

Anomaly Detection based on Compressed Data: an Information Theoretic Characterization

Alex Marchioni, *Student Member, IEEE*, Andriy Enttsel, Mauro Mangia, *Member, IEEE*,
Riccardo Rovatti, *Fellow, IEEE*, and Gianluca Setti, *Fellow, IEEE*

Abstract—We analyze the effect of lossy compression in the processing of sensor signals that must be used to detect anomalous events in the system under observation. The intuitive relationship between the quality loss at higher compression and the possibility of distinguishing anomalous behaviours from normal ones is formalized in terms of information-theoretic quantities. Some analytic derivations are made both in a Gaussian framework and in the asymptotic case for what concerns the extent of signals considered.

Analytical conclusions are matched with the performance of practical detectors in a simple case allowing the assessment of different compression/detector configurations.

Index Terms—Outlier detection, lossy compression, rate-distortion curve Internet of Things, Edge computing.

I. INTRODUCTION

A typical scenario for nowadays massive acquisition systems can be modelled as a large number of sensing units, each transforming some physical unknown quantity into samples of random processes that are then transmitted over a network. To reduce transmission bitrate, signals are often compressed by a lossy mechanism that is theoretically capable of preserving useful information. Before reaching some cloud facility in which they will be ultimately stored or processed, the corresponding bitstreams may traverse several levels of hierarchical aggregation and intermediate devices that are often indicated as the *edge* of the cloud [1]. For latency or privacy reasons, some computational tasks may benefit from their deployment at the edge. One of those tasks is the detection of anomalies/novelities.

This is especially true when dealing, for example, with networks that sensorize plants or structures subject to monitoring as depicted in Fig. 1. The aggregated sensor readings may be processed in the cloud for off-line monitoring relying on long-term historical trends, while the outputs of subsets of sensors may be processed at the edge to give low-latency feedback on possible critical events that require immediate intervention.

A. Marchioni, A. Enttsel, M. Mangia and R. Rovatti are with the Department of Electrical, Electronic, and Information Engineering, University of Bologna, 40136 Bologna, Italy, and also with the Advanced Research Center on Electronic Systems, University of Bologna, 40125 Bologna, Italy (e-mail: alex.marchioni@unibo.it, andriy.enttsel@unibo.it, mauro.mangia@unibo.it, riccardo.rovatti@unibo.it).

R. Rovatti is also with the Alma Mater Research Institute for Human Centered AI University of Bologna, 40015 Bologna, Italy

G. Setti is with the Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Torino, Italy, and also with the Advanced Research Center on Electronic Systems (ARCES), University of Bologna, 40125 Bologna, Italy (e-mail: gianluca.setti@polito.it).

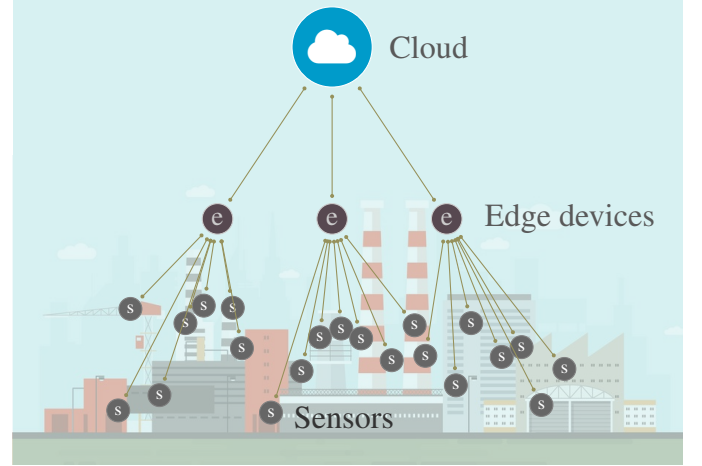


Fig. 1. A sensorized plant whose acquisitions are aggregated at the edge before being sent to the cloud.

Usually, compression schemes applied to sensor data are asymmetric and entail a lightweight encoding performed on very-low complexity devices paired with a possibly expensive decoding stage running on the cloud. In these conditions, it is sensible that anomaly detectors work on compressed data and not on the recovered signal.

Yet, lossy compression bases its effectiveness on neglecting some of the signal details. This translates into a distortion between the original and the recovered signal but also in a loss of details that, in principle, could have been used to tell normal behaviours from anomalous ones.

In general, acquisition systems must obey a distortion constraint so that they are designed to best address the trade-off between compression and distortion. However, such a trade-off goes in parallel to the one between distortion and the ability to determine if the signal is normal or anomalous. Here, we analyze the latter with the same information theoretic machinery used in the well-known rate-distortion analysis and implicitly show that the two trade-offs are different.

How compression affects distinguishability has been investigated in the literature. In [2] the problem of hypothesis testing is discussed for a single source under a rate constraint. Such a basis has been extended to information-theoretic problems of statistical inference in the case of multiterminal data compression in [3]. These works address the inference problem with no constraint on distortion since compressed data is not required to be recoverable. On the contrary, we assume that compression is designed to guarantee the quality of service

needed by the processing tasks that receive the reconstructed data.

In a sense, the framework we identify is somehow similar to the information-bottleneck scheme [4], [5]. In that scheme, distortion is replaced by a very general criterion which identifies the features that should be preserved when compressing with the information that the original signal contains about a second (suitably introduced) signal. Yet, our discussion takes a different direction as, when dealing with anomaly/novelty/outlier, we may completely ignore the statistics of the anomaly and, even if we have priors on that, we need to be able to treat also cases in which the mutual information between normal and anomalous signals is null.

This information-bottleneck principle has also been employed for unsupervised tasks. To tackle one-class classification, in [6], [7] an optimization problem is considered in terms of rate-distortion trade-off and solve it by applying the information-bottleneck principle. However, this trade-off is used for anomaly detection with no consideration about distortion.

Another way to relate unsupervised anomaly detection to data compression is described in [8]. Here, the level of abnormality of a data point with respect to the entire data set, called *coding cost*, is given by its ability to be efficiently compressed in a Huffman coding fashion.

The same reason that differentiates our work from the information-bottleneck principle makes the analysis we propose different from other modifications of classical rate-distortion theory that substitute energy-based distortion with perceptive criteria [9], [10].

Though not overlapping with the problem we address, it is also worthwhile to mention [11], [12], in which it is assumed that the original signal is characterized by some parameters (e.g., their mean) and study how the estimation of such parameters is affected by lossy compression.

Note also that other applications exist in which rate and distortion are paired with additional merit figures taking into account relevant features of the system. As an example [13] adds computational effort considerations to the analysis of rate-distortion of wavelet-based video coding.

Finally, even without emphasis on compression, the relationship between the analysis of suitably defined subcomponents of a signal to detect possible outlier behaviours is a classic theme that is still under investigation [14], [15], [16].

In this paper, we propose an analysis of the performance of a generic detector working on a signal distorted by the compression mechanism that minimizes the rate given a constraint on distortion. To characterize the detector, we define two information-theoretic measures of distinguishability to model anomaly-agnostic and anomaly-aware scenarios. Specializing our analysis to the case of Gaussian sources, we show that: *i*) the distinguishability metrics in case of white anomalies are representative of the average performance of the detector evaluated on many other different anomalies; *ii*) as the signal dimension increases, any possible anomaly tends to resemble the white anomaly; *iii*) in case of an anomaly-agnostic detector, there exists at least one critical distortion level that makes the white anomaly undetectable.

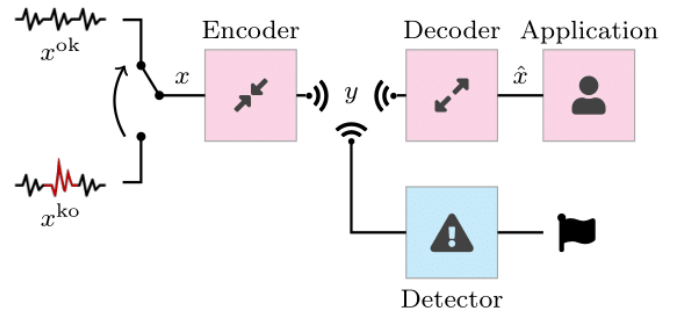


Fig. 2. The signal chain is tuned on the normal signal x^{ok} to best address the rate-distortion trade-off, guaranteeing a certain quality of service to a given application. An anomalous signal x^{ko} may occur and a detector working on the compressed signal y should be able to detect it.

The paper is organised as follows. Section II reviews the classical rate-distortion theory in a general setting first and then in the specific case of Gaussian sources with considerations on the optimal encoding mapping expression. Section III provides the definition of the normal and anomalous signals together with the formulation of the distinguishability measures for both anomaly-agnostic and anomaly-aware scenarios. Section IV focuses on the distinguishability in the average case, with an emphasis on the asymptotic characterization of high-dimensional signals. Section V reports some numerical evidence analysing the behaviour of some suitably simplified anomaly detection strategies with respect to ideal and sub-optimal compression strategies. Theoretical curves anticipate many aspects of practical performance trends and show that compression that optimizes the rate-distortion trade-off is not necessarily addressing at best the compromise with distinguishability. The conclusion is finally drawn. Proofs of the theorems and lemmas stated in the discussion are reported in the Appendix.

II. RATE VS. DISTORTION

We consider the context in which a system has the main task of transferring the information content of a signal source x to a receiver through a communication channel that has a constraint on rate. At any time instant t , an instance $x[t]$ is passed to an encoding stage producing a compressed version $y[t]$ that may then be decompressed into $\hat{x}[t] \in \mathbb{R}^n$, where $\mathbb{R}^n \subset \mathbb{R}^n$.

The constraint on rate is such that it implies a lossy compression mechanism. The encoding stage is therefore not injective and introduces some distortion. The encoder is tuned on the source x , which is modelled as a independent discrete-time, n -dimensional stochastic processes.

The trade-off between rate and distortion is addressed in the rate-distortion theory [17, Chapter 13]. Distortion may be defined as

$$D = \mathbf{E} [\|x[t] - \hat{x}[t]\|^2] \quad (1)$$

where $\mathbf{E}[\cdot]$ stands for expectation, and the minimal achievable rate ρ can be expressed as a function of the maximal accepted

distortion δ as follows [17, Theorem 13.2.1]

$$\rho(\delta) = \inf_{f_{\hat{x}|x}} I(\hat{x}; x) \quad \text{s.t. } D \leq \delta \quad (2)$$

where $I(\hat{x}; x)$ is the mutual information between \hat{x} and x [17, Chapter 8], and $f_{\hat{x}|x}$ is a conditional probability density function (PDF) modeling the possibly stochastic mapping characterizing the encoder-decoder pair. Although [17, Theorem 13.2.1] defines the rate-distortion function in the discrete case, it can also be proved for well-behaved continuous sources [17, Chapter 13] as considered in this work.

If the source is memoryless (thus allowing us to drop the time index t) and generates vectors of independent and zero-mean Gaussian variables, i.e., when $x \sim \mathcal{G}(0, \Sigma)$ where Σ is a diagonal covariance matrix such that $\Sigma = \text{diag}(\lambda_0, \dots, \lambda_{n-1})$ with $\lambda_0 \geq \lambda_1 \geq \dots \geq \lambda_{n-1} \geq 0$, then the solution of (2) is

$$\rho = \frac{1}{2} \sum_{j=0}^{n-1} \log_2 \frac{\lambda_j}{\min\{\theta, \lambda_j\}} = -\frac{1}{2} \sum_{j=0}^{n-1} \log_2 \tau_j \quad (3)$$

$$\delta = \sum_{j=0}^{n-1} \min\{\theta, \lambda_j\} = \sum_{j=0}^{n-1} \lambda_j \tau_j \quad (4)$$

where $\theta \in [0, \lambda_0]$ is the so called reverse water-filling parameter [17, Theorem 13.3.3], and $\tau_j = \min\{1, \theta/\lambda_j\}$ accounts for the fraction of energy cancelled by distortion along the j -th component.

The coding theorems behind such a classical development imply that the optimal trade-off (2) between rate and distortion is asymptotically obtained by simultaneously encoding an increasing number of subsequent source symbols into a single block that can be then reverted to a sequence of distorted symbols. Hence, in principle, the intermediate symbols y feeding the anomaly detector in Fig. 2 cause it to work simultaneously on multiple instances of the signals.

