d(A \mathbf{X}^n) \rightarrow 1$.

In a case that $p < r$, we rewrite 197 as

$$\begin{aligned} \frac{1}{m} d(A \mathbf{X}^n) &= \mathbb{P} \left(\sum_{i=1}^n \nu_i > m \right) \cdot \underbrace{\left(1 - \mathbb{E}_{\nu} \left[\frac{\sum_{i=1}^n \nu_i}{m} \mid \sum_{i=1}^n \nu_i > m \right] \right)}_A \end{aligned}$$

³The direction of the inequality is misprinted in the referenced theorem.

$$+ \mathbb{E}_\nu \left[\frac{\sum_{i=1}^n \nu_i}{m} \right]. \quad (198)$$

Here, with the same reasoning as in the other case, we have $\mathbb{P}(\sum_{i=1}^n \nu_i > m) \rightarrow 0$. Further, the term A is upper- and lower-bounded by 1 and $1 - \frac{1}{r}$, respectively. Moreover, the average of Bernoulli random variables $\mathbb{E}_\nu \left[\frac{\sum_{i=1}^n \nu_i}{m} \right]$ converges to $\frac{p}{r}$. This proves that $\frac{1}{m} d(\mathbf{A}\mathbf{X}^n) \rightarrow \frac{p}{r}$. These two cases show that $\frac{1}{m} d(\mathbf{A}\mathbf{X}^n) \rightarrow \min\{1, \frac{p}{r}\}$.

APPENDIX F PROOF OF LEMMA 6

We prove two parts of this lemma (direct part and converse) as follows.

First, we assume that $\mu_{\mathbf{Y}}(\cdot)$ is an affinely singular probability measure on set $\mathcal{S}_{\mathbf{Y}} \subseteq \mathcal{S}_{\mathbf{X}}$ of affine subsets, and each of its measures $\mu_{\mathbf{Y}}^{\mathcal{A}}$ on set $\mathcal{A} \in \mathcal{S}_{\mathbf{Y}}$ is absolutely continuous with respect to $\mu_{\mathbf{X}}^{\mathcal{A}}$. Then, for any set \mathcal{C} , if we have

$$\mu_{\mathbf{X}}(\mathcal{C}) = 0 = \sum_i p_i \mu_{\mathbf{X}}^{\mathcal{A}_i}(\mathcal{C} \cap \mathcal{A}_i), \quad (199)$$

one concludes that

$$\mu_{\mathbf{X}}^{\mathcal{A}_i}(\mathcal{C} \cap \mathcal{A}_i) = 0, \quad (200)$$

for every $\mathcal{A}_i \in \mathcal{S}_{\mathbf{X}}$. Next, because of absolute continuity of $\mu_{\mathbf{Y}}^{\mathcal{A}_i}$ with respect to $\mu_{\mathbf{X}}^{\mathcal{A}_i}$, we have

$$\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\mathcal{C} \cap \mathcal{A}_i) = 0, \quad (201)$$

that results in

$$\mu_{\mathbf{Y}}(\mathcal{C}) = \sum_i q_i \mu_{\mathbf{Y}}^{\mathcal{A}_i}(\mathcal{C} \cap \mathcal{A}_i) = 0. \quad (202)$$

Note that since $\mathcal{S}_{\mathbf{Y}} \subseteq \mathcal{S}_{\mathbf{X}}$, then q_i s could get zero values. The above identity shows that $\mu_{\mathbf{Y}}(\cdot)$ is absolutely continuous with respect to $\mu_{\mathbf{X}}(\cdot)$.

Secondly, we assume that $\mu_{\mathbf{Y}}(\cdot)$ is absolutely continuous with respect to $\mu_{\mathbf{X}}(\cdot)$. We order \mathcal{A}_i s in a way that e_i is increasing with i . Then, we define \mathcal{B}_i as

$$\mathcal{B}_i := \mathcal{A}_i \setminus \cup_{j=1}^{i-1} \mathcal{A}_j.$$

One can see that based on such definition, we have $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$, where $i \neq j$, and $\cup_i \mathcal{B}_i = \cup_i \mathcal{A}_i$.

Next, for every set \mathcal{C} , we have

$$\mu_{\mathbf{Y}}(\mathcal{C}) = \mu_{\mathbf{Y}}(\mathcal{C} \cap \cup_i \mathcal{B}_i) + \mu_{\mathbf{Y}}(\mathcal{C} \setminus \cup_i \mathcal{B}_i) \quad (203)$$

$$\stackrel{(a)}{=} \mu_{\mathbf{Y}}(\mathcal{C} \cap \cup_i \mathcal{B}_i) \quad (204)$$

$$\stackrel{(b)}{=} \sum_i \mu_{\mathbf{Y}}(\mathcal{C} \cap \mathcal{B}_i), \quad (205)$$

where (a) holds because $\mu_{\mathbf{Y}}(\cdot)$ is absolutely continuous with respect to $\mu_{\mathbf{X}}(\cdot)$, and $\mu_{\mathbf{X}}(\mathcal{C} \setminus \cup_i \mathcal{B}_i) = 0$, and (b) is followed by mutual exclusion of \mathcal{B}_i s.

Now, we define q_i and $\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\cdot)$ as

$$q_i := \mu_{\mathbf{Y}}(\mathcal{B}_i), \quad (206)$$

and

$$\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\cdot) = \frac{\mu_{\mathbf{Y}}(\cdot \cap \mathcal{B}_i)}{\mu_{\mathbf{Y}}(\mathcal{B}_i)}, \quad (207)$$

if $q_i \neq 0$. One can check that $\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\cdot)$ is a probability measure. Further, since $\mu_{\mathbf{Y}}(\cdot \cap \mathcal{B}_i)$ is absolutely continuous with respect to $\mu_{\mathbf{X}}(\cdot \cap \mathcal{B}_i)$, and $\mu_{\mathbf{X}}(\cdot \cap \mathcal{B}_i)$ is absolutely continuous with respect to the Lebesgue measure on \mathcal{B}_i , and because of transitivity of absolute continuity, one can see that $\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\cdot)$ is absolutely continuous with respect to the Lebesgue measure on \mathcal{B}_i . Hence, one can write $\mu_{\mathbf{Y}}(\mathcal{C})$ as

$$\mu_{\mathbf{Y}}(\mathcal{C}) = \sum_i q_i \mu_{\mathbf{Y}}^{\mathcal{A}_i}(\mathcal{C} \cap \mathcal{B}_i), \quad (208)$$

for a set of absolutely continuous probability measures $\{\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\cdot)\}$ on the collection of affine subsets $\mathcal{S}_{\mathbf{Y}} \subseteq \mathcal{S}_{\mathbf{X}}$ (these collections could be not equal since q_i could take zero values). The absolute continuity of each $\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\cdot)$ with respect to $\mu_{\mathbf{X}}^{\mathcal{A}_i}(\cdot)$ is followed by the absolute continuity of $\mu_{\mathbf{Y}}(\cdot)$ with respect to $\mu_{\mathbf{X}}(\cdot)$, which completes the proof. Finally, since $\mathcal{A}_i \cap \cup_{j=1}^{i-1} \mathcal{A}_j$ is formed by affine sets with dimension strictly lower than e_i , and because of absolute continuity of $\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\cdot)$, we have $\mu_{\mathbf{Y}}^{\mathcal{A}_i}(\mathcal{A}_i \cap \cup_{j=1}^{i-1} \mathcal{A}_j) = 0$, therefore, we can rewrite (208) as

$$\mu_{\mathbf{Y}}(\mathcal{C}) = \sum_i q_i \mu_{\mathbf{Y}}^{\mathcal{A}_i}(\mathcal{C} \cap \mathcal{A}_i). \quad (209)$$

APPENDIX G PROOF OF LEMMA 7

The necessary and sufficient condition of existence of $D(\mu_{\mathbf{X}} \parallel \mu_{\mathbf{Y}})$ is followed by Lemma 6 and by the fact that $D(\mu_{\mathbf{X}} \parallel \mu_{\mathbf{Y}})$ is defined if and only if $\mu_{\mathbf{X}}$ is absolutely continuous with respect to $\mu_{\mathbf{Y}}$.

