Farhad Shirani Chaharsooghi

CONTACT INFORMATION

NYU Tandon School of Eng.,
Department of ECE,
Two Metrotech Center,
Brooklyn, NY, 11201

Cell. Phone: (+1) 775-233-9238
E-mail: fsc265@nyu.edu
Homepage: https://wp.nyu.edu/farhad_shirani/

LIST OF THREE SIGNIFICANT PUBLICATIONS, SUBMISSIONS AND PREPRINTS

F. Shirani Chaharsooghi, S. Garg, E. Erkip, *A Concentration of Measure Approach to Matching of Correlated Graphs*, to be submitted to IEEE Transactions on Information Theory (earlier version appeared in [C6,9,12]).

F. Shirani Chaharsooghi, S. Pradhan, *On the Sub-optimality of Single-Letter Coding in Networks*, IEEE Transactions on Information Theory, vol. 65, no. 10, pp. 6115-6135, Oct. 2019.

S. Shahsavari, **F. Shirani Chaharsooghi**, E. Erkip, *A General Framework for Temporal Fair User Scheduling in NOMA Systems*, IEEE Journal on Selected Topics on Signal Processing, vol. 13, no. 3, pp. 408-422, 2019.

COMPLETE LIST OF PUBLICATIONS, SUBMISSIONS AND PREPRINTS

Journals: Accepted Papers

[J1] **F. Shirani Chaharsooghi**, S. Pradhan, *On the Sub-optimality of Single-Letter Coding in Networks*, IEEE Transactions on Information Theory, vol. 65, no. 10, pp. 6115-6135, Oct. 2019.

[J2] H. Heidari, **F. Shirani Chaharsooghi**, S. Pradhan, *Quasi Structured Codes for Multi-Terminal Communications*, IEEE Transactions on Information Theory, vol. 65, no. 10, pp. 6263-6289, Oct. 2019.

[J3] S. Shahsavari, **F. Shirani Chaharsooghi**, E. Erkip, *A General Framework for Temporal Fair User Scheduling in NOMA Systems*, IEEE Journal on Selected Topics on Signal Processing, vol. 13, no. 3, pp. 408-422, 2019.

[J4] **F. Shirani Chaharsooghi**, S. Pradhan, *An achievable rate-distortion region for multiple descriptions source coding based on coset codes*, IEEE Transactions on Information Theory, vol. 64, no. 5, pp. 3781-3809, 2018.

Journals: Preprints/Working Papers

[J5] **F. Shirani Chaharsooghi**, S. Pradhan, *A New Achievable Rate-Distortion Region for Distributed Source Coding*, submitted to IEEE Transactions on Information Theory (earlier version appeared in [C23,25]).

[J6] A. Khalili, **F. Shirani Chaharsooghi**, E. Erkip, Y. C. Eldar, *On MIMO Communication with Low Resolution Quantization at the Receivers*, to be submitted to IEEE Transactions on Wireless Communications (earlier version appeared in [C3,4]).

[J7] **F. Shirani Chaharsooghi**, S. Garg, E. Erkip, *A Concentration of Measure Approach to Matching of Correlated Graphs*, to be submitted to IEEE Transactions on Information Theory (earlier version appeared in [C6,9,12]).

[J8] **F. Shirani Chaharsooghi**, S. Pradhan, *Lattices