Though this is not incoherent with what happens in real detectors that observe more than one suspect instance before declaring an anomaly, we here instead consider a *per-use* analysis which is typical and scales the key merit figures (rate, distortion and, in our case, distinguishability – see Section III) by the number of source symbols aggregated to obtain them.

This allows us to pursue the classical approach defining a test channel whose single use has the same expected behaviour as the average of infinite uses and, in the case of Gaussian sources, has a particularly simple expression that we derive and exploit to imagine that a source instance x is encoded into a compressed symbol y from which \hat{x} can be recovered [17, Chapter 13], [18].

In the same Gaussian framework, it is also possible to derive the PDF of the distorted signal \hat{x} and the conditional PDF $f_{\hat{x}|x}$ that stochastically maps an input $x \sim \mathcal{G}(0, \Sigma)$ to \hat{x} . If we accept to identify a zero-variance Gaussian with a Dirac's delta and define $S_\theta = I_n - T_\theta$ with $T_\theta = \text{diag}(\tau_0, \dots, \tau_{n-1})$ to account for the fraction of energy that survives distortion along each component, then we can derive the following Lemma whose proof is in the Appendix.

Lemma 1. *If $x \sim \mathcal{G}(0, \Sigma)$ is a memory-less source and we constraint the distortion $D \leq \delta$, the optimally distorted signal has distribution*

$$\hat{x} \sim \mathcal{G}(0, \Sigma S_\theta) \quad (5)$$

and the optimal encoding mapping is

$$f_{\hat{x}|x}(\alpha, \beta) = G_{\beta S_\theta, \Sigma S_\theta T_\theta}(\alpha) \quad (6)$$

where $G_{m,K}(\cdot)$ represents the PDF of a Gaussian variable with mean m and covariance matrix K .

Although in general it is not explicitly reported, the expression of $f_{\hat{x}|x}$ is important when the compression mechanism is employed to encode a signal different from the one for which it was designed. This is the case of an unexpected anomalous source that replaces the normal signal.

III. ANOMALIES AND THEIR DETECTABILITY

In the path from encoder to decoder, the compressed signal y may be intercepted for some local processing. The local processing we focus on is the task of distinguishing whether the transmitted signal differs from what is usually observed, i.e., anomaly detection.

To include this aspect in our model, each observable instance $x[t]$ has to be considered as a realization of two different sources: one modeling the normal behaviour x^{ok} and one representing an anomaly x^{ko} . These two sources are modelled as two discrete-time, stationary, n -dimensional stochastic processes each generating independent and identically distributed (i.i.d.) vectors $x^{\text{ok}} \in \mathbb{R}^n$ and $x^{\text{ko}} \in \mathbb{R}^n$ with different PDFs $f^{\text{ok}} : \mathbb{R}^n \rightarrow \mathbb{R}^+$ and $f^{\text{ko}} : \mathbb{R}^n \rightarrow \mathbb{R}^+$. As a result, at any time t the observable process is either $x[t] = x^{\text{ok}}[t]$ or $x[t] = x^{\text{ko}}[t]$ (visually represented in Fig. 2). Since, we assume the generated vectors as i.i.d. from now on we may drop time indication.

More specifically, according to the framework characterizing Lemma 1, we here consider the case in which both sources are Gaussian. In particular we focus on signals with zero-mean and covariance matrices $\Sigma^{\text{ok}}, \Sigma^{\text{ko}} \in \mathbb{R}^{n \times n}$. In general, $\Sigma^{\text{ok}} \neq \Sigma^{\text{ko}}$, but we will assume $\text{tr}(\Sigma^{\text{ok}}) = \text{tr}(\Sigma^{\text{ko}}) = n$, where $\text{tr}(\cdot)$ stands for matrix trace, meaning that, on the average, each sample in the vector contributes with a unit energy. With the assumption of signals to be zero-mean and of equal energy, we can focus our analysis on one of the possible effects of anomalies, i.e., the distribution of energy over the signal subspace.

Moreover, with no loss of generality, we assume $\Sigma^{\text{ok}} = \text{diag}(\lambda_0^{\text{ok}}, \dots, \lambda_{n-1}^{\text{ok}})$ with $\lambda_0^{\text{ok}} \geq \lambda_1^{\text{ok}} \geq \dots \geq \lambda_{n-1}^{\text{ok}} \geq 0$.

The signal x is encoded with a compression mechanism tailored for the typical condition in which $x = x^{\text{ok}}$. The objective consists in guaranteeing a proper quality of service $D = \mathbb{E}[\|x^{\text{ok}}[t] - \hat{x}^{\text{ok}}[t]\|^2] \leq \delta$ to the final user. Hence, in this specific case, the rate-distortion function in (3) considers $\Sigma = \Sigma^{\text{ok}}$ and $f_{\hat{x}|x} = f_{\hat{x}|x}^{\text{ok}}$.

Simultaneously, a detector observes y for anomaly detection. Since we assume the decoding stage to be injective, y brings the same information of \hat{x} so that, in abstract terms, processing y is equivalent to working on \hat{x} . As a result, the

detector works on the difference between the two marginal distributions $f_{\hat{x}}^{\text{ok}}$ and $f_{\hat{x}}^{\text{ko}}$ that can be computed as follows

$$f_{\hat{x}}^{\text{ok}}(\alpha) = \int_{\mathbb{R}^n} f_{\hat{x}|x}^{\text{ok}}(\alpha, \beta) f_x^{\text{ok}}(\beta) d\beta \quad (7)$$

$$f_{\hat{x}}^{\text{ko}}(\alpha) = \int_{\mathbb{R}^n} f_{\hat{x}|x}^{\text{ok}}(\alpha, \beta) f_x^{\text{ko}}(\beta) d\beta \quad (8)$$

From (8), it is evident that the compression mechanism $f_{\hat{x}|x}^{\text{ok}}$ that optimally addresses the rate-distortion trade-off for the normal source is used also on the anomalous instances. Under the i.i.d. Gaussian assumption, (7) reduces to (5) with $\Sigma = \Sigma^{\text{ok}}$, while the PDF of \hat{x}^{ko} is given by the following Lemma, whose proof is in the appendix.

Lemma 2. *If an anomalous source $x^{\text{ko}} \sim \mathcal{G}(0, \Sigma^{\text{ko}})$ is encoded with the compression scheme $f_{\hat{x}|x}^{\text{ok}}$ of Lemma 1, then*

$$\hat{x}^{\text{ko}} \sim \mathcal{G}(0, S_{\theta} \Sigma^{\text{ko}} S_{\theta} + \theta S_{\theta}) \quad (9)$$

Such a result has two noteworthy corner cases.

- If $\theta \rightarrow 0^+$ there is no distortion. In fact, since $S_{\theta} = I_n$, Lemma 2 gives $\hat{x}^{\text{ko}} \sim x^{\text{ko}}$.
- If $x^{\text{ko}} \sim x^{\text{ok}}$ there is no anomaly, $\Sigma^{\text{ok}} = \Sigma^{\text{ko}}$, and

$$S_{\theta} \Sigma^{\text{ko}} S_{\theta} + \theta S_{\theta} = [S_{\theta} + \theta(\Sigma^{\text{ok}})^{-1}] \Sigma^{\text{ok}} S_{\theta} = \Sigma^{\text{ok}} S_{\theta}$$

where the last equality holds since $S_{\theta} = \max\{0, I_n - \theta(\Sigma^{\text{ok}})^{-1}\}$, the possible disagreements between $S_{\theta} + \theta(\Sigma^{\text{ok}})^{-1}$ and I_n correspond to components multiplied by zero by the last S_{θ} factor. Hence, Lemma 2 can be compared with Lemma 1 to confirm that $\hat{x}^{\text{ko}} \sim \hat{x}^{\text{ok}}$.

Lemma 1 and Lemma 2 imply that when the normal and anomalous signals are Gaussian before compression, performance of anomaly detectors depends on how much we are capable of distinguishing between the two distributions in (5) and (9). We quantify the difference between them with two kinds of information-theoretic measures, which model two distinct scenarios, one in which the detector knows both $f_{\hat{x}}^{\text{ok}}$ and $f_{\hat{x}}^{\text{ko}}$ and one in which it knows only $f_{\hat{x}}^{\text{ok}}$.

To proceed further it is convenient to define the functional

$$L(x'; x'') = - \int_{\mathbb{R}^n} f_{x'}(\alpha) \log_2 [f_{x''}(\alpha)] d\alpha \quad (10)$$

that is the average coding rate, measured in bits per symbol, of a source characterized by the PDF $f_{x'}$ with a code optimized for a source with PDF $f_{x''}$, so that $L(x; x)$ is equal to the differential entropy of x [17, Chapter 8]. As an alternative statistical point of view, if $f_{x'}$ is the PDF of the symbols generated by a source x' , $f_{x''}$ is the PDF of the symbols generated by a source x'' and $\ell_x(\alpha) = -\log_2 f_x(\alpha)$ is the negative log-likelihood that the symbol α has been generated by the sources x , then $L(x'; x'') = \mathbf{E}[\ell_{x''}(\alpha)|x']$, i.e., the average negative likelihood that an instance is generated by the source x'' when it is actually generated by the source x' .

Within the Gaussian assumption, we can derive the analytical expression for L in the following Lemma whose derivation is in the appendix.

Lemma 3. *If $x' \sim \mathcal{G}(0, \Sigma')$ and $x'' \sim \mathcal{G}(0, \Sigma'')$ then*

$$L(x'; x'') = \frac{1}{2 \ln 2} \{ \ln [(2\pi)^n |\Sigma''|] + \text{tr} [(\Sigma'')^{-1} \Sigma'] \} \quad (11)$$

where $|\cdot|$ indicates the determinant of its matrix argument.

A. Distinguishability in anomaly-agnostic detection

When $f_{\hat{x}}^{\text{ko}}$ is unknown and only $f_{\hat{x}}^{\text{ok}}$ is given, we can only consider the average coding rates referring to code optimized for \hat{x}^{ok} , i.e., $L(\hat{x}^{\text{ko}}; \hat{x}^{\text{ok}})$ and $L(\hat{x}^{\text{ok}}; \hat{x}^{\text{ok}})$. One may quantify the difference between the normal behaviour and an anomalous one by measuring the increase or decrease in the average coding rate with respect to the expected case $L(\hat{x}^{\text{ok}}; \hat{x}^{\text{ok}})$ as follows:

$$\zeta = L(\hat{x}^{\text{ko}}; \hat{x}^{\text{ok}}) - L(\hat{x}^{\text{ok}}; \hat{x}^{\text{ok}}) \quad (12)$$

$$= \int_{\mathbb{R}^n} [f_{\hat{x}}^{\text{ok}}(\alpha) - f_{\hat{x}}^{\text{ko}}(\alpha)] \log_2 f_{\hat{x}}^{\text{ok}}(\alpha) d\alpha \quad (13)$$

Since there may be anomalies whose encoding yields a lower rate with respect to normal signals, ζ is not always positive. As a result, a distinguishability measure is given by considering its magnitude, i.e., $|\zeta|$.

From a statistical perspective, ζ corresponds to the difference in the expectations of the negative log-likelihood that α is normal given either α is actually an instance of \hat{x}^{ok} or \hat{x}^{ko}

$$\zeta = \mathbf{E}[\ell_{\hat{x}}^{\text{ok}}(\alpha)|\hat{x}^{\text{ko}}] - \mathbf{E}[\ell_{\hat{x}}^{\text{ok}}(\alpha)|\hat{x}^{\text{ok}}]$$

The use of the quantity $\ell_{\hat{x}}^{\text{ok}}(\alpha) = -\log_2 f_{\hat{x}}^{\text{ok}}(\alpha)$ can be found in other anomaly detection related works, e.g., in [8] where it is referred as a *coding cost* of α .