For calculating $D(\mu_{\mathbf{X}} \parallel \mu_{\mathbf{Y}})$, firstly we order the collection $\mathcal{S}_{\mathbf{X}}$ of the affine sets $\{\mathcal{A}_i\}_i$ in the way that the dimension e_i of the set \mathcal{A}_i is an increasing function of i . Next, we define \mathcal{B}_i as

$$\mathcal{B}_i = \mathcal{A}_i \setminus \cup_{j=1}^{i-1} \mathcal{A}_j. \quad (210)$$

Note that $\cup_i \mathcal{B}_i = \cup_i \mathcal{A}_i$ and \mathcal{B}_i s are mutually exclusive (i.e., $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ if $i \neq j$).

Next, we write the formulation of $D(\mu_{\mathbf{X}} \parallel \mu_{\mathbf{Y}})$ as

$$\begin{aligned} D(\mu_{\mathbf{X}} \parallel \mu_{\mathbf{Y}}) &= \int_{\cup_i \mathcal{A}_i} d\mu_{\mathbf{X}} \log \frac{d\mu_{\mathbf{X}}}{d\mu_{\mathbf{Y}}} \\ &\stackrel{(a)}{=} \int_{\cup_i \mathcal{B}_i} d\mu_{\mathbf{X}} \log \frac{d\mu_{\mathbf{X}}}{d\mu_{\mathbf{Y}}} \\ &\stackrel{(b)}{=} \sum_i \int_{\mathcal{B}_i} d\mu_{\mathbf{X}} \log \frac{d\mu_{\mathbf{X}}}{d\mu_{\mathbf{Y}}} \\ &\stackrel{(c)}{=} \sum_i p_{\mathbf{X}}^{\mathcal{A}_i} \int_{\mathcal{B}_i} d\mu_{\mathbf{X}}^{\mathcal{A}_i} \log \frac{p_{\mathbf{X}}^{\mathcal{A}_i} d\mu_{\mathbf{X}}^{\mathcal{A}_i}}{p_{\mathbf{Y}}^{\mathcal{A}_i} d\mu_{\mathbf{Y}}^{\mathcal{A}_i}} \\ &= \sum_i p_{\mathbf{X}}^{\mathcal{A}_i} \log \frac{p_{\mathbf{X}}^{\mathcal{A}_i}}{p_{\mathbf{Y}}^{\mathcal{A}_i}} + \sum_i p_{\mathbf{X}}^{\mathcal{A}_i} \int_{\mathcal{B}_i} d\mu_{\mathbf{X}}^{\mathcal{A}_i} \log \frac{d\mu_{\mathbf{X}}^{\mathcal{A}_i}}{d\mu_{\mathbf{Y}}^{\mathcal{A}_i}} \\ &\stackrel{(d)}{=} D(p_{\mathbf{X}} \parallel p_{\mathbf{Y}}) + \sum_i p_{\mathbf{X}}^{\mathcal{A}_i} \int_{\mathcal{A}_i} d\mu_{\mathbf{X}}^{\mathcal{A}_i} \log \frac{d\mu_{\mathbf{X}}^{\mathcal{A}_i}}{d\mu_{\mathbf{Y}}^{\mathcal{A}_i}} \\ &= D(p_{\mathbf{X}} \parallel p_{\mathbf{Y}}) + \sum_{\mathcal{A} \in \mathcal{S}_{\mathbf{X}}} p_{\mathbf{X}}^{\mathcal{A}} D(\mu_{\mathbf{X}}^{\mathcal{A}} \parallel \mu_{\mathbf{Y}}^{\mathcal{A}}), \end{aligned}$$

which completes the proof. Note that (a) holds because $\cup_i \mathcal{B}_i = \cup_i \mathcal{A}_i$, (b) is followed by mutual exclusion of \mathcal{B}_i s,

(c) holds because of the form of affinely singular probability measures $\mu_{\mathbf{X}}$ and $\mu_{\mathbf{Y}}$, which for every set $\mathcal{C} \subseteq \cup_i \mathcal{A}_i$ is as

$$\mu_{\mathbf{X}}(\mathcal{C}) = \sum_i p_{\mathbf{X}}^{A_i} \mu_{\mathbf{X}}^{A_i}(\mathcal{C} \cap \mathcal{A}_i), \quad (211)$$

and

$$\mu_{\mathbf{Y}}(\mathcal{C}) = \sum_i p_{\mathbf{Y}}^{A_i} \mu_{\mathbf{Y}}^{A_i}(\mathcal{C} \cap \mathcal{A}_i). \quad (212)$$

Finally, (d) is correct because \mathcal{A}^{-i} is mutually singular with respect to $\cup_{j=1}^{i-1} \mathcal{A}_j$, and therefore $\mu_{\mathbf{X}}^{A_i}(\mathcal{C} \cap \mathcal{B}_i) = \mu_{\mathbf{X}}^{A_i}(\mathcal{C} \cap (\mathcal{B}_i \cup \cup_{j=1}^{i-1} \mathcal{A}_j)) = \mu_{\mathbf{X}}(\mathcal{C} \cap \mathcal{A}_i)$.

APPENDIX H PROOF OF THEOREM 7

Recalling the definition of BID in (15) and the result in Theorem 4, (82) is immediate. To prove (84), we continue with the following three steps: (i) we first prove that $R(\epsilon) \leq d_B(\{\mathbf{Z}_t\})$, (ii) then, we show that $R^*(\epsilon) \geq d_B(\{\mathbf{Z}_t\})$, and (iii) finally we use [10, Eqn. 75] which for a general source states that

$$R^*(\epsilon) \leq R_B(\epsilon) \leq R(\epsilon). \quad (213)$$

The following definition of rectifiability in [43, Section 3.2.14] is also used in the development of the proof.

Definition 14: The set E is m -rectifiable if there exists a Lipschitz function from a bounded subset of \mathbb{R}^m to E .

- **Step (i):** In this step we prove that

$$R(\epsilon) \leq d_B(\{\mathbf{Z}_t\}). \quad (214)$$

In order to do this, we utilize [10, Lemma 12] that provides a sufficient condition to upper-bound $R(\epsilon) \leq r$. More specifically, the condition is that for large ms , we have an $\lfloor mr \rfloor$ -rectifiable set $\mathcal{R}_m \in \mathbb{R}^m$, in which $\mathbb{P}(\mathbf{Z}^m \in \mathcal{R}_m) \geq 1 - \epsilon$. In fact, for an arbitrary $\delta \in [0, 1]$ we provide a set \mathcal{R}_m with $r = (d_B(\{\mathbf{Z}_t\}) + \delta)$. Thereby, using the arbitrariness on ϵ and δ , and the above discussion we complete the proof.

To begin with, for independent vectors $\{\mathbf{u}_{i,0}, \mathbf{u}_{i,1}, \dots, \mathbf{u}_{i,e_i}\}$ in \mathbb{R}^n , let

$$\mathcal{S}_i = \text{span}(\{\mathbf{u}_{i,j}\}_{j=1}^{e_i}) + \mathbf{u}_{i,0} \quad (215)$$

be an affine subset. Obviously, any affine subset can be expressed this way. Further, any bounded subset of \mathcal{S}_i like \mathcal{A} is also e_i -rectifiable. To check this, note that for each $\mathbf{x} \in \mathcal{A}$ we can write that

$$\mathbf{x} = \sum_{j=1}^{e_i} a_j \mathbf{u}_j + \mathbf{u}_0. \quad (216)$$

Hence, \mathbf{x} is a linear, and thus, Lipschitz function of $\mathbf{a}^{e_i} = (a_1, \dots, a_{e_i})^T$. Moreover, due to the independence of $\{\mathbf{u}_i\}$ and the boundedness of \mathcal{A} , we conclude that \mathbf{a}^{e_i} s are also bounded. Thus, \mathcal{A} is e_i -rectifiable (Definition 14). Recalling [10, Lemma 11], we conclude that every bounded subset of $\cup_i \mathcal{S}_i$ is $(\max_k \{e_k\})$ -rectifiable. Similarly, if

$$\mathcal{I}_m = \left\{ i : e_i \leq \lfloor mr \rfloor \right\}, \quad (217)$$

and

$$\mathcal{R}_m = \left(\bigcup_{i \in \mathcal{I}_m} \mathcal{K}_i \right) \cap [-l, l]^m, \quad (218)$$

for arbitrary $l \in \mathbb{R}^+$, then, \mathcal{R}_m is $\lfloor mr \rfloor$ -rectifiable (See the definition of \mathcal{K}_i in Section VII-C). Furthermore, using the assumption in (83), for every $\delta, \epsilon \in \mathbb{R}^+$, we know that there exists a large enough m such that $e_i < mr$ (or equivalently $e_i \leq \lfloor mr \rfloor$) with probability at least $1 - \epsilon/2$; formally, $\mathbb{P}(V_m \in \mathcal{I}_m) \geq 1 - \frac{\epsilon}{2}$, for sufficiently large m . Besides, one can choose large enough e so as to

$$\mathbb{P}(\mathbf{Z}^m \in [-l, l]^m | V_m \in \mathcal{I}_m) \geq 1 - \frac{\epsilon}{2}. \quad (219)$$

Thus, we have

$$\mathbb{P}(\mathbf{Z}^m \in \mathcal{R}_m) = \mathbb{P}(\mathbf{Z}^m \in [-l, l]^m, V_m \in \mathcal{I}_m) \geq 1 - \epsilon, \quad (220)$$

which completes the proof.

- **Step (ii) – proof by contradiction:** Assume that $R^*(\epsilon) < d_B(\{\mathbf{Z}_t\})$ and define $\delta = d_B(\{\mathbf{Z}_t\}) - R^*(\epsilon)$. We can check that $R = d_B(\{\mathbf{Z}_t\}) - \delta/2$ satisfies the conditions in Lemma 1. In other words, there should exist $M_1 \in \mathbb{N}$, $m \geq M_1$, $\mathcal{S}^m \in \mathbb{R}^m$, and a $\lceil (1 - R)m \rceil$ -dimensional subspace $\mathcal{H}^m \subset \mathbb{R}^m$ such that

$$\mathbb{P}(\mathbf{Z}^m \in \mathcal{S}^m) \geq 1 - \epsilon \quad (221)$$

and $(\mathcal{S}^m - \mathcal{S}^m) \cap \mathcal{H}^m = \{0\}$. Below, we find a non-zero vector in $(\mathcal{S}^m - \mathcal{S}^m) \cap \mathcal{H}^m$, which contradicts the assumption and proves the claim. Let $k_m = \lfloor mR \rfloor$ and $k'_m = \lfloor m(d_B(\{\mathbf{Z}_t\}) - \delta/4) \rfloor$. Since $R < d_B(\{\mathbf{Z}_t\}) - \delta/4$, for large enough m we have

$$k'_m > k_m. \quad (222)$$

Next, let us define $\mathcal{F}_m^{k'_m}$ as the set of all affinely singular subsets (in \mathbb{R}^m) for the measure of \mathbf{Z}^m with dimension k'_m or higher. Formally,

$$\mathcal{F}_m^{k'_m} := \{ \mathcal{F} \in \mathcal{K}, \dim(\mathcal{F}) \geq k'_m \}, \quad (223)$$

where \mathcal{K} is defined in Section VII-C. We recall that due to the definition of affinely singular subsets, \mathbf{Z}^m has an absolutely continuous distribution on each $\mathcal{F} \in \mathcal{F}_m^{k'_m}$.

For each $\mathcal{F} \in \mathcal{F}_m^{k'_m}$, we know that $\mathcal{F} - \mathcal{F}$ is a subspace of \mathbb{R}^m (since \mathcal{F} is an affine subset of \mathbb{R}^m). Furthermore,

$$\begin{aligned} \dim(\mathcal{H}^m) &= m - k_m > m - k'_m \geq m - \dim(\mathcal{F} - \mathcal{F}) \\ \Rightarrow \dim(\mathcal{H}^m) + \dim(\mathcal{F} - \mathcal{F}) &> m. \end{aligned} \quad (224)$$

This shows that $\mathcal{H}^m \cap (\mathcal{F} - \mathcal{F})$ is non-trivial; i.e., there exists $\mathbf{u} \in \mathcal{H}^m \cap (\mathcal{F} - \mathcal{F})$ with $\|\mathbf{u}\|_2 = 1$. As we have

$$\begin{aligned} \mathbb{P}_{V_m}(e_{V_m} \geq k'_m) &\geq \mathbb{P}_{V_m}(e_{V_m} \geq m(d_B(\{\mathbf{Z}_t\}) - \delta/4)) \\ &= \mathbb{P}_{V_m}\left(\frac{e_{V_m}}{m} - d_B(\{\mathbf{Z}_t\}) \geq -\delta/4\right) \\ &\geq \mathbb{P}_{V_m}\left(\left|\frac{e_{V_m}}{m} - d_B(\{\mathbf{Z}_t\})\right| \leq \delta/4\right), \end{aligned} \quad (225)$$

due to the assumption of the theorem, it is possible to set

m large enough that the latter probability exceeds $\frac{1}{2} + \frac{\epsilon}{2}$ (for $\epsilon < \frac{1}{2}$):

$$m \gg 1 : \mathbb{P}_{V_m}(e_{V_m} \geq k'_m) \geq \frac{1+\epsilon}{2}. \quad (226)$$

Next, we have

$$\begin{aligned} & \mathbb{P}\left(\mathbf{Z}^m \in \left(\bigcup_{\mathcal{F} \in \mathcal{K}} \mathcal{F} \setminus \bigcup_{\mathcal{F}' \in \mathcal{K} \setminus \mathcal{F}} \mathcal{F}'\right) \cap \mathcal{S}^m\right) \\ & \stackrel{(a)}{\geq} -\mathbb{P}\left(\mathbf{Z}^m \notin \bigcup_{\mathcal{F} \in \mathcal{K}} \mathcal{F} \setminus \bigcup_{\mathcal{F}' \in \mathcal{K} \setminus \mathcal{F}} \mathcal{F}'\right) + \mathbb{P}(\mathbf{Z}^m \in \mathcal{S}^m) \\ & \stackrel{(b)}{=} -\mathbb{P}\left(\mathbf{Z}^m \in \bigcup_{\mathcal{F}' \in \mathcal{K} \setminus \mathcal{F}_m^{k'_m}} \mathcal{F}'\right) + \mathbb{P}(\mathbf{Z}^m \in \mathcal{S}^m) \end{aligned} \quad (227)$$

$$\stackrel{(b)}{=} -\mathbb{P}\left(\mathbf{Z}^m \in \bigcup_{\mathcal{F}' \in \mathcal{K} \setminus \mathcal{F}_m^{k'_m}} \mathcal{F}'\right) + \mathbb{P}(\mathbf{Z}^m \in \mathcal{S}^m) \quad (228)$$

$$= -\underbrace{\mathbb{P}_{V_m}(e_{V_m} < k'_m)}_{\leq \frac{1-\epsilon}{2}} + \underbrace{\mathbb{P}(\mathbf{Z}^m \in \mathcal{S}^m)}_{\geq 1-\epsilon} \quad (229)$$

$$\geq \frac{1-\epsilon}{2} > 0, \quad (230)$$

where (a) is a result of the fact that $\mathbb{P}(A \setminus B) \geq -\mathbb{P}(B) + \mathbb{P}(A)$, and (b) holds because $\mathbb{P}(\mathbf{Z}^m \notin \bigcup_{\mathcal{F} \in \mathcal{K}} \mathcal{F}) = 0$. The positive probability in (230) (and the fact that $\mathcal{F}_m^{k'_m}$ is countable)

shows that at least for one $\mathcal{F} \in \mathcal{F}_m^{k'_m}$, if we define \mathcal{L} as

$$\mathcal{L} = \left(\mathcal{F} \setminus \bigcup_{\mathcal{F}' \in \mathcal{K} \setminus \mathcal{F}_m^{k'_m}} \mathcal{F}'\right) \quad (231)$$

the probability $\mathbb{P}(\mathbf{Z}^m \in \mathcal{L} \cap \mathcal{S}^m)$ (and therefore $\mathbb{P}(\mathbf{Z}^m \in \mathcal{L})$) is nonzero:

$$\mathbb{P}(\mathbf{Z}^m \in \mathcal{L} \cap \mathcal{S}^m | \mathbf{Z}^m \in \mathcal{L}) = \frac{\mathbb{P}(\mathbf{Z}^m \in \mathcal{L} \cap \mathcal{S}^m)}{\mathbb{P}(\mathbf{Z}^m \in \mathcal{L})} > 0. \quad (232)$$