With the assumption of Gaussian sources, the optimal encoder (in the rate-distortion sense) lets survive only the components j for which $\lambda_j^{\text{ok}} > \theta$. Hence, $f_{\hat{x}}^{\text{ok}}$ and $f_{\hat{x}}^{\text{ko}}$ given in (5) and (9) have only the first n_{θ} components non-null with $n_{\theta} = \arg \max_j \{\lambda_j^{\text{ok}} > \theta\}$. The other $n - n_{\theta}$ components are set to 0 and thus cannot be used to tell anomalous from normal cases. We therefore focus on the first n_{θ} components of \hat{x}^{ok} and \hat{x}^{ko} which are Gaussian with covariance matrices $\hat{\Sigma}_{\theta}^{\text{ok}}$ and $\hat{\Sigma}_{\theta}^{\text{ko}}$ corresponding to the $n_{\theta} \times n_{\theta}$ upper-left submatrix of $\Sigma^{\text{ok}} S_{\theta}$ in (5) and of $S_{\theta} \Sigma^{\text{ok}} S_{\theta} + \theta S_{\theta}$ in (9), respectively.

By properly combining the definition of ζ in (12) with the expression of L within the Gaussian assumption in (11), we obtain

$$\zeta = \frac{1}{2 \ln 2} \text{tr} [\tilde{\Sigma}_{\theta} - I_{n_{\theta}}] \quad (14)$$

where $\tilde{\Sigma}_{\theta} = (\hat{\Sigma}_{\theta}^{\text{ok}})^{-1} \hat{\Sigma}_{\theta}^{\text{ko}}$ which corresponds to the $n_{\theta} \times n_{\theta}$ upper-left submatrix of $(\Sigma^{\text{ok}})^{-1} \Sigma^{\text{ko}} S_{\theta} + T_{\theta}$. Note that, since $\tilde{\Sigma}_{\theta}$ is linear with respect to $\hat{\Sigma}_{\theta}^{\text{ko}}$, so is ζ . In addition, ζ vanishes when $\hat{\Sigma}_{\theta}^{\text{ok}} = \hat{\Sigma}_{\theta}^{\text{ko}}$.

As a noteworthy particular case, when the normal signal is white, i.e., when $\Sigma^{\text{ok}} = I_n$, we have that $\theta \in [0, 1]$ and that for any $\theta < 1$, $T_{\theta} = \theta I_n$ and $n_{\theta} = n$. Hence, $\tilde{\Sigma}_{\theta} = (1 - \theta) \Sigma^{\text{ko}} + \theta I_n$ that leads to $\zeta = 0$. This result is not surprising since the distinguishability modelled by $|\zeta|$ depends only on the statistics of x^{ok} that has no exploitable structure.

B. Distinguishability in anomaly-aware detection

When both $f_{\hat{x}}^{\text{ok}}$ and $f_{\hat{x}}^{\text{ko}}$ are known, the anomaly detection task reduces to a binary classification problem for which we may resort to the Neyman Pearson Lemma [17, Theorem 12.7.1], [19, Theorem 3.1]. This lemma can be understood in the sense that the cardinal quantity to observe is

$$r(\alpha) = \log_2 \left[\frac{f_{\hat{x}}^{\text{ko}}(\alpha)}{f_{\hat{x}}^{\text{ok}}(\alpha)} \right]$$

which can be interpreted as a measure of abnormality of α , i.e., a score that the detector employs to distinguish whether the single α behaves normally or not. Consequently, one may measure the distinguishability between the distributions $f_{\hat{x}}^{\text{ok}}$ and $f_{\hat{x}}^{\text{ko}}$ as the difference between the score observed in average when $\hat{x} = \hat{x}^{\text{ok}}$ and the score obtained in average when $\hat{x} = \hat{x}^{\text{ko}}$.

$$\kappa = \mathbf{E} [r(\alpha)|\hat{x}^{\text{ko}}] - \mathbf{E} [r(\alpha)|\hat{x}^{\text{ok}}] \quad (15)$$

$$= \int_{\mathbb{R}^n} f_{\hat{x}}^{\text{ko}}(\alpha) \log_2 \left[\frac{f_{\hat{x}}^{\text{ko}}(\alpha)}{f_{\hat{x}}^{\text{ok}}(\alpha)} \right] d\alpha + \int_{\mathbb{R}^n} f_{\hat{x}}^{\text{ok}}(\alpha) \log_2 \left[\frac{f_{\hat{x}}^{\text{ok}}(\alpha)}{f_{\hat{x}}^{\text{ko}}(\alpha)} \right] d\alpha \quad (16)$$

$$= L(\hat{x}^{\text{ko}}; \hat{x}^{\text{ok}}) - L(\hat{x}^{\text{ko}}; \hat{x}^{\text{ko}}) + L(\hat{x}^{\text{ok}}; \hat{x}^{\text{ko}}) - L(\hat{x}^{\text{ok}}; \hat{x}^{\text{ok}}) \quad (17)$$

$$= \mathcal{D}_{\text{KL}}(f_{\hat{x}}^{\text{ko}} \| f_{\hat{x}}^{\text{ok}}) + \mathcal{D}_{\text{KL}}(f_{\hat{x}}^{\text{ok}} \| f_{\hat{x}}^{\text{ko}}) \quad (18)$$

where, given distributions f' and f'' , $\mathcal{D}_{\text{KL}}(f' \| f'')$ refers to the Kullback-Leibler divergence [17, Chapter 2], of which κ results to be the symmetrized version.

The measure κ models a detector that knows the distributions of both normal and anomalous sources such that their optimal codes are also known. From (17), it is evident that κ may be interpreted as the sum of the differences in the average coding rate for both distorted sources with a code optimized for the normal source $L(\hat{x}^{\text{ko}}; \hat{x}^{\text{ok}}) - L(\hat{x}^{\text{ok}}; \hat{x}^{\text{ok}})$ and optimized for the anomalous source $L(\hat{x}^{\text{ok}}; \hat{x}^{\text{ko}}) - L(\hat{x}^{\text{ko}}; \hat{x}^{\text{ko}})$. Since the average coding rate is expected to be shorter when employed to code a source for which it is optimized, these differences are expected to be greater when the difference of two distributions $f_{\hat{x}}^{\text{ok}}$ and $f_{\hat{x}}^{\text{ko}}$ increases. As a result, large κ values correspond to system configurations with high detection capability.

Differently from ζ , κ is a quantity that is always positive and can be directly used as distinguishability measure.

Within the Gaussian assumption, the distinguishability measure κ becomes

$$\kappa = \frac{1}{2 \ln 2} \text{tr} \left[\tilde{\Sigma}_{\theta} + \tilde{\Sigma}_{\theta}^{-1} - 2I_{n_{\theta}} \right] \quad (19)$$

from which it is evident that κ is convex with respect to $\hat{\Sigma}_{\theta}^{\text{ko}}$ and, as for ζ , κ vanishes for $\hat{\Sigma}_{\theta}^{\text{ok}} = \hat{\Sigma}_{\theta}^{\text{ko}}$.

As a final remark, coherently with the typical *per use* analysis, distinguishability measures implicitly consider detectors that scrutiny an increasing number of subsequent source instances and scale their performance by such a number. Hence, as rate and distortion coming from (2) are best-case

bounds that can be approximated by increasing the complexity of the system, the distinguishability measures indicate how fast a detector accumulates information allowing to declare an anomaly. The higher such a figure, the lower the number of subsequent symbols needed to arrive at a conclusion or, alternatively, the higher the confidence in a conclusion drawn after analyzing as single instance.

IV. AVERAGE AND LARGE-WINDOW DISTINGUISHABILITY

A. Average on the set of possible anomalies

Anomalies modelled as zero-mean Gaussian vectors with fixed energy, are completely defined by their covariance matrix Σ^{ko} where $\text{tr}(\Sigma^{\text{ko}}) = n$. We decompose $\Sigma^{\text{ko}} = U^{\text{ko}} \Lambda^{\text{ko}} U^{\text{ko} \top}$ with $\Lambda^{\text{ko}} = \text{diag}(\lambda_0^{\text{ko}}, \dots, \lambda_{n-1}^{\text{ko}})$ and U^{ko} orthonormal.

The set of all possible $\lambda^{\text{ko}} = (\lambda_0^{\text{ko}}, \dots, \lambda_{n-1}^{\text{ko}})^{\top}$ is

$$\mathbb{S}^n = \left\{ \lambda \in \mathbb{R}^{+n} \mid \sum_{j=0}^{n-1} \lambda_j = n \right\}$$

while the set of all possible U^{ko} is that of orthonormal matrices

$$\mathbb{O}^n = \{ U \in \mathbb{R}^{n \times n} \mid U^{\top} U = I_n \}$$

By indicating with $\mathcal{U}(\cdot)$ the uniform distribution in the argument domain, we will assume that when λ^{ko} is not known then $\lambda^{\text{ko}} \sim \mathcal{U}(\mathbb{S}^n)$ and, similarly, when U^{ko} is not known then $U^{\text{ko}} \sim \mathcal{U}(\mathbb{O}^n)$, independently of λ^{ko} .

Note now that \mathbb{S}^n is invariant with respect to any permutation of the λ_j . Since $\lambda^{\text{ko}} \sim \mathcal{U}(\mathbb{S}^n)$, also $\mathbf{E}[\lambda^{\text{ko}}]$ must be invariant with respect to the same permutations so that $\mathbf{E}[\lambda_j^{\text{ko}}] = \mathbf{E}[\lambda_k^{\text{ko}}]$ for any j, k . Since λ^{ok} has a constrained sum and is the diagonal of Λ^{ko} we have $\mathbf{E}[\Lambda^{\text{ko}}] = I_n$. This implies

$$\begin{aligned} \mathbf{E}[\Sigma^{\text{ko}}] &= \mathbf{E} [U^{\text{ko}} \Lambda^{\text{ko}} U^{\text{ko} \top}] \\ &= \mathbf{E} [U^{\text{ko}} \mathbf{E}[\Lambda^{\text{ko}}] U^{\text{ko} \top}] \\ &= \mathbf{E} [U^{\text{ko}} U^{\text{ko} \top}] = I_n \end{aligned} \quad (20)$$

Hence, in our setting, the average anomaly is white and we may compute the corresponding distinguishability measures ζ_I and κ_I , i.e., ζ and κ when $\Sigma^{\text{ko}} = I_n$. Note that, in this case, $\tilde{\Sigma}_{\theta}$ is the $n_{\theta} \times n_{\theta}$ upper-left submatrix of $(\Sigma^{\text{ok}})^{-1} S_{\theta} + T_{\theta}$, which is a diagonal matrix whose diagonal elements are

$$u_{\theta,j} = \frac{1}{\lambda_j^{\text{ok}}} \left(1 - \frac{\theta}{\lambda_j^{\text{ok}}} \right) + \frac{\theta}{\lambda_j^{\text{ok}}}$$

With these quantities, the expressions of the distinguishability measures become

$$\zeta_I = \frac{1}{2 \ln 2} \sum_{j=0}^{n_{\theta}-1} (u_{\theta,j} - 1) \quad (21)$$

$$\kappa_I = \frac{1}{2 \ln 2} \sum_{j=0}^{n_{\theta}-1} \left(u_{\theta,j} + \frac{1}{u_{\theta,j}} - 2 \right) \quad (22)$$

Note that due to the Jensen's inequality, the linearity of ζ and the convexity of κ , we have $\zeta_I = \mathbf{E}[\zeta]$ and $\kappa_I \leq \mathbf{E}[\kappa]$.

Moreover, the very simple structure of ζ_I allows the derivation of the following Theorem whose proof is in the appendix.

Theorem 1. *If $\bar{k} = \arg \max_k \{\lambda_k^{\text{ok}} \geq \lambda_k^{\text{ko}} = 1\}$, then $\zeta_I = 0$ for at least one point $0 < \theta < \lambda_{\bar{k}}^{\text{ok}}$*

Considering a white anomaly, the intuition behind this theorem is the following. When distortion is null (no compression), since \hat{x}^{ko} and \hat{x}^{ok} have the same average energy and the coding is tuned on \hat{x}^{ok} , $L(\hat{x}^{\text{ko}}, \hat{x}^{\text{ok}}) > L(\hat{x}^{\text{ok}}, \hat{x}^{\text{ok}})$ such that ζ_I is positive. On the other hand, when distortion is so high that only the first component of x^{ok} survives, i.e., $\hat{\Sigma}_{\theta}^{\text{ok}} = \lambda_0^{\text{ok}} - \theta$, a single component also survives in \hat{x}^{ko} . In this setting, ζ_I depends on the difference between the two scalar quantities $\hat{\Sigma}_{\theta}^{\text{ok}}$ and $\hat{\Sigma}_{\theta}^{\text{ko}}$. With few numerical manipulations, it is possible to prove that $\hat{\Sigma}_{\theta}^{\text{ok}} > \hat{\Sigma}_{\theta}^{\text{ko}}$ thus ζ_I results to be negative. Since ζ_I is continuous in θ , it must pass through zero at least once. Therefore, at least one critical level of distortion exists that makes the detectors that do not use the information of the anomaly ineffective.