Since \mathbf{Z}^m has an absolutely continuous measure on \mathcal{L} , the set $\mathcal{E} = \mathcal{L} \cap \mathcal{S}^m$ should have a non-zero Lebesgue measure in $\mathbb{R}^{\dim(\mathcal{F})}$. Using this fact, and since every $\mathcal{F}' \in \mathcal{K} \setminus \mathcal{F}_m^{k'_m}$ has zero Lebesgue measure in $\mathbb{R}^{\dim(\mathcal{F})}$, we can show that $\mathcal{G} = \mathcal{F} \cap \mathcal{S}^m$ has non-zero Lebesgue measure in $\mathbb{R}^{\dim(\mathcal{F})}$. Now, utilizing Steinhaus Theorem [44, Theorem VIII], we conclude the existence of $a \in \mathbb{R}^+$ such that

$$\text{Ball}_a^{\dim(\mathcal{F})} \subset \mathcal{G} - \mathcal{G} \subset (\mathcal{F} - \mathcal{F}) \cap (\mathcal{S}^m - \mathcal{S}^m). \quad (233)$$

Hence, for all $\bar{\mathbf{u}} \in \mathcal{F} - \mathcal{F}$ with $\|\bar{\mathbf{u}}\|_2 \leq a$, we know that $\bar{\mathbf{u}} \in \mathcal{S}^m - \mathcal{S}^m$. Now, if we set $\bar{\mathbf{u}} = a\mathbf{u}$ where $\mathbf{u} \in \mathcal{H}^m \cap (\mathcal{F} - \mathcal{F})$ and $\|\mathbf{u}\|_2 = 1$, we obtain that

$$\bar{\mathbf{u}} \in \mathcal{H}^m \cap (\mathcal{F} - \mathcal{F}) \cap (\mathcal{S}^m - \mathcal{S}^m). \quad (234)$$

This reveals that \mathcal{H}^m and $\mathcal{S}^m - \mathcal{S}^m$ have a non-zero intersection, which completes the proof.

- **Step (iii):** (84) follows directly from (214), the fact that $R_B^*(\epsilon) \geq d_B(\{\mathbf{Z}_t\})$, and (213).

APPENDIX I PROOF OF LEMMA 8

Recalling Lemma 3, we know that an i -dimensional singularity occurs when $\boldsymbol{\nu} = \mathbf{s} \in \{0, 1\}^n$ such that $\text{rank}(A_m^{[\mathbf{s}]}) = i$. Besides, the columns of A_m indexed in the range $[l_1 + l_2 + 1 : n]$ are linearly independent. Hence, if $\text{rank}(A_m^{\mathbf{s}}) = i$, then $\|\mathbf{s}\|_1 \leq l_2 + l_1 + i$ (at most i columns in the range $[l_1 + l_2 + 1 : n]$ can be selected). As a consequence, we have

$$\begin{aligned} \mathbb{P}(e_{V_m} \leq k) & \leq \sum_{i=0}^{k+l_1+l_2} \binom{n}{i} \alpha^i (1-\alpha)^{n-i} \\ & \stackrel{(a)}{\leq} \exp\left(-nD\left(\frac{k+l_2+l_1}{n} \parallel \alpha\right)\right), \end{aligned} \quad (235)$$

where (a) is obtained from [37, Theorem 1] by assuming $\frac{k+l_2+l_1}{n} < \alpha$.

In contrast, if we select k columns all in the range $[l_1 + l_2 + 1 : n]$, then $\text{rank} A_m^{[\mathbf{s}]} = k$. Thus,

$$\begin{aligned} \mathbb{P}_{V_m}(e_{V_m} \geq k) & \geq \sum_{i=k}^{n-l_1-l_2} \binom{n-l_2-l_1}{i} \alpha^i (1-\alpha)^{n-l_2-l_1} \\ & \stackrel{(b)}{\geq} \exp\left(- (n-l_1-l_2)D\left(\frac{k}{n-l_2-l_1} \parallel \alpha\right)\right), \end{aligned} \quad (236)$$

where (b) is also obtained from [37, Theorem 1] using $\frac{k}{n-l_2-l_1} > \alpha$. Substituting $n = m + l_1 + l_2$ in the two previous inequalities, the desired claim is achievable.

APPENDIX J PROOF OF LEMMA 9

Using (50) and (53), we have

$$nb(X_1) = H(\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}}) + h(\mathbf{X}_c^{\nu} | \boldsymbol{\nu}). \quad (237)$$

Theorem 5 shows that $b(\mathbf{Y}^m) = H(\Upsilon_m) + h(\tilde{\mathbf{Y}}_{\Upsilon_m} | \Upsilon_m)$. Therefore,

$$b(\mathbf{Y}^m) - nb(X_1) \quad (238)$$

$$= \underbrace{H(\Upsilon_m) - H(\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}})}_{\Delta_1} + h(\tilde{\mathbf{Y}}_{\Upsilon_m} | \Upsilon_m) - h(\mathbf{X}_c^{\nu} | \boldsymbol{\nu}) \quad (239)$$

$$= \Delta_1 + \underbrace{h(\tilde{\mathbf{Y}}_{\Upsilon_m} | \Upsilon_m) - h(\mathbf{W}_{\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}}} | \boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}})}_{\Delta_2} + h(\mathbf{W}_{\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}}} | \boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}}) - h(\mathbf{X}_c^{\nu} | \boldsymbol{\nu}). \quad (240)$$

Thus, we have that

$$\frac{|b(\mathbf{Y}^m) - nb(X_1) - m\psi_{m,\boldsymbol{\nu}}(A_m)|}{m} \leq \frac{|\Delta_1| + |\Delta_2| + |\Delta_3|}{m}, \quad (241)$$

where

$$\Delta_3 = h(\mathbf{W}_{\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}}} | \boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}}) - h(\mathbf{X}_c^{\nu} | \boldsymbol{\nu}) - m\psi_{m,\boldsymbol{\nu}}(A_m).$$

Let Υ_m and $\mathcal{T}_i^{(m)}$ for $i \in \mathbb{N}$ denote the RV V_m and the sets $\mathcal{T}_i^{(m)}$ defined in Section VII-C for the mixing matrix A_m . Below, we prove the claim of the lemma for $\alpha_i \neq 0$

in six steps: (i) finding an upper-bound for the probability $\mathbb{P}_{V_m}(|\mathcal{T}_{V_m}^{(m)}| \geq 2)$ (this is the probability that a singular subset appears for more than one choice of ν), (ii) upper-bounding $|\Delta_1|$, (iii) upper-bounding $|\Delta_2|$, (iv) bounding the difference between the differential entropy of $T\mathbf{X}_c^s$ and the differential entropy of \mathbf{X}_c^s as

$$\Delta_4 = h(T\mathbf{X}_c^s) - h(\mathbf{X}_c^s), \quad (242)$$

in which T is formed by $k < l$ rows of an $l \times l$ unitary matrix, where $l = \sum_{i \in \mathbb{N}} s_i$, (v) upper-bounding $|\Delta_3|$, and (vi) combining the previous bounds to conclude the claim for $\alpha_i \neq 0$. Next, we explain how the claim for $\alpha_i = 0$ is obtained by a similar approach.

- **Step (i):** Let $A_m = [A_m^{[1]}, \dots, A_m^{[n]}]$, where $A_m^{[i]}$ s stand for the columns. For each $s \in \{0, 1\}^n$, we define $A_m^{[s]} = \bigcup_{i: s_i=1} \{A_m^{[i]}\}$, and for simplicity of notation, we define $\mathcal{A}_m \triangleq \mathcal{A}_m^{(1,1,\dots,1)}$.

To bound $\mathbb{P}_{\Upsilon_m}(|\mathcal{T}_{\Upsilon_m}^{(m)}| \geq 2)$, where the randomness in $\Upsilon_m = F((\nu, \mathbf{X}_d^{\bar{\nu}}))$ is due to the randomness of ν and $\mathbf{X}_d^{\bar{\nu}}$, note that $|\mathcal{T}_i^{(m)}| \geq 2$ implies that for every pair $(s, \mathbf{x}_d^{\bar{s}})$ in $\mathcal{T}_i^{(m)}$, there exists a distinct pair $(s', \mathbf{x}_d^{\bar{s}'})$, such that $\text{span}(\mathcal{A}_m^{[s]}) = \text{span}(\mathcal{A}_m^{[s']})$. There are now two possibilities:

- The set of non-zero locations in s' is a subset of the non-zero locations in s . Hence, $A_m^{[s]}$ is column-rank-deficient (i.e., $I_{\text{fcr}}(A_m^{[s]}) = 0$).
- There is an i for which we have $s'_i = 1$ and $s_i = 0$. Hence, $(A_m^{[s]}, A_m^{[i]})$ is column-rank-deficient (i.e., $I_{\text{fcr}}((A_m^{[s]}, A_m^{[i]})) = 0$).

We can now upper-bound $\mathbb{P}_{\Upsilon_m}(|\mathcal{T}_{\Upsilon_m}^{(m)}| \geq 2)$ with

$$\mathbb{P}_{\nu} \left(I_{\text{fcr}}(A_m^{[\nu]}) = 0 \text{ or } \exists i \in [n], \nu_i = 0 : I_{\text{fcr}}((A_m^{[\nu]}, A_m^{[i]})) = 0 \right) \quad (243)$$

To evaluate the above upper-bound, let us consider the example $A_m = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. As A_m has 4 columns, ν has $2^4 = 16$ possibilities. In Figure 7, each vertex represents a submatrix of A_m corresponding to the written 4-tuple (which columns are present and which columns are dropped).

In this graph, vertex i is connected to vertex j (with a directed edge) if $A_m^{[\nu^j]}$ has exactly one additional column with respect to $A_m^{[\nu^i]}$ (the color of the edges in Figure 7 distinguish this additional column). Red vertices in this graph are column-rank-deficient matrices. The upper-bound in (243) actually sums over the probability of red vertices as well as the vertices connected to the red vertices. Note that the probability of a vertex whose 4-tuple has i ones is $\alpha^i(1-\alpha)^{n-i}$ ($n = 4$ in this example). Let L_i denote the number of red vertices whose n -tuple has i ones. Therefore, the probability of rank-deficiency $\rho_m(A_m, \alpha)$ is given as

$$\rho_m(A_m, \alpha) = \sum_{i=0}^n L_i \alpha^i (1-\alpha)^{n-i}. \quad (244)$$

We now express the upper-bound in (243) in terms of L_i s. Note that there are i vertices connected to a red vertex whose n -tuple has i ones, and also their n -tuples have $i-1$ ones.

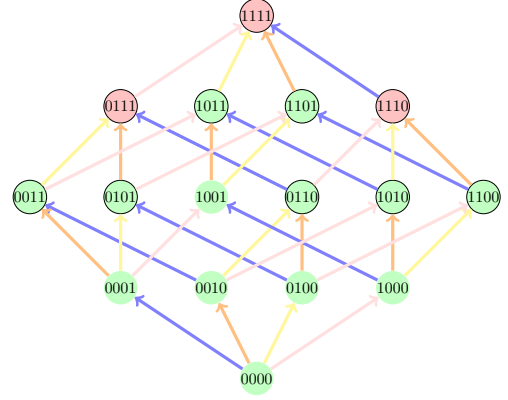


Fig. 7. Each circle $a_1 a_2 a_3 a_4$, where $a_i \in \{0, 1\}^4$ for $i \in [1 : 4]$, represents the event $\nu = (a_1, a_2, a_3, a_4)^T$. The red circles point out that $A_m^{[\nu]}$ is not a full column-rank matrix, while green circles stand for full column-rank matrices $A_m^{[\nu]}$. Each directional edge which goes out from a node, denotes the augmentation of the associated matrix with a specific column.

Hence, the probability of vertices connected to red vertices is upper-bounded by $\sum_{i=1}^n i L_i \alpha^{i-1} (1-\alpha)^{n-i+1}$; vertices could be counted more than once in this expression. However, as red vertices are connected only to red vertices, we know that the latter expression contains the term $\sum_{i=1}^n (n-i) L_i \alpha^i (1-\alpha)^{n-i}$ just for red vertices. As a result, we have that

$$\begin{aligned} \mathbb{P}_{V_m}(|\mathcal{T}_{V_m}^{(m)}| \geq 2) &\leq \rho_m(A_m, \alpha) + \sum_{i=1}^n i L_i \alpha^{i-1} (1-\alpha)^{n-i+1} \\ &\quad - \sum_{i=1}^n (n-i) L_i \alpha^i (1-\alpha)^{n-i} \\ &= \sum_{i=0}^n \left(\underbrace{\frac{i}{\alpha} - n + 1}_{\leq \frac{n}{\alpha}} \right) L_i \alpha^i (1-\alpha)^{n-i} \\ &= \left(\frac{n}{\alpha} - n + 1 \right) \rho_m(A_m, \alpha) \leq n C'_0 \rho_m(A_m, \alpha), \end{aligned} \quad (245)$$

where $C'_0 = \frac{1}{\alpha}$.

- **Step (ii):** Since $X_{d,i}$ is supported on a finite set (\mathcal{X}_d) , the cardinality of the sample spaces of $(\nu, \mathbf{X}_d^{\bar{\nu}})$, and V_m is upper-bounded by $2^{C'_1 n}$ where $C'_1 = \log(|\mathcal{X}_d| + 1) > 0$ (note that V_m is a probability distribution on a partition of pairs $\{(s, \mathbf{x}_d^{\bar{s}}) : s \in \{0, 1\}^n, \mathbf{x}_d^{\bar{s}} \in \mathcal{X}_d^{\otimes \|\mathbf{s}\|_1}\}$).

Let us define $g : \mathbb{N} \rightarrow (\cup_i \mathcal{T}_i^{(m)}) \cup \mathbb{N}$ as

$$g(i) := \begin{cases} F^{-1}(i), & |\mathcal{T}_i^{(m)}| = 1, \\ i, & \text{otherwise,} \end{cases} \quad (246)$$

where $F(\cdot)$ was defined in Section VII-C. This implies that when $|\mathcal{T}_{\Upsilon_m}^{(m)}| = 1$, we have $g(\Upsilon_m) = (\nu, \bar{\nu})$; when $|\mathcal{T}_{\Upsilon_m}^{(m)}| > 1$, $g(\Upsilon_m)$ is an integer (not a pair). As a result, the total variation distance between the distributions of $g(\Upsilon_m)$ and $(\nu, \mathbf{X}_d^{\bar{\nu}})$ does not exceed $2\mathbb{P}_{\Upsilon_m}(|\mathcal{T}_{\Upsilon_m}^{(m)}| \geq 2)$. Using the assumption that $\mathbb{P}_V(|\mathcal{T}_{\Upsilon_m}^{(m)}| \geq 2) \leq n C'_0 \rho_m(A_m, \alpha) \leq 1/2e$, [45, Lemma 2.7] provides the following bound on the distance of the entropies:

$$|\mathbb{H}(\Upsilon_m) - \mathbb{H}(\nu, \mathbf{X}_d^{\bar{\nu}})|$$

$$= |\Delta_1| \leq -2\mathbb{P}_{\Upsilon_m}(|\tau_{\Upsilon_m}^{(m)}| \geq 2) \left(\log(2\mathbb{P}_{\Upsilon_m}(|\tau_{\Upsilon_m}^{(m)}| \geq 2)) - C'_1 n \right). \quad (247)$$

Now, by using (245), the above inequality results in

$$\begin{aligned} |\Delta_1| &\leq -2nC'_0\rho_m(A_m, \alpha) \times \\ &\quad \left(\log(\rho_m(A_m, \alpha)) + \log(\underbrace{nC'_0}_{\geq 0}) - C'_1 n \right) \\ &\leq -2nC'_0\rho_m(A_m, \alpha) (\log(\rho_m(A_m, \alpha)) - C'_1 n). \quad (248) \end{aligned}$$

• **Step (iii):** Using the definition of $\tilde{\mathbf{Y}}_i$ in (34), one can see that

$$\begin{aligned} 0 \leq \Delta_2 &= \mathbb{E}_{\Upsilon_m} [\mathbb{I}(\tilde{\mathbf{Y}}_{\Upsilon_m}; \Upsilon_m^{(\Upsilon_m)})] \leq \mathbb{E}_{\Upsilon_m} [\mathbb{H}(\Upsilon_m^{(\Upsilon_m)})] \\ &\leq \mathbb{E}_{\Upsilon_m} [\log(|\text{sample space of } \Upsilon_m^{(\Upsilon_m)}|)] \\ &\leq \mathbb{E}_{\Upsilon_m} [\log(2^{C'_1 n}) \mid |\tau_{\Upsilon_m}^{(m)}| \geq 2] \cdot \mathbb{P}_{\Upsilon_m}(|\tau_{\Upsilon_m}^{(m)}| \geq 2) \\ &\leq nC'_1 \mathbb{P}_{\Upsilon_m}(|\tau_{\Upsilon_m}^{(m)}| \geq 2). \quad (249) \end{aligned}$$