B. Asymptotic distinguishability

White signals are not only the average anomalies but are also *typical* anomalies in a sense specified by the following Theorem whose proof is in the appendix.

Theorem 2. *If $\lambda^{\text{ko}} \sim \mathcal{U}(\mathbb{S}^n)$ and $U^{\text{ko}} \sim \mathcal{U}(\mathbb{O}^n)$ then, as $n \rightarrow \infty$, $\Sigma^{\text{ko}} = U^{\text{ko}} \text{diag}(\lambda_0^{\text{ko}}, \dots, \lambda_{n-1}^{\text{ko}}) U^{\text{ko}\top}$ tends to I_n in probability.*

Hence, when n increases, most of the possible anomalies behave as white signals, i.e., ζ tends to ζ_I , that thus enjoys the property shown in Theorem 1. From an anomaly detection perspective, if the signal is characterized by a sufficiently large dimension n , the designer may consider the white anomaly as a reference.

V. NUMERICAL EXAMPLES

In this section we match the theoretical derivations with the quantitative assessment of the performance of some practical anomaly detectors applied to compressed signals.

Normal signals are assumed to be $x^{\text{ok}} \sim \mathcal{G}(0, \Sigma^{\text{ok}})$ where Σ^{ok} is the diagonal matrix of the eigendecomposition of the matrix $\Sigma = U \Sigma^{\text{ok}} U^\top$, with $\Sigma_{j,k} = \omega^{|j-k|}$, for $j, k = 0, \dots, n-1$ and U an orthonormal matrix. The parameter ω is set to yield a different degree of non-whiteness measured with the so-called *localization* defined as

$$\mathcal{L}_{x^{\text{ok}}} = \frac{\text{tr}(\Sigma^{\text{ok}^2})}{\text{tr}^2(\Sigma^{\text{ok}})} - \frac{1}{n}$$

The localization goes from $\mathcal{L}_{x^{\text{ok}}} = 0$ when the signal is white to $\mathcal{L}_{x^{\text{ok}}} = 1 - \frac{1}{n}$ when all the energy is concentrated along a single direction of the signal space (see [20] for more details). To show the effect of realistic localization [21] we consider values of ω corresponding to $\mathcal{L}_{x^{\text{ok}}} \in \{0, 0.05, 0.2\}$.

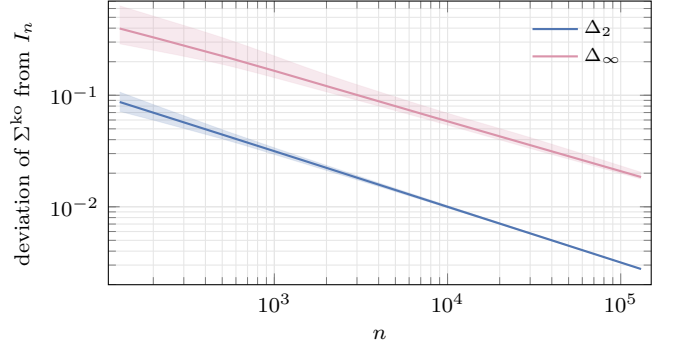


Fig. 3. Trend of $\Delta_2 = \frac{1}{n} \sqrt{\sum_{j,k=0}^{n-1} [\Sigma_{j,k}^{\text{ko}} - (I_n)_{j,k}]^2}$ and $\Delta_\infty = \max_{j,k} |\Sigma_{j,k}^{\text{ko}} - (I_n)_{j,k}|$ when n increases. Solid lines are mean trends while shaded areas contain 98% of the population.

Anomalous signals are generated as $x^{\text{ko}} \sim \mathcal{G}(0, \Sigma^{\text{ko}})$, where $\Sigma^{\text{ko}} = U^{\text{ko}} \Lambda^{\text{ko}} U^{\text{ko}\top}$ is randomly picked according to the uniform distribution defined in Section IV-A.

To generate $\lambda^{\text{ko}} \sim \mathcal{U}(\mathbb{S}^n)$, we follow [22] to first draw $\xi_j \sim \mathcal{U}([0, 1])$ for $j = 0, \dots, n-1$ and then set

$$\lambda_j^{\text{ko}} = \frac{\log \xi_j}{\sum_{k=0}^{n-1} \log \xi_k}$$

To generate $U^{\text{ko}} \sim \mathcal{U}(\mathbb{O}^n)$, we follow [23] and start by generating a matrix A within the Ginibre ensemble [24], i.e., with independent entries $A_{j,k} \sim \mathcal{G}(0, 1)$ for $j, k = 0, \dots, n-1$. We then set U^{ko} to the orthonormal factor of the QR -decomposition of A .

A first use of this random sampling is the possibility of pairing Theorem 2 with some numerical evidence. Fig. 3 reports the vanishing trend of the average squared and uniform deviation from I_n of a population of uniformly distributed covariance matrices Σ^{ko} . Though not a theoretical result, note that empirical evidence supports a classical $1/\sqrt{n}$ convergence.

As far as detector assessment is concerned, we decide to set $n = 32$ and consider three compression techniques tuned to the normal signal and applied to both normal and anomalous instances. More specifically, x is mapped to \hat{x} by

- the minimum-rate-given-distortion compression in (6) (Rate-Distortion Compression RDC);
- projecting x along the subspace spanned by the eigenvectors of Σ^{ok} with the largest eigenvalues (Principal Component Compression PCC);
- a family of autoencoders [25, Chapter 14] with an increasingly deficient latent representation (Auto-Encoder Compression AEC). Assuming that p is the dimensionality of the representation, the encoder is a neural network with fully connected layers of dimensions $n, 4n, 2n, p$, and the decoder is the dual network whose layers have dimensions $2n, 4n$, and n and the number of inputs is p . The family of autoencoders is trained to minimize distortion computed as in (1). To smooth performance degradation we first train an autoencoder with $p = n-1$. Then, the node of the latent representation along which we measure the least average energy is dropped to produce a smaller network with an $(p-1)$ -dimensional latent space. The

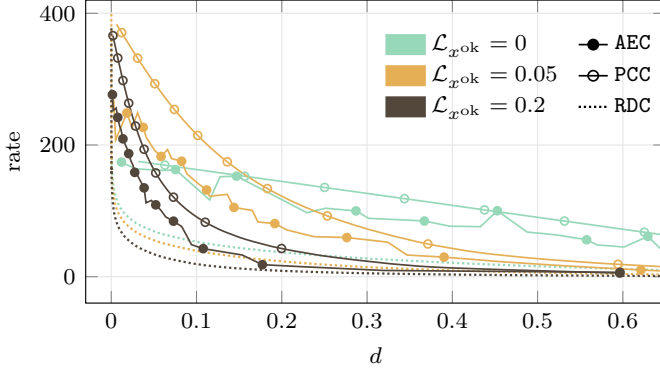


Fig. 4. Rate distortion curves for the three compression schemes we consider and for different value of the localization of the original signal.

obtained network is re-trained using the previous weights as initialization. This process is repeated decreasing p and thus considering larger distortion values.

These three schemes address in a different way the trade-off between compression and distortion. Since we refer to a theoretical model based on continuous quantities and for which rate is potentially infinite, the compressors have to be paired with a quantization stage ensuring that rate values are finite. In particular we encode each component of \hat{x} with 16 bits and this yields rates of less than $16n = 512$ bits per time step. We assume that quantization is fine enough to substantially preserve the Gaussian distribution of \hat{x} and thus evaluate the mutual information between x and \hat{x} as if they were jointly gaussian with a covariance matrix that we estimate by Monte Carlo simulation [26]. Such estimation yields the rate-distortion curves in Fig. 4.

As expected, RDC yields the smallest rates while PCC gives the largest ones. Between the two we have AEC, whose performance depends on the effectiveness of the training.

Note that, only the results of Fig. 4 refer to the additional quantization stage, while in the remaining part of our analysis we consider continuous sources.

The compressed version of the signal is then passed to a detector whose task is to compute a score such that high-score instances should be more likely to be anomalous. The final binary decision is taken by matching the score against a threshold.

We consider two detectors not relying on information of the anomaly

- a Likelihood Detector (LD) whose score is the same considered for ζ , so that to each instance x we associate the score $\ell_{\hat{x}}^{\text{ok}}(\hat{x}) = -\log f_{\hat{x}}^{\text{ok}}(\hat{x})$;
- a One-Class Support-Vector Machine (OCSVM) [27] with a Gaussian kernel¹, trained on a set of instances of normal signals contaminated by 1% of unlabelled white instances to help the algorithm in finding the envelope of normal instances.

We also consider two detectors that are able to leverage information on the anomaly

¹The signal components are normalized by their variance and the scale parameter of the Gaussian kernel is fixed to $1/n_{\theta}$.

TABLE I
NUMBER OF ANOMALIES (Σ^{ko}) AND, FOR EACH ANOMALY, THE NUMBER OF NORMAL (ok) AND ANOMALOUS (ko) SIGNAL INSTANCES USED IN THE TRAINING AND ASSESSMENT OF THE DETECTORS.

detector	training			assessment		
	# Σ^{ko}	#instances $\times \Sigma^{\text{ko}}$ ok	ko	# Σ^{ko}	#instances $\times \Sigma^{\text{ko}}$ ok	ko
LD				10^3	10^3	10^3
OCSVM	1	99×10^3	10^3	10^3	10^3	10^3
NPD				10^3	10^3	10^3
DNN	50	10^5	10^5	50	10^5	10^5

- a Neyman-Pearson Detector (NPD), whose score is the same considered for κ , so that to instance x we associate the score $r(\hat{x}) = \log f_{\hat{x}}^{\text{ko}}(\hat{x}) - \log f_{\hat{x}}^{\text{ok}}(\hat{x})$;
- a Deep Neural Network (DNN) with three fully connected hidden layers with p , $2n$, n neurons with ReLu activations and a final sigmoid neuron producing the score. The network is trained² with a binary cross-entropy loss against a dataset containing labelled normal and anomalous instances.

LD and NPD detectors can be employed only on signals compressed by RDC or by PCC method since they rely on the statistical characterization of the signals that is not available after the nonlinear processing in AEC.

Table I shows how many different anomalies and how many signal instances are generated for the training (when needed) and for the assessment of the detectors. Note that in the DNN case we limited the analysis to 50 anomalies since the training process must be repeated for each of them.

To be independent of the choice of thresholds, detectors' performance is assessed by the Area-Under-the-Curve (AUC) methodology [29]. AUC estimates the probability that given a random normal instance and a random anomalous instance, the former has a lower score with respect to the latter, as it should be in an ideal setting. Hence, AUC is a positive performance index.

Clearly, detectors with $\text{AUC} = \frac{1}{2}$ are no better than coin tossing. Yet, if $\text{AUC} < \frac{1}{2}$, the score has some ability to distinguishing normal and anomalous signals if it is interpreted in a reverse way. Hence, it is convenient to set our *empirical distinguishability* measure to

$$\psi = \begin{cases} \text{AUC} & \text{if } \text{AUC} \geq \frac{1}{2} \\ 1 - \text{AUC} & \text{if } \text{AUC} < \frac{1}{2} \end{cases}$$

Note that, if AUC must be estimated from samples, reversing values lower than $\frac{1}{2}$ is not always possible. There are classes of estimators for which values less than $\frac{1}{2}$ are not reliable [30], [31]. From now on, we report results referring to AUC estimated as in [29] for which reversing values lower than $\frac{1}{2}$ is possible.

²Training of DNN involves the backpropagation algorithm with ADAM optimizer [28], a batch-size of 20 instances, and an initial learning rate of 0.01 that is scaled by 0.2 any 5 epochs for which the validation loss is not decreasing where the validation set consists of the 10% of the instances initially devoted to the training. These training parameters are the result of a tuning.