Again we recall (245) to bound the latter probability

$$|\Delta_2| \leq n^2 C'_1 C'_0 \rho_m(A_m, \alpha). \quad (250)$$

• **Step (iv):** We start by studying the moments of $T\mathbf{X}_c^s$, when T is a submatrix of a unitary matrix:

$$\mathbb{E} \left[\|T\mathbf{X}_c^s\|_{\alpha}^{\beta} \right] \stackrel{(a)}{\leq} k^{\beta/\alpha} l^{\beta} \mathbb{E} [\|\mathbf{X}_c^s\|_{\alpha}^{\beta}] \quad (251)$$

$$\stackrel{(b)}{\leq} k^{\beta/\alpha} l^{\beta+\beta/\alpha-1} M_{X_{c,1}}(\beta) \quad (252)$$

$$\leq n^{C'_2+1} M_{X_{c,1}}(\beta), \quad (253)$$

where $C'_2 = \beta(2/\alpha + 1) - 2$. The validity of (a) is due to (190) and the fact that the entries of T do not exceed 1 in absolute value (T is a submatrix of a unitary matrix). (b) is also achieved via (188).

Since $T\mathbf{X}_c^s$ has some bounded moments, $\mathbb{h}(T\mathbf{X}_c^s)$ is also finite. In particular, [6, Corollary 1] establishes

$$\mathbb{h}(T\mathbf{X}_c^s) \leq \log M, \quad (254)$$

where M is

$$M = V_{\alpha,n} \left(\alpha e n^{C'_2} M_{X_{c,1}}(\beta) \right)^{n/\beta} \Gamma(1 + \frac{n}{\beta}), \quad (255)$$

in which $V_{\alpha,n}$ indicates the volume of the n -dimensional unit-ball associated with the α -norm. Obviously, $V_{\alpha,n} \leq V_{\infty,n} < 2^n$. Now, for $n \geq \beta e$ we have

$$\begin{aligned} M &\leq (2^{\beta} \alpha e M_{X_{c,1}}(\beta) n^{C'_2})^{n/\beta} \Gamma(1 + \frac{n}{\beta}) \\ &\leq (2^{\beta} \alpha e M_{X_{c,1}}(\beta) n^{C'_2})^{n/\beta} \lceil \frac{n}{\beta} \rceil! \\ &\stackrel{(a)}{\leq} (2^{\beta} \alpha e M_{X_{c,1}}(\beta) n^{C'_2})^{n/\beta} e^{\frac{3}{2}} \left(\frac{\lceil \frac{n}{\beta} \rceil}{e} \right)^{\lceil \frac{n}{\beta} \rceil + \frac{1}{2}} \\ &\leq (2^{\beta} \alpha e M_{X_{c,1}}(\beta) n^{C'_2})^{n/\beta} e^{\frac{3}{2}} \left(\frac{2n}{\beta e} \right)^{\frac{n}{\beta} + \frac{3}{2}} \\ &\leq \left(\frac{2}{\beta} \right)^{\frac{3}{2}} (C'_3)^n n^{C'_4 n}, \quad (256) \end{aligned}$$

for $C'_3 = \sqrt{\beta} \frac{2^{\beta+1} \alpha M_{X_{c,1}}(\beta)}{\beta}$ and $C'_4 = \frac{\alpha+2}{\alpha} \geq \frac{C'_2}{\beta} + \frac{1}{\beta} + \frac{3}{2n}$ (note that $\frac{n}{\beta} \geq \frac{3}{2} \geq 1$). (a) is followed by the Stirling's approximation. If $n \geq \frac{3}{2} \log(\frac{2}{\beta})$, we can use (256) in (254)

as

$$\mathbb{h}(T\mathbf{X}_c^s) \leq \frac{3}{2} \log\left(\frac{2}{\beta}\right) + n \log C'_3 + C'_4 n \log n \leq C'_5 n \log n, \quad (257)$$

for $C'_5 = 1 + |\log C'_3| + C'_4$.

Returning to (242), we know

$$\begin{aligned} \Delta_4 &\leq C'_5 \log n + |\mathbb{h}(\mathbf{X}_c^s)| \leq C'_5 \log n + |\mathbb{h}(X_{c,1})| n \\ &\leq C'_6 n \log n, \quad (258) \end{aligned}$$

where $C'_6 = |\mathbb{h}(X_{c,1})| + C'_5$ (\mathbf{X}_c^s consists of a number of $X_{c,i}$ s, and $X_{c,i}$ s are i.i.d.).

Since T is a submatrix of a unitary matrix, we can form \tilde{T} such that $(T; \tilde{T})$ is this unitary matrix. This implies that $\mathbb{h}((T; \tilde{T})\mathbf{X}_c^s) = \mathbb{h}(\mathbf{X}_c^s)$. Besides,

$$\mathbb{h}((T; \tilde{T})\mathbf{X}_c^s) \leq \mathbb{h}(T\mathbf{X}_c^s) + \mathbb{h}(\tilde{T}\mathbf{X}_c^s). \quad (259)$$

Hence,

$$\begin{aligned} -\Delta_4 &= \mathbb{h}(\mathbf{X}_c^s) - \mathbb{h}(T\mathbf{X}_c^s) = \mathbb{h}((T; \tilde{T})\mathbf{X}_c^s) - \mathbb{h}(T\mathbf{X}_c^s) \\ &\leq \mathbb{h}(\tilde{T}\mathbf{X}_c^s) \leq C'_5 n \log n. \quad (260) \end{aligned}$$

The latter inequality uses the same technique as in (257) for \tilde{T} . Combining (258) and (260), we obtain

$$|\Delta_4| \leq C'_6 n \log n. \quad (261)$$

• **Step (v):** Recalling $\psi_{m,\nu}(A_m) = \frac{1}{m} \mathbb{E}_{\nu} [\log \det^+ A_m^{[\nu]}]$ and the definition of $\mathbf{W}_{s, \mathbf{x}_d^s}$ in (33), we have that

$$\mathbb{h}(\mathbf{W}_{\nu, \mathbf{x}_d^s} | \nu, \mathbf{X}_d^s) = m \psi_{m,\nu}(A_m) + \mathbb{E}_{\nu} [\mathbb{h}(\tilde{U}_{\nu}^{\dagger} X_c^{\nu})], \quad (262)$$

where \tilde{U}_{ν} is the matrix formed by the first rank($A_m^{[\nu]}$) left singular vectors of $A_m^{[\nu]}$. As a result

$$\begin{aligned} |\Delta_3| &= \left| \mathbb{E}_{\nu} [\mathbb{h}(\tilde{U}_{\nu}^{\dagger} \mathbf{X}_c^{\nu})] - \mathbb{h}(\mathbf{X}_c^{\nu} | \nu) \right| \\ &= \left| \mathbb{E}_{\nu} [\mathbb{h}(\tilde{U}_{\nu}^{\dagger} \mathbf{X}_c^{\nu}) - \mathbb{h}(\mathbf{X}_c^{\nu})] \right| \\ &\leq \mathbb{E}_{\nu} \left[\left| \mathbb{h}(\tilde{U}_{\nu}^{\dagger} \mathbf{X}_c^{\nu}) - \mathbb{h}(\mathbf{X}_c^{\nu}) \right| \right] \\ &\leq C'_6 n \log(n) \rho_m(A_m, \alpha), \quad (263) \end{aligned}$$

where we used (261) for $T = \tilde{U}_{\nu}^{\dagger}$ in the last inequality.

Note that $\rho_m(A_m, \alpha)$ is the probability that $A_m^{[\nu]}$ is not of full column-rank. When $A_m^{[\nu]}$ has full column-rank, \tilde{U}_{ν} is a square

unitary matrix and $\mathbb{h}(\tilde{U}_{\nu}^{\dagger} \mathbf{X}_c^{\nu}) = \mathbb{h}(\mathbf{X}_c^{\nu})$.