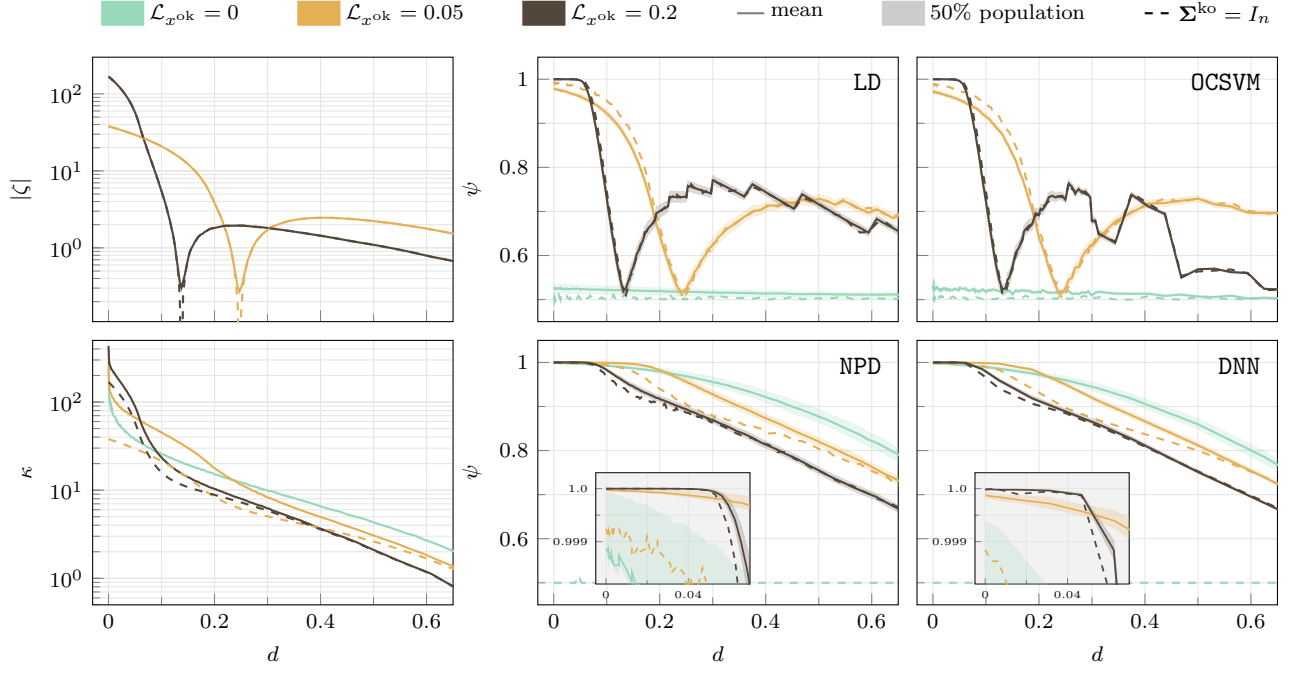


Fig. 5. Distinguishability measures ζ , κ and ψ against normalized distortion d in case of RDC.

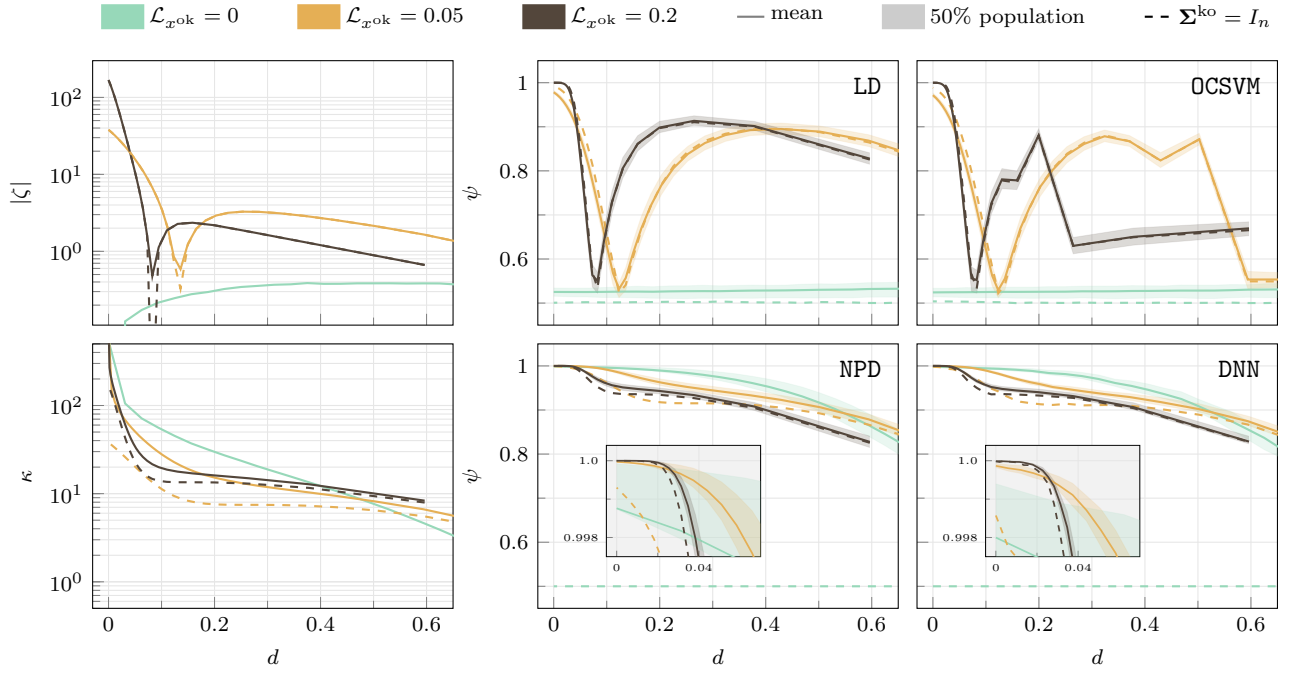


Fig. 6. Distinguishability measures ζ , κ and ψ against normalized distortion d in case of PCC.

In the following, the trends of ψ are reported and matched with the trends of $|\zeta|$ and κ to show how theoretical properties reflect on real cases. Comparisons must be partially qualitative as ζ and κ quantify the distinguishability with bits per symbol while ψ comes from the probability of correct detection. Note also that ζ and κ refer to the difference between the average values of the score in the normal and anomalous cases, while ψ takes into account the entire distributions of these scores.

All plots are made against a normalized distortion $d = D/n$ in the range $d \in [0, 0.64]$ as larger relative distortions are usually beyond operative ranges.

A. RDC

Fig. 5 summarizes the results we have in this case with two rows of 3 plots each. The upper row of plots corresponds to detectors that do not exploit information on the anomaly, while the lower row of plots concerns detectors that may leverage information on the anomaly. Colors correspond to different $\mathcal{L}_{x^{\text{ok}}}$, dashed trends assume that the anomaly is the average one, i.e., white, and shaded areas show the span of 50% of the Monte Carlo population. The profiles of $|\zeta|$ and κ on the left shall be matched with the profiles on the right that correspond to the four detectors we consider. No $|\zeta|$ profile appears for $\mathcal{L}_x = 0$ as in that case $\zeta = 0$.

Numerical results confirm that $\zeta_I = \mathbf{E}[\zeta]$, $\kappa_I \leq \mathbf{E}[\kappa]$ as discussed in Section IV-A. This corroborates the role of the white anomaly as a reference case since it represents the average behaviour in case of anomaly-agnostic detector or a lower bound in the anomaly-aware scenarios. The white anomaly is not only a reference case but also the case to which any possible anomaly tends when n increases as demonstrated in Theorem 2.

Theory also anticipates that without any knowledge of the anomaly (upper row), a limited amount of distortion may cause distinguishability to vanish and thus detectors to fail. This happens for practical detectors such as LD and OCSVM. The distortion level at which detectors fail is also anticipated by $|\zeta|$ and depends on $\mathcal{L}_{x^{\text{ok}}}$ as predicted by Theorem 1. Overall, theoretical measures $|\zeta|$ and κ anticipate that in the low-distortion region, more localized signals are more distinguishable from anomaly though they cause detector failures at smaller distortions with respect to less localized signals.

Detectors leveraging the knowledge of the anomaly (lower row) fail completely only at the maximum level of distortion as revealed by the abstract distinguishability measure κ . Also in this case, by comparing the trend of κ with the zoomed areas in the NPD and DNN plots we see how theoretical measures anticipate that in the low-distortion region more localized signals tend to be more distinguishable from anomalies but cause a more definite performance degradation of detectors when d increases.

B. PCC

From the point of view of the rate-distortion trade-off PCC is largely suboptimal. Yet, due to its linear nature, x and \hat{x} are still jointly Gaussian, so that, also in this case, we can compute the theoretical $|\zeta|$ and κ by means of (21) and (19).

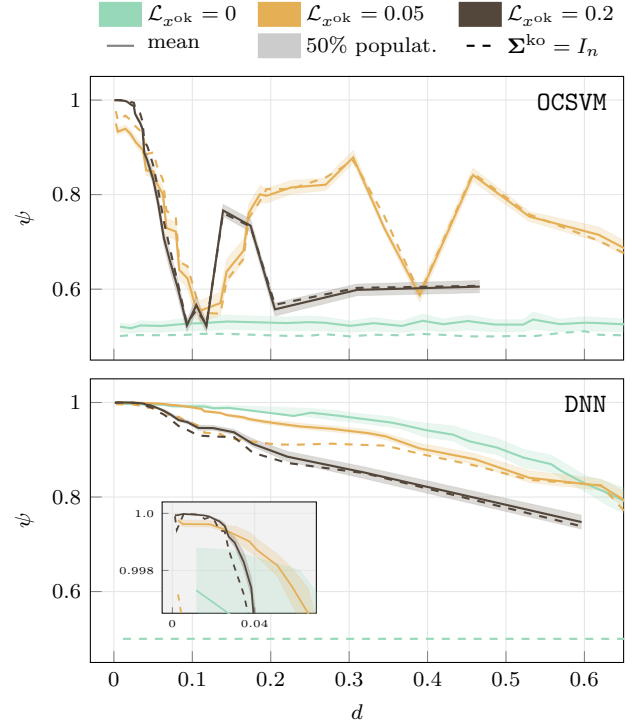


Fig. 7. Distinguishability measure ψ against normalized distortion d in case of AEC.

Fig. 6 summarizes the results we have in this case with plots of the same kind of Fig. 5. The qualitative behaviours commented in the previous subsection appear in the new plots and are anticipated by the trends of the theoretical quantities.

The distortion levels at which anomaly-agnostic detectors fail change with respect to the RDC case but are still anticipated by the theoretical curves and Theorem 1.

In this case, the values of $|\zeta|$ beyond breakdown distortion levels increase slightly more than in the optimal compression scenario. Hence, by adopting a compression strategy that is suboptimal in the rate-distortion sense one may obtain a better distinguishability of the compressed normal signal from the compressed anomalies. This is, indeed, what happens in practice as highlighted by the LD and OCSVM plots in the first row of Fig. 6.

C. AEC

In this case, compression is non-linear so that x and \hat{x} may not be jointly Gaussian. This prevents us from computing the theoretical curves $|\zeta|$ and κ and from applying LD and NPD that rely on the knowledge of the distribution of the signals. For this reason, Fig. 7 reports only the performance of OCSVM and DNN detectors.

Notice how the qualitative trends of those performances still follow, though with a larger level of approximation, what is indicated by the theoretical curves for PCC.

VI. CONCLUSION

Massive sensing systems may rely on lossy compression to reduce the bitrate needed to transmit acquisitions to the cloud

while theoretically maintaining the important information. At some intermediate point along their path to centralized servers, compressed sensor readings may be processed for early detection of anomalies in the systems under observation. Such detection must be performed on compressed data.

To measure detection performance we define two information theory metrics referring to the anomaly-agnostic and anomaly-aware cases, for which a statistical interpretation is also provided.

In a framework approximating normal and anomalous signals with Gaussian sources, we revise the classical rate-distortion theory to report the distributions of the distorted signals, the mapping to obtain them (see Lemma 1 and Lemma 2), and closed forms for the distinguishability metrics.