• **Step (vi):** For $\alpha_1 \neq 0$, it is now easy to complete the proof using (248), (250), (263), and by setting $C_1 = C'_6 + 3C'_1 C'_0$ and $C_2 = -2C'_0$.

In the case of $\alpha_1 = 0$, X_1 and \mathbf{Y}^m (i.e., a linear combination of X_i s) are purely discrete. Hence, by (50) and (53), we have

$$nb(X_1) = \mathbb{H}(\nu, \mathbf{X}_d^s). \quad (264)$$

Furthermore, Theorem 5 implies that

$$b(\mathbf{Y}^m) = \mathbb{H}(\Upsilon_m). \quad (265)$$

As a result, we have

$$\frac{|b(\mathbf{Y}^m) - nb(X_1)|}{m} \leq \frac{|\Delta_1|}{m}, \quad (266)$$

for $\Delta_1 = H(\Upsilon_m) - H(\boldsymbol{\nu}, \mathbf{X}_d^{\bar{\nu}})$ as also defined in (239).

Similar to Step (i), we first bound $\mathbb{P}_{\Upsilon_m}(|\mathcal{T}_{\Upsilon_m}^{(m)}| \geq 2)$, and then, follow the same approach as in Step (ii) to bound $|\Delta_1|$. Since $\boldsymbol{\nu} = 0_{1 \times n}$, $|\mathcal{T}_i^{(m)}| \geq 2$ implies that for every pair $(0_{1 \times n}, \mathbf{x}_d) \in \mathcal{T}_i^{(m)}$, there exists $\mathbf{x}'_d \neq \mathbf{x}_d$, such that $(0_{1 \times n}, \mathbf{x}'_d) \in \mathcal{T}_i^{(m)}$ and $A_m \mathbf{x}_d = A_m \mathbf{x}'_d$. This only happens when $\text{span}(\mathcal{A}_m^{\mathbf{t}}) = \text{span}(\mathcal{A}_m^{\mathbf{t}'})$, where \mathbf{t} and \mathbf{t}' are n -dimensional indicators to show the non-zero status of the elements in \mathbf{x}_d and \mathbf{x}'_d , respectively. One can verify that \mathbf{t} and \mathbf{t}' are distributed as $\boldsymbol{\xi}$ which is defined in Lemma 9. Consequently, similar to Step (i), we can prove that

$$\mathbb{P}_{V_m}(|\mathcal{T}_{V_m}^{(m)}| \geq 2) \leq nC'_0 \tilde{\rho}_m(A_m, \boldsymbol{\xi}), \quad (267)$$

where $\tilde{\rho}_m(A_m, \boldsymbol{\xi})$ is defined in (105). Finally, by setting $\tilde{C}_1 = -2C'_0$ and $\tilde{C}_2 = 2C'_0 C'_1$ in (247), and using the latter inequality, we can achieve (104) that completes the proof.

APPENDIX K PROOF OF PROPOSITION 3

We prove this theorem in five steps:

- (i) for an n -dimensional random vector $\boldsymbol{\nu}$ with i.i.d. Bernoulli elements, we examine the distribution of the length of maximal sub-blocks with all 1 elements,
- (ii) we study the pseudo-determinant of four classes of square matrices; we provide lower- and upper-bounds on some of them, while for the rest, we derive closed-form expressions,
- (iii) for a given \mathbf{s} , we express $\det^+(A_m^{[\mathbf{s}]})$ via the block-lengths in Step (i) and the pseudo-determinants introduced in Step (ii),
- (iv) we prove the existence of the expected value of the logarithm of the pseudo-determinants introduced in Step (ii) by bounding them, and
- (v) we find $\Psi_\alpha(c_1, c_2)$ in terms of an expected value of a function of an α -geometric RV.

To simplify the results, we set $c_1 = a$ and $c_2 = b$.

• Step (i):

Definition 15: For an n -dimensional binary vector \mathbf{s} and integers $1 \leq i \leq j \leq n$, let $E_i^j(\mathbf{s})$ be the event that $s_i = \dots = s_j = 1$ while $s_{i-1} = s_{j+1} = 0$; by convention, we assume $s_0 = s_{n+1} = 0$. Besides, we denote the the indicator of E_i^j by $\varphi_i^j(\mathbf{s})$:

$$\varphi_i^j(\mathbf{s}) = (1 - s_{i-1})(1 - s_{j+1}) \prod_{k=i}^{k=j} s_k. \quad (268)$$

To account for the length of the 1-blocks, we define

$$\varphi_i(\mathbf{s}) := \begin{cases} \sum_{k=i}^{n-1} (k - i + 1) \varphi_i^k(\mathbf{s}), & 1 \leq i \leq n - 1, \\ \sum_{k=2}^n (n - k + 1) \varphi_k^n(\mathbf{s}), & i = n, \\ 1 + (n - 1) \varphi_1^n(\mathbf{s}), & i = n + 1. \end{cases} \quad (269)$$

Indeed, for $1 \leq i < n$, $\varphi_i(\mathbf{s})$ indicates the length of the 1-block starting at the i th location (except when the vector consists solely of 1s), $\varphi_n(\mathbf{s})$ shows the length of the 1-block ending at the last location (except when the vector consists solely of 1s), and $\varphi_{n+1}(\mathbf{s})$ takes the value n if the vector consists solely of 1s, and 1 otherwise. Note that if the i th location ($i < n$) is not the starting place of a 1-block, then, $\varphi_i(\mathbf{s}) = 0$.

Remark 4: Let $\boldsymbol{\nu}$ be an n -dimensional vector with i.i.d. elements distributed as $\text{Bern}(\alpha)$. The distribution of $\varphi_i(\boldsymbol{\nu})$ can be obtained as

$$\mathbb{P}(\varphi_i(\boldsymbol{\nu}) = x) = \begin{cases} \alpha^x (1 - \alpha), & i = 1, n, 1 \leq x \leq n - 1, \\ \alpha^n, & i = n + 1, x = n, \\ 1 - \alpha^n, & i = n + 1, x = 1, \\ \alpha^x (1 - \alpha)^2, & 1 < i < n, 1 \leq x \leq n - i, \end{cases} \quad (270)$$

which includes all possible non-zero values of x .

- **Step (ii):** To simplify the below arguments we define $b_k(x_1, x_2) := \det^+ B_k(x_1, x_2)$ for the $k \times k$ tridiagonal matrix $B_k(x_1, x_2)$ given as

$$B_k(x_1, x_2) := \begin{pmatrix} x_1 & ab & \dots & \dots & 0 \\ ab & a^2 + b^2 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \dots & \ddots & a^2 + b^2 & ab \\ 0 & \dots & \dots & ab & x_2 \end{pmatrix}, \quad (271)$$

where a, b are non-zero real numbers. We need to evaluate and bound

$$\begin{aligned} E_k &:= b_k(a^2 + b^2, a^2 + b^2), \\ F_k &:= b_k(a^2, a^2 + b^2), \\ G_k &:= b_k(a^2 + b^2, b^2), \\ H_k &:= b_k(a^2, b^2). \end{aligned} \quad (272)$$

First note that if

$$A_k = \begin{pmatrix} a & b & 0 & 0 & \dots & 0 & 0 \\ 0 & a & b & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & 0 & 0 & \dots & a & b \end{pmatrix}_{k \times (k+1)}, \quad (273)$$

then, $A_k^T \times A_k = B_{k+1}(a^2, b^2)$ and $A_k \times A_k^T = B_k(a^2 + b^2, a^2 + b^2)$. Thus, $B_{k+1}(a^2, b^2)$ and $B_k(a^2 + b^2, a^2 + b^2)$ are non-negative-definite matrices. Since $\det^+(A_k^T \times A_k) = \det^+(A_k \times A_k^T)$, we conclude that

$$H_{k+1} = E_k. \quad (274)$$

Besides, as $B_k(a^2, a^2 + b^2)$ and $B_k(a^2 + b^2, b^2)$ are principal submatrices of $B_{k+1}(a^2, b^2)$, they are also non-negative-definite as well. The non-negative-definite property of $B_k(a^2 + b^2, a^2 + b^2)$, $B_k(a^2, a^2 + b^2)$ and $B_k(a^2 + b^2, b^2)$ implies that their determinants coincide with their \det^+ if they are full-rank. Below, we evaluate the determinants and as they are non-zero, they coincide with their \det^+ .