Focusing on the anomaly-agnostic case, we prove with Theorem 1, and confirm with numerical evidences, that there exists at least one critical level of distortion for which the detector is ineffective.

We also prove that the white anomaly is a reference case that can be employed in the design of the system. Indeed, it provides information about the average and minimum performance in the anomaly-agnostic and anomaly-aware scenarios, respectively. Moreover, we demonstrate with Theorem 2 that any possible anomaly tends to be white in the asymptotic case.

All these results are confirmed with numerical examples in a toy case. We show that the theoretical measure of distinguishability anticipate the performances of real detectors in case of both optimal (in the rate-distortion sense) and sub-optimal compressors.

APPENDIX

Proof of Lemma 1. Distortion is tuned to the normal case that entails a memoryless sources. Hence we may drop time indications and concentrate on a vector x with independent components $x_j \sim \mathcal{G}(0, \lambda_j)$ for $j = 0, \dots, n-1$.

We know from [18] that for a given value of the parameter θ , each component x_j is transformed separately into \hat{x}_j . In particular,

$$\hat{x}_j = \begin{cases} 0 & \text{if } \lambda_j \leq \theta \\ x_j + \Delta_j & \text{if } \lambda_j > \theta \end{cases} \quad (23)$$

where, to achieve the Shannon lower bound, Δ_j must be an instance of a Gaussian random variable independent of \hat{x}_j . Hence, the three quantities \hat{x}_j , x_j and Δ_j must be such that $(\hat{x}_j, x, \Delta_j)^\top \sim \mathcal{G}(0, \Sigma_{\hat{x}_j, x_j, \Delta_j})$ with

$$\Sigma_{\hat{x}_j, x_j, \Delta_j} = \begin{pmatrix} \lambda_j - \theta & \lambda_j - \theta & 0 \\ \lambda_j - \theta & \lambda_j & -\theta \\ 0 & -\theta & \theta \end{pmatrix} \quad (24)$$

That explains in which sense \hat{x}_j encodes x_j . In fact, the non-diagonal elements $\lambda_j - \theta$ are positive and thus \hat{x}_j and x_j are positively correlated.

From (24), if we agree to identify a Gaussian with 0 variance with a Dirac's delta we infer that $\hat{x}_j \sim \mathcal{G}(0, \max\{0, \lambda_j - \theta\})$ and thus $\hat{x} \sim \mathcal{G}(0, \Sigma_{\hat{x}})$.

Moreover, $(\hat{x}_j, x_j)^\top \sim \mathcal{G}(0, \Sigma_{\hat{x}_j, x_j})$ with $\Sigma_{\hat{x}_j, x_j}$ the upper-left 2×2 submatrix of $\Sigma_{\hat{x}_j, x_j, \Delta_j}$ in (24). If we assume

that $\theta < \lambda_j$, from the joint probability of x_j and \hat{x}_j , we may compute the action of $f_{\hat{x}|x}$ on the j -th component of x_j as the PDF of \hat{x}_j given x_j , i.e.,

$$\begin{aligned} f_{\hat{x}_j|x_j}(\alpha, \beta) &= \frac{f_{\hat{x}_j, x_j}(\alpha, \beta)}{f_{x_j}(\beta)} = \frac{G_{0, \Sigma_{\hat{x}_j, x_j}}(\alpha)}{G_{0, \lambda_j}(\beta)} \\ &= \frac{1}{\sqrt{2\pi\lambda_j\tau_j s_j}} \exp\left(-\frac{1}{2} \frac{[\alpha - s_j\beta]^2}{\lambda_j\tau_j s_j}\right) \end{aligned}$$

where $\tau_j = \min\{1, \theta/\lambda_j\} \in [0, 1]$, and $s_j = 1 - \tau_j$. Note that, $f_{\hat{x}_j|x_j}$ becomes $\delta(\alpha)$ for $\tau_j \rightarrow 1$ (maximum distortion of this component implies that the corresponding output is set to 0) and $\delta(\alpha - \beta)$ for $\tau_j \rightarrow 0$ (no distortion of this component, the output is equal to the input).

We may collect the component-wise PDFs into a vector PDF by using the matrix $T_\theta = \text{diag}(\tau_0, \dots, \tau_{n-1}) = \min\{I_n, \theta(\Sigma^{\text{ok}})^{-1}\}$, and the matrix $S_\theta = I_n - T_\theta$ thus yielding the thesis. \square

Proof of Lemma 2. The PDF of \hat{x}^{ko} distorted by means of $f_{\hat{x}|x}^{\text{ok}}$ can be computed as

$$f_{\hat{x}}^{\text{ko}}(\alpha) = \int_{\mathbb{R}^n} f_{\hat{x}, x}^{\text{ko}}(\alpha, \beta) d\beta = \int_{\mathbb{R}^n} f_{\hat{x}|x}^{\text{ok}}(\alpha, \beta) f_x^{\text{ko}}(\beta) d\beta$$

Assume first to be in the low-distortion condition $\theta < \lambda_{n-1}^{\text{ok}}$ that implies $T_\theta = \theta(\Sigma^{\text{ok}})^{-1}$, and write

$$\begin{aligned} f_{\hat{x}}^{\text{ko}}(\alpha) &= \int_{\mathbb{R}^n} G_{S_\theta \beta, \Sigma^{\text{ok}} S_\theta T_\theta}(\alpha) G_{0, \Sigma^{\text{ko}}}(\beta) d\beta \\ &= G_{0, \Sigma^{\text{ok}} S_\theta T_\theta}(\alpha) \times \\ &\quad \int_{\mathbb{R}^n} e^{-\frac{1}{2} [\beta^\top S_\theta (\Sigma^{\text{ok}} S_\theta T_\theta)^{-1} S_\theta \beta - 2\alpha^\top (\Sigma^{\text{ok}} S_\theta T_\theta)^{-1} S_\theta \beta]} \times \\ &\quad G_{0, \Sigma^{\text{ko}}}(\beta) d\beta \\ &= G_{0, \Sigma^{\text{ok}} S_\theta T_\theta}(\alpha) \times \\ &\quad \frac{1}{\sqrt{(2\pi)^n \det \Sigma^{\text{ko}}}} \underbrace{\int_{\mathbb{R}^n} e^{-\frac{1}{2} (\beta^\top Q \beta - 2q^\top \beta)} d\beta}_{g(\alpha)} \end{aligned}$$

with $Q = S_\theta (\Sigma^{\text{ok}} S_\theta T_\theta)^{-1} S_\theta + (\Sigma^{\text{ko}})^{-1} = (\theta I_n)^{-1} - (\Sigma^{\text{ok}})^{-1} + (\Sigma^{\text{ko}})^{-1}$ and $q = (\Sigma^{\text{ok}} S_\theta T_\theta)^{-1} S_\theta \alpha = \alpha/\theta$. To compute $g(\alpha)$ let $Q = UDU^\top$ with D diagonal and U orthonormal, and set $\beta' = D^{1/2} U^\top \beta$ so that $\beta = UD^{-1/2} \beta'$ and $d\beta = d\beta'/\sqrt{\det Q}$. With this write

$$g(\alpha) = \frac{1}{\sqrt{\det Q}} \int_{\mathbb{R}^n} e^{-\frac{1}{2} (\beta'^\top \beta' - 2q^\top UD^{-1/2} \beta')} d\beta'$$

at the exponent of which one may add and subtract $q^\top Q^{-1} q = q^\top UD^{-1/2} D^{-1/2} U^\top q$ to yield

$$\begin{aligned} g(\alpha) &= \frac{1}{\sqrt{\det Q}} \int_{\mathbb{R}^n} e^{-\frac{1}{2} (\|\beta' - D^{-1/2} U^\top q\|^2 - q^\top Q^{-1} q)} d\beta' \\ &= \sqrt{\frac{(2\pi)^n}{\det Q}} e^{\frac{1}{2} q^\top Q^{-1} q} \end{aligned}$$

Putting this back into $f_{\hat{x}}^{\text{ok}}$ we get

$$f_{\hat{x}}^{\text{ko}}(\alpha) = G_{0,[(\theta I_n)^{-1} - (\Sigma^{\text{ok}})^{-1} + (\Sigma^{\text{ko}})^{-1}] \Sigma^{\text{ko}} \Sigma^{\text{ok}} S_{\theta} T_{\theta}}(\alpha)$$

A straightforward expansion of the definitions under the low-distortion assumption finally rearranges the covariance matrix into

$$\begin{aligned} & [(\theta I)^{-1} - (\Sigma^{\text{ok}})^{-1} + (\Sigma^{\text{ko}})^{-1}] \Sigma^{\text{ko}} \Sigma^{\text{ok}} S_{\theta} T_{\theta} = \\ & = [(\theta I_n)^{-1} - (\Sigma^{\text{ok}})^{-1} + (\Sigma^{\text{ko}})^{-1}] \Sigma^{\text{ko}} \Sigma^{\text{ok}} \theta (\Sigma^{\text{ok}})^{-1} S_{\theta} \\ & = [\Sigma^{\text{ko}} - \theta (\Sigma^{\text{ok}})^{-1} \Sigma^{\text{ko}} + \theta I_n] S_{\theta} \\ & = [I_n - \theta (\Sigma^{\text{ok}})^{-1}] \Sigma^{\text{ko}} S_{\theta} + \theta S_{\theta} \\ & = S_{\theta} \Sigma^{\text{ko}} S_{\theta} + \theta S_{\theta} \end{aligned} \quad (25)$$

as in the statement of the Lemma.

To address the case in which θ exceeds $\lambda_{n-1}^{\text{ok}}$ note that for $\theta \rightarrow (\lambda_{n-1}^{\text{ok}})^{-}$, the last diagonal entry of S_{θ} tends to 0 and thus by (25) the covariance tends to have zeros in its last row and column. Since a Gaussian with vanishing-variance can be considered Dirac's delta, this models the fact that the last component of both x and x^{ko} is fully distorted and set to 0. With this, (25), is valid also for $\lambda_{n-1}^{\text{ok}} < \theta < \lambda_{n-2}^{\text{ok}}$. Yet, analogous considerations can be carried out for $\theta \rightarrow (\lambda_j^{\text{ok}})^{-}$ and $j = n-2, n-3, \dots, 0$ so that (25) is valid for any value of θ . \square

Proof of Lemma 3.

$$\begin{aligned} L(x'; x'') &= - \int_{\mathbb{R}^n} G_{0, \Sigma'}(\alpha) \log_2 [G_{0, \Sigma''}(\alpha)] d\alpha \\ &= \frac{1}{2} \log_2 [(2\pi)^n |\Sigma''|] \int_{\mathbb{R}^n} G_{0, \Sigma'}(\alpha) d\alpha \\ &\quad + \frac{1}{2 \ln 2} \int_{\mathbb{R}^n} \alpha^{\top} (\Sigma'')^{-1} \alpha G_{0, \Sigma'}(\alpha) d\alpha \\ &= \frac{1}{2} \log_2 [(2\pi)^n |\Sigma''|] + \frac{1}{2 \ln 2} \text{tr} [(\Sigma'')^{-1} \Sigma'] \end{aligned}$$

Where the last summand has been computed as the expectation of a quadratic form in a Gaussian multivariate for which Corollary 3.2b.1 in [32, chapter 3] gives a formula. \square

Proof of Theorem 1. From (21) we have that

$$\zeta_I = \frac{1}{2 \ln 2} \sum_{j=0}^{n_{\theta}-1} \alpha_j(\theta)$$

with

$$\alpha_j(\theta) = \frac{1}{\lambda_j^{\text{ok}}} \left(1 - \frac{\theta}{\lambda_j^{\text{ok}}} \right) + \frac{\theta}{\lambda_j^{\text{ok}}} - 1$$

Note that $\alpha_j(\theta)$ is continuous and its derivative is $\frac{\partial}{\partial \theta} \alpha_j = (1 - 1/\lambda_j^{\text{ok}})/\lambda_j^{\text{ok}}$.

For simplicity's sake assume $\lambda_0^{\text{ok}} > \lambda_1^{\text{ok}} > \dots > \lambda_{n-1}^{\text{ok}} > 0$, set $\lambda_n^{\text{ok}} = 0$, and define $\Theta_j =]\lambda_{j+1}^{\text{ok}}, \lambda_j^{\text{ok}}[$ for $j = 0, \dots, n-1$ so that if $\theta \in \Theta_j$ then $n_{\theta} = j+1$.