We start by the recurrence relation of E_k (the det version) as

$$\begin{cases} E_1 = a^2 + b^2 \\ E_2 = a^4 + b^4 - a^2b^2 \\ E_k = (a^2 + b^2)E_{k-1} - a^2b^2E_{k-2} \end{cases}. \quad (275)$$

It is not difficult to solve the above constant-coefficient linear recursive equation to find

$$E_k = \frac{a^{2k+2} - b^{2k+2}}{a^2 - b^2}, \quad (276)$$

if $a^2 \neq b^2$, and

$$E_k = a^{2k}(1+k), \quad (277)$$

if $a^2 = b^2$. Using (274), H_k is also obtained as

$$H_k = \begin{cases} \frac{a^{2k} - b^{2k}}{a^2 - b^2}, & a \neq b, \\ k a^{2k-2}, & a = b. \end{cases} \quad (278)$$

Using these identities, one can show that

$$e_l^k \leq E_k = H_{k+1} \leq e_u^k, \quad (279)$$

where $e_l := a^2$ and $e_u := a^2 + b^2$.

If we expand the determinant with respect to the first row of the matrix, we can express F_k and G_k in terms of E_k as

$$F_k = a^2 E_{k-1} - a^2 b^2 E_{k-2} = a^{2k}, \quad (280)$$

and

$$G_k = b^2 E_{k-1} - a^2 b^2 E_{k-2} = b^{2k}. \quad (281)$$

By convention, we set $E_0 = F_0 = G_0 = 1$.

• **Step (iii):** Let ς denote the Gramian matrix $A_n^\top A_n = B_{n+1}(a^2, b^2)$. We know that

$$(\det^+ A_n^{[s]})^2 = \det^+ ((A_n^{[s]})^\top A_n^{[s]}) = \det^+ \varsigma_s, \quad (282)$$

where ς_s is the principal submatrix of ς formed by columns and rows for which $s_i = 1$.

Because ς is a tridiagonal matrix, ς_s is a block-diagonal matrix consisting of blocks associated with 1-blocks in \mathbf{s} . More specifically, by definition of $\varphi_i(\mathbf{s})$ in (269) and E_k, F_k, G_k, H_k in Step (ii), we conclude that

$$\det^+ \varsigma_s = F_{\varphi_1(\mathbf{s})} G_{\varphi_n(\mathbf{s})} H_{\varphi_{n+1}(\mathbf{s})} \prod_{i \in [2:n-1]} E_{\varphi_i(\mathbf{s})}. \quad (283)$$

• **Step (iv):** In this step, we show that $\mathbb{E}_Y[\log E_Y]$ exists and is bounded when Y has the following α -geometric distribution:

$$\mathbb{P}(Y = k) = \alpha^k (1 - \alpha), \quad k=0,1,\dots \quad (284)$$

Due to (279), we know that

$$k \log e_l \leq \log E_k \leq k \log e_u. \quad (285)$$

Therefore,

$$\underbrace{\mathbb{E}_Y[Y]}_{\frac{1}{1-\alpha}} \log e_l \leq \mathbb{E}_Y[\log E_Y] \leq \underbrace{\mathbb{E}_Y[Y]}_{\frac{1}{1-\alpha}} \log e_u. \quad (286)$$

Note that $\mathbb{E}_Y[\log E_Y] = \sum_{k=0}^{\infty} \mathbb{P}(Y = k) \log E_k$. Based on (276) and (277), we know that E_k is increasing for large values

of k if $\max(|a|, |b|) \geq 1$ and decreasing for large values of k otherwise. Thereby, the sign of $\log E_k$ remains the same for large k s. This shows that the terms in $\sum_{k=0}^{\infty} \mathbb{P}(Y = k) \log E_k$ after some k , are all positive or negative. Besides, the sum is bounded; hence, because of the monotone convergence theorem [46, pp. 125] the sum is convergent and bounded.

• **Step (v):** Our goal is to show that for $\alpha < 1$ (the distribution is not absolutely continuous), $\frac{1}{n} \mathbb{E}_\nu[\log \det^+(A^{[\nu]})]$ asymptotically approaches $\frac{1-\alpha}{2} \mathbb{E}_Y[\log E_Y]$ when $n \rightarrow \infty$, where Y is an α -geometric RV. To show this, first note that

$$\begin{aligned} \mathbb{E}_\nu[\log \det^+(A^{[\nu]})] &= \frac{1}{2} \mathbb{E}_\nu[\log F_{\varphi_1(\nu)} + \log G_{\varphi_n(\nu)}] \\ &\quad + \frac{1}{2} \alpha^n \log H_n + \frac{1}{2} \sum_{i=2}^{n-1} \mathbb{E}_\nu[\log E_{\varphi_i(\nu)}]. \end{aligned} \quad (287)$$

We evaluate the involved terms separately:

$$\begin{aligned} \mathbb{E}_\nu[\log F_{\varphi_1(\nu)} + \log G_{\varphi_n(\nu)}] &= \sum_{k=1}^{n-1} 2k \alpha^k (1 - \alpha) \log(|ab|) \\ &= \frac{2\alpha(1 - n\alpha^{n-1} + (n-1)\alpha^n)}{1 - \alpha} \log(|ab|). \end{aligned} \quad (288)$$

As $\alpha < 1$, it is easy to check that $\lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_\nu[\log F_{\varphi_1(\nu)} + \log G_{\varphi_n(\nu)}] = 0$. Similarly, from (279), we have that

$$\alpha^n (n-1) \log(e_l) \leq \alpha^n \log(H_n) \leq \alpha^n (n-1) \log(e_u). \quad (289)$$

Thus, $\lim_{n \rightarrow \infty} \frac{1}{n} \alpha^n \log(H_n) = 0$.

Finally, we consider

$$\begin{aligned} \sum_{i=2}^{n-1} \mathbb{E}_\nu[\log E_{\varphi_i(\mathbf{s})}] &= \sum_{i=2}^{n-1} \sum_{k=1}^{n-i} \alpha^k (1 - \alpha)^2 \log(E_k) \\ &= \sum_{k=1}^{n-2} (n-k) \alpha^k (1 - \alpha)^2 \log(E_k) \\ &= n(1 - \alpha) \sum_{k=1}^{n-2} \alpha^k (1 - \alpha) \log(E_k) - (1 - \alpha)^2 \sum_{k=1}^{n-2} k \alpha^k \log(E_k) \\ &= n(1 - \alpha) \underbrace{\mathbb{E}_Y[\log E_Y]}_{\Delta_1} - (1 - \alpha)^2 \underbrace{\sum_{k=1}^{n-2} k \alpha^k \log(E_k)}_{\Delta_2} \\ &\quad - n(1 - \alpha) \underbrace{\sum_{k=n-1}^{\infty} \alpha^k (1 - \alpha) \log(E_k)}_{\Delta_2}. \end{aligned} \quad (290)$$

To complete the proof, we need to show $\lim_{n \rightarrow \infty} \frac{\Delta_1}{n} = \lim_{n \rightarrow \infty} \Delta_2 = 0$. The following two qualities are helpful for this purpose:

$$\begin{aligned} \ell_1(n) &:= \sum_{k=n}^{\infty} k \alpha^k \\ &= \frac{-n\alpha^{n+1} + \alpha^{n+1} + n\alpha^n}{(1-\alpha)^2}, \\ \ell_2(n) &:= \sum_{k=1}^n k^2 \alpha^k \end{aligned} \quad (291)$$

$$= \frac{-n^2\alpha^{n+3} + (2n^2 + 2n - 1)\alpha^{n+2} - (n+1)^2\alpha^{n+1} + \alpha^2 + \alpha}{(1-\alpha)^3}. \quad (292)$$

Now, based on (279), we have that

$$\ell_2(n-2)\log(e_l) \leq \Delta_1 \leq \ell_2(n-2)\log(e_u) \quad (293)$$

and

$$\ell_1(n-1)\log(e_l) \leq \Delta_2 \leq \ell_1(n-1)\log(e_u). \quad (294)$$

For both cases, it is now straightforward to conclude that $\lim_{n \rightarrow \infty} \frac{\Delta_1}{n} = \lim_{n \rightarrow \infty} \Delta_2 = 0$.