As a function of θ , ζ_I is continuous. In fact, it is trivially continuous in each Θ_j . Yet, it is continuous also at any chosen λ_j^{ok} with $j = 0, \dots, n-1$. To see why, note that

$$\begin{aligned} \lim_{\theta \rightarrow \lambda_j^{\text{ok}}-} \zeta_I &= \frac{1}{2 \ln 2} \lim_{\theta \rightarrow \lambda_j^{\text{ok}}-} \sum_{j=0}^{\bar{j}} \alpha_j(\theta) \\ &= \frac{1}{2 \ln 2} \lim_{\theta \rightarrow \lambda_j^{\text{ok}}-} \alpha_{\bar{j}}(\theta) + \sum_{j=0}^{\bar{j}-1} \alpha_j(\theta) \\ &= \frac{1}{2 \ln 2} \lim_{\theta \rightarrow \lambda_j^{\text{ok}}+} \sum_{j=0}^{\bar{j}-1} \alpha_j(\theta) = \lim_{\theta \rightarrow \lambda_j^{\text{ok}}+} \zeta_I \end{aligned}$$

where we have exploited that the $\alpha_j(\theta)$ are continuous and thus their left and right limits coincide, and that $\alpha_{\bar{j}}(\lambda_{\bar{j}}^{\text{ok}}) = 0$.

On the left-hand side of its domain, When $\theta = \lambda_n^{\text{ok}} = 0$ (no distortion), we have $n_{\theta} = n$ and thus

$$\zeta_I = \frac{1}{2 \ln 2} \sum_{j=0}^{n-1} \left(\frac{1}{\lambda_j^{\text{ok}}} - 1 \right) \geq 0$$

where the last inequality follows from the fact that $\sum_{j=0}^n \lambda_j^{\text{ok}} = n$ and thus $\sum_{j=0}^n 1/\lambda_j^{\text{ok}} \geq n$.

On the right-hand side of its domain, when $\theta = \lambda_0^{\text{ok}}$ (maximum distortion), we have $n_{\theta} = 0$ and thus $\zeta_I = 0$. Yet, we also have that

$$\frac{\partial}{\partial \theta} \zeta_I = \frac{1}{2 \ln 2} \sum_{j=0}^{n_{\theta}-1} \frac{1}{\lambda_j^{\text{ok}}} \left(1 - \frac{1}{\lambda_j^{\text{ok}}} \right)$$

in which the summands are positive if $\lambda_j^{\text{ok}} > 1$. Hence, if $\bar{k} = \arg \max_k \{\lambda_k^{\text{ok}} \geq 1\}$, for $\theta \geq \lambda_{\bar{k}}^{\text{ok}}$, all the summands in the above expression are positive and thus $\frac{\partial}{\partial \theta} \zeta_I > 0$ for $\lambda_{\bar{k}}^{\text{ok}} < \theta \leq \lambda_0^{\text{ok}}$. Given that $\zeta_I = 0$ at the end of that interval, it must be negative in its interior.

Since we know that ζ_I is positive for $\theta = \lambda_n^{\text{ok}} = 0$ and it is continuous for $\theta \in]\lambda_n^{\text{ok}}, \lambda_0^{\text{ok}}[$, it must pass through zero at least once whenever it is not negative, i.e., for $0 < \theta < \lambda_{\bar{k}}^{\text{ok}}$. \square

Proof of Theorem 2. We will use the following Lemma whose proof follows this one.

Lemma 4. *If $\lambda^{\text{ko}} \sim \mathcal{U}(\mathbb{S}^n)$, then for any integrable function $f : \mathbb{R} \rightarrow \mathbb{R}$ and any $j = 0, \dots, n-1$*

$$\mathbf{E} [f(\lambda_j^{\text{ko}})] = \frac{n-1}{n^{n-1}} \int_0^n f(p)(n-p)^{n-2} dp$$

From [33] we know that if Q is uniformly distributed in \mathbb{O}^n (i.e., if it is distributed according to the Haar measure on the orthogonal group) then, for any sequence of integers $M_n < n$ increasing with n but such that $M_n = o\left(\frac{n}{\log n}\right)$, the entries of the first M_n columns of Q converge in probability to independent random variables such that $\sqrt{n}Q_{j,k} \sim \mathcal{G}(0, 1)$ for $j = 0, \dots, n-1, k = 0, \dots, M_n-1$.

Such a property can be extended to any subset of M_n columns. In fact, given any subset of M_n columns of Q , there is a permutation matrix P such that QP has such columns as the first ones.

Yet, since $P \in \mathbb{O}^n$ and Q is distributed according to the Haar measure in that group, also QP is distributed according

to that measure and the entries in those columns tend to independent Gaussians.

Divide now n by M_n as in $n = N_n M_n + m_n$, where N_n is the quotient and $0 \leq m_n < M_n$ is the remainder. We can look at Q as the concatenation of N_n matrices Q_i , for $i = 0, \dots, N_n - 1$, each $n \times M_n$, and of a last matrix Q_{N_n} that is $n \times m_n$. From $M_n = o\left(\frac{n}{\log n}\right)$, we have $\lim_{n \rightarrow \infty} N_n / \log n = \infty$ and we can choose M_n such that $N_n = o(n^\alpha)$ for any $\alpha > 0$.

If we set $U^{\text{ko}} = Q$ then, $\Sigma^{\text{ko}} = U^{\text{ko}} \Lambda^{\text{ko}} U^{\text{ko}^\top}$ can be written componentwise

$$\begin{aligned} \Sigma_{j,k}^{\text{ok}} &= \sum_{l=0}^{n-1} U_{j,l}^{\text{ko}} \lambda_l^{\text{ko}} U_{k,l}^{\text{ko}} = \\ &= \underbrace{\sum_{i=0}^{N_n-1} \sum_{l=iM_n}^{(i+1)M_n-1} \frac{1}{n} \nu_{j,l} \lambda_l^{\text{ko}} \nu_{k,l}}_{W_i} + \underbrace{\sum_{l=n-m_n}^{n-1} \frac{1}{n} \nu_{j,l} \lambda_l^{\text{ko}} \nu_{k,l}}_{W_{N_n}} \end{aligned}$$

$i = 0, \dots, N_n - 1$ scans the first submatrices Q_i , the last summand accounts for the *remainder* matrix Q_{N_n} , and, thanks to the above considerations, $\nu_{j,l} \sim \nu_{k,l} \sim \mathcal{G}(0, 1)$ for all j, k, l .

We now have to address that case $j \neq k$ and the case $j = k$ separately.

A. Asymptotics of $\Sigma_{j,k}^{\text{ko}}$ for $j \neq k$

Let us now consider W_0 as the representative of all other W_i for $i = 0, \dots, N_n - 1$, written as $W_0 = \sum_{l=0}^{M_n-1} X_{n,l}$ with $X_{n,l} = \frac{1}{n} \nu_{j,l} \lambda_l^{\text{ko}} \nu_{k,l}$. All the normal random variables involved in such a sum are asymptotically independent but this is not true for the λ_l^{ko} since the eigenvalues are constrained to sum to n .

Hence, W_0 is a triangular array of row-dependent random variables whose asymptotic behaviour can be analyzed by means of [34, Theorem 2.1] that is essentially a Lindeberg-Feller Central Limit Theorem with the row-wise independence relaxed to asymptotic row-wise incorrelation. To analyze the asymptotics of W_0 we note that

$$\mathbf{E}[X_{n,l}] = \mathbf{E}[\lambda_l^{\text{ko}}] \mathbf{E}[\nu_{j,l}] \mathbf{E}[\nu_{k,l}] = 0$$

Note also that though not independent, the covariance and the correlation between $X_{n,l'}$ and $X_{n,l''}$ is

$$\begin{aligned} \mathbf{E}[X_{n,l'} X_{n,l''}] &= \\ &= \frac{1}{n^2} \mathbf{E}[\lambda_{l'}^{\text{ko}} \lambda_{l''}^{\text{ko}}] \mathbf{E}[\nu_{j,l'} \nu_{j,l''}] \mathbf{E}[\nu_{k,l'} \nu_{k,l''}] \\ &= \frac{1}{n^2} \begin{cases} 0 & \text{if } l' \neq l'' \\ \mathbf{E}[(\lambda_l^{\text{ko}})^2] & \text{if } l' = l'' = l \end{cases} \end{aligned}$$

With this we also know that

$$\begin{aligned} \sigma_{W_0}^2 &= \mathbf{E}[W_0^2] = \sum_{l'=0}^{M_n-1} \sum_{l''=0}^{M_n-1} \mathbf{E}[X_{n,l'} X_{n,l''}] = \\ &= \sum_{l=0}^{M_n-1} \mathbf{E}[X_{n,l}^2] = \frac{1}{n^2} \sum_{l=0}^{M_n-1} \mathbf{E}[(\lambda_l^{\text{ko}})^2] \end{aligned}$$

To compute the last expectation we may resort to Lemma 4 that gives

$$\mathbf{E}[(\lambda_l^{\text{ko}})^2] = \frac{n-1}{n^{n-1}} \int_0^n p^2 (n-p)^{n-2} dp = \frac{2n}{n+1}$$

Hence we have $\sigma_{W_0}^2 = \frac{2M_n}{n(n+1)} \rightarrow 0$ for $n \rightarrow \infty$.

This helps satisfying the Lindeberg condition since, if for a given $\epsilon > 0$ we indicate with $\mathbf{E}[X_{n,l}^2 | |X_{n,l}| \geq \epsilon]$ the expectation of $X_{n,l}^2$ restricted to its values that are not less than ϵ in modulus, then

$$\sum_{l=0}^{n-1} \mathbf{E}[X_{n,l}^2 | |X_{n,l}| \geq \epsilon] \leq \sum_{l=0}^{n-1} \mathbf{E}[X_{n,l}^2] = \sigma_{W_0}^2 = \frac{2M_n}{n(n+1)}$$

that vanishes asymptotically.

Finally, let $L_{M_n}, R_{M_n} \subset \{0, \dots, M_n - 1\}$ be two index subsets such that $L_{M_n} \cap R_{M_n} = \emptyset$. If $g_{L_{M_n}}$ is any function of the random variables $X_{n,l}$ with $l \in L_{M_n}$ and $h_{R_{M_n}} = \prod_{l \in R_n} X_{n,l}$, the covariance between $g_{L_{M_n}}$ and $h_{R_{M_n}}$ is

$$\begin{aligned} \mathbf{E}[g_{L_{M_n}} h_{R_{M_n}}] &= \mathbf{E}\left[g_{L_{M_n}} \prod_{l \in R_n} \frac{1}{n} \lambda_l^{\text{ko}} \nu_{j,l} \nu_{k,l}\right] \\ &= \mathbf{E}\left[g_{L_{M_n}} \prod_{l \in R_n} \lambda_l^{\text{ko}}\right] \prod_{l \in R_n} \frac{1}{n} \mathbf{E}[\nu_{j,l}] \mathbf{E}[\nu_{k,l}] = 0 \end{aligned}$$

that is enough to satisfy the assumptions in equation (2.3) and in equation (2.4) of [34, Theorem 2.1]. From that Theorem, we finally now that $W_0 \sim \mathcal{G}\left(0, \frac{2M_n}{n(n+1)}\right)$ when $n \rightarrow \infty$ where convergence is in probability and thus also in distribution. Clearly, the same happens to any W_i for $i = 0, \dots, N_n - 1$, while $W_{N_n} \sim \mathcal{G}\left(0, \frac{2m_n}{n(n+1)}\right)$.

Let us now consider

$$\begin{aligned} \Pr\{|\Sigma_{j,k}^{\text{ko}}| \leq \epsilon\} &= \\ &= \Pr\left\{\left|\sum_{i=0}^{N_n-1} W_i + W_{N_n}\right| \leq \epsilon\right\} \\ &\geq \Pr\left\{\sum_{i=0}^{N_n-1} |W_i| + |W_{N_n}| \leq \epsilon\right\} \\ &\geq \Pr\left\{\max\{|W_0|, \dots, |W_{N_n}|\} \leq \frac{\epsilon}{N_n+1}\right\} \\ &= 1 - \Pr\left\{\max\{|W_0|, \dots, |W_{N_n}|\} > \frac{\epsilon}{N_n+1}\right\} \end{aligned}$$

Yet

$$\begin{aligned} \Pr\left\{\max\{|W_0|, \dots, |W_{N_n}|\} > \frac{\epsilon}{N_n+1}\right\} &= \\ &= \Pr\left\{|W_0| > \frac{\epsilon}{N_n+1} \vee \dots \vee |W_{N_n}| > \frac{\epsilon}{N_n+1}\right\} \\ &\leq (N_n+1) \Pr\left\{|W_0| > \frac{\epsilon}{N_n+1}\right\} \end{aligned}$$

so that

$$\Pr \{ |\Sigma_{j,k}^{\text{ko}}| \leq \epsilon \} \geq 1 - (N_n + 1) \Pr \left\{ |W_0| > \frac{\epsilon}{N_n + 1} \right\}$$

From this and from the asymptotic normality of W_0 we may say

$$\Pr \{ |\Sigma_{j,k}^{\text{ko}}| \leq \epsilon \} \geq 1 - \frac{N_n + 1}{2} \operatorname{erfc} \left(\frac{\epsilon}{2\sqrt{\frac{(N_n + 1)^2 M_n}{n(n+1)}}} \right) \quad (26)$$

in which the probability tends to 1 for $n \rightarrow \infty$, and $M_n = o\left(\frac{n}{\log n}\right)$ chosen to have $N_n = o(n^{1/2})$.

B. Asymptotics of $\Sigma_{j,k}^{\text{ko}}$ for $j = k$

In this case, exploiting the fact that $\sum_{j=0}^{n-1} \lambda_j^{\text{ko}} = n$, we may write

$$\Sigma_{j,j}^{\text{ok}} = 1 + \underbrace{\sum_{i=0}^{N_n-1} \sum_{l=iM_n}^{(i+1)M_n-1} \frac{1}{n} (\nu_{j,l}^2 - 1) \lambda_l^{\text{ko}}}_{W_i} + \underbrace{\sum_{l=n-m_n}^{n-1} \frac{1}{n} (\nu_{j,l}^2 - 1) \lambda_l^{\text{ko}}}_{W_{N_n}}$$

in which the summands W_i are a triangular arrays of elements with features similar to the previous ones.

In fact, we may focus on $W_0 = \sum_{l=0}^{M_n-1} X_{n,l}$ with $X_{n,l} = \frac{1}{n} \lambda_l^{\text{ko}} (\nu_{j,l}^2 - 1)$ and note that $\mathbf{E}[X_{n,l}] = 0$ and

$$\begin{aligned} \mathbf{E}[X_{n,l'} X_{n,l''}] &= \frac{1}{n^2} \mathbf{E}[\lambda_{l'}^{\text{ko}} \lambda_{l''}^{\text{ko}}] \mathbf{E}[(\nu_{j,l'}^2 - 1)(\nu_{j,l''}^2 - 1)] \\ &= \frac{2}{n^2} \begin{cases} 0 & \text{if } l' \neq l'' \\ \mathbf{E}[(\lambda_l^{\text{ko}})^2] & \text{if } l' = l'' = l \end{cases} \end{aligned}$$

where we have exploited the fact that $\mathbf{E}[(\nu_{j,l}^2 - 1)^2] = \mathbf{E}[\nu_{j,l}^4] - 2\mathbf{E}[\nu_{j,l}^2] + 1 = 2$. With this, $\sigma_{W_0}^2 = \frac{4M_n}{n(n+1)} \rightarrow 0$ for $n \rightarrow \infty$.

As before, this makes the Lindeberg condition automatically satisfied and is also enough to satisfy the covariance constraints in equations (2.3) and (2.4) of [34, Theorem 2.1] from which we get that $W_0 \sim \mathcal{G}\left(0, \frac{4M_n}{n(n+1)}\right)$ for $n \rightarrow \infty$ where convergence is in probability thus also in distribution. An analogous path leads to the asymptotic behaviour $W_{N_n} \sim \mathcal{G}\left(0, \frac{4m_n}{n(n+1)}\right)$.

The same inequalities as before lead to

$$\Pr \{ |\Sigma_{j,j}^{\text{ko}} - 1| \leq \epsilon \} \geq 1 - \frac{N_n + 1}{2} \operatorname{erfc} \left(\frac{\epsilon}{4\sqrt{\frac{(N_n + 1)^2 M_n}{n(n+1)}}} \right) \quad (27)$$

in which the probability tends to 1 for $n \rightarrow \infty$, and $M_n = o\left(\frac{n}{\log n}\right)$ chosen to have $N_n = o(n^{1/2})$.

From (26) and (27) we finally get that U^{ko} tends to I_n in probability as $n \rightarrow \infty$. \square

Proof of Lemma 4. For any function $f : \mathbb{R} \mapsto \mathbb{R}$ we have

$$\begin{aligned} \mathcal{I}[f(p)] &= \int_{\mathbb{S}^n} f(p_0) dp_0 \dots dp_{n-1} \\ &= \int_0^n f(p_0) \int_0^{n-p_0} \int_0^{n-p_0-p_1} \dots \int_0^{n-p_0-p_1-\dots-p_{n-3}} dp_0 \dots dp_{n-2} \\ &= \int_0^n f(p_0) \frac{(n-p_0)^{n-2}}{(n-2)!} dp_0 \end{aligned}$$

Since λ^{ko} is uniformly distributed over \mathbb{S}^n the probability density is the constant $1/\mathcal{I}[1] = n^{-(n-1)}(n-1)!$ and the expectation of f is

$$\begin{aligned} \mathbf{E}[f(\lambda_j^{\text{ok}})] &= n^{-(n-1)}(n-1)! \mathcal{I}[f(p)] \\ &= \frac{(n-1)!}{n^{n-1}} \int_0^n f(p) \frac{(n-p)^{n-2}}{(n-2)!} dp \\ &= \frac{n-1}{n^{n-1}} \int_0^n f(p) (n-p)^{n-2} dp \end{aligned}$$

\square

REFERENCES

- [1] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.
- [2] R. Ahlswede and I. Csiszar, "Hypothesis testing with communication constraints," *IEEE Transactions on Information Theory*, vol. 32, no. 4, pp. 533–542, 1986.
- [3] T. S. Han and S. Amari, "Statistical inference under multiterminal data compression," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2300–2324, 1998.
- [4] N. Tishby, F. C. Pereira, and W. Bialek, "The information bottleneck method," in *Proceedings of the 37-th Annual Allerton Conference on Communication, Control and Computing*, 1999, p. 368–377.
- [5] N. Slonim and N. Tishby, "Agglomerative information bottleneck," in *Proceedings of the 12th International Conference on Neural Information Processing Systems*, ser. NIPS'99. MIT Press, 1999, p. 617–623.
- [6] K. Crammer and G. Chechik, "A needle in a haystack: Local one-class optimization," in *Proceedings of the Twenty-First International Conference on Machine Learning*, ser. ICML '04. Association for Computing Machinery, 2004, p. 26.
- [7] K. Crammer, P. P. Talukdar, and F. Pereira, "A rate-distortion one-class model and its applications to clustering," in *Proceedings of the 25th International Conference on Machine Learning*, ser. ICML '08. Association for Computing Machinery, 2008, p. 184–191.
- [8] C. Böhm, K. Haegler, N. S. Müller, and C. Plant, "Coco: Coding cost for parameter-free outlier detection," in *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '09. Association for Computing Machinery, 2009, p. 149–158.
- [9] Y. Blau and T. Michaeli, "The perception-distortion tradeoff," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018, pp. 6228–6237.
- [10] —, "Rethinking lossy compression: The rate-distortion-perception tradeoff," in *Proceedings of the 36th International Conference on Machine Learning, ICML 2019*, ser. Proceedings of Machine Learning Research, K. Chaudhuri and R. Salakhutdinov, Eds., vol. 97. PMLR, 2019, pp. 675–685.
- [11] M. R. D. Rodrigues, N. Deligiannis, L. Lai, and Y. C. Eldar, "Rate-distortion trade-offs in acquisition of signal parameters," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 6105–6109.
- [12] N. Shlezinger, Y. C. Eldar, and M. R. D. Rodrigues, "Hardware-limited task-based quantization," *IEEE Transactions on Signal Processing*, vol. 67, no. 20, pp. 5223–5238, 2019.

- [13] B. Foo, Y. Andreopoulos, and M. van der Schaar, "Analytical complexity modeling of wavelet-based video coders," in *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*, vol. 3, 2007, pp. III-789-III-792.
- [14] V. Menon and S. Kalyani, "Structured and unstructured outlier identification for robust pca: A fast parameter free algorithm," *IEEE Transactions on Signal Processing*, vol. 67, no. 9, pp. 2439-2452, 2019.
- [15] L. Kong, C. Qi, and H.-D. Qi, "Classical multidimensional scaling: A subspace perspective, over-denoising, and outlier detection," *IEEE Transactions on Signal Processing*, vol. 67, no. 14, pp. 3842-3857, 2019.
- [16] M. Rahmani and P. Li, "Fast and provable robust pca via normalized coherence pursuit," in *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2021, pp. 5305-5309.
- [17] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 1991.
- [18] 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.
- [19] S. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*. Prentice Hall PTR, 1988.
- [20] M. Mangia, F. Pareschi, V. Cambareri, R. Rovatti, and G. Setti, "Rakeness-based design of low-complexity compressed sensing," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 5, pp. 1201-1213, 2017.
- [21] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "A rakeness-based design flow for analog-to-information conversion by compressive sensing," in *2013 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2013, pp. 1360-1363.
- [22] S. Onn and I. Weissman, "Generating uniform random vectors over a simplex with implications to the volume of a certain polytope and to multivariate extremes," *Annals of Operations Research*, vol. 189, no. 1, pp. 331-342, 2011.
- [23] F. Mezzadri, "How to generate random matrices from the classical compact groups," *Notices of the American Mathematical Society*, vol. 54, no. 5, pp. 592-604, 2006.
- [24] J. Ginibre, "Statistical ensembles of complex, quaternion, and real matrices," *Journal of Mathematical Physics*, vol. 6, no. 3, pp. 440-449, 1965.
- [25] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016, <http://www.deeplearningbook.org>.
- [26] R. B. Arellano-Valle, J. E. Contreras-Reyes, and M. G. Genton, "Shannon entropy and mutual information for multivariate skew-elliptical distributions," *Scandinavian Journal of Statistics*, vol. 40, no. 1, pp. 42-62, 2013.
- [27] B. Schölkopf, R. Williamson, A. Smola, J. Shawe-Taylor, and J. Platt, "Support vector method for novelty detection," in *Proceedings of the 12th International Conference on Neural Information Processing Systems*, ser. NIPS'99. Cambridge, MA, USA: MIT Press, 1999, p. 582-588.
- [28] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," in *3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings*, Y. Bengio and Y. LeCun, Eds., 2015.
- [29] T. Fawcett, "An introduction to roc analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861-874, 2006, rOC Analysis in Pattern Recognition.
- [30] H. Jamalabadi, S. Alizadeh, M. Schönauer, C. Leibold, and S. Gais, "Classification based hypothesis testing in neuroscience: Below-chance level classification rates and overlooked statistical properties of linear parametric classifiers," *Human Brain Mapping*, vol. 37, no. 5, pp. 1842-1855, may 2016.
- [31] L. Snoek, S. Miletić, and H. S. Scholte, "How to control for confounds in decoding analyses of neuroimaging data," *NeuroImage*, vol. 184, pp. 741-760, jan 2019.
- [32] S. B. Provost and A. Mathai, *Quadratic Forms in Random Variables: Theory and Applications/ A.M. Mathai, Serge B. Provost*, ser. Statistics: textbooks and monographs. Marcel Dekker, 1992.
- [33] T. Jiang, "How many entries of a typical orthogonal matrix can be approximated by independent normals?" *The Annals of Probability*, vol. 34, no. 4, pp. 1497 - 1529, 2006.
- [34] M. H. Neumann, "A central limit theorem for triangular arrays of weakly dependent random variables, with applications in statistics," *ESAIM: Probability and Statistics*, vol. 17, pp. 120 - 134, 2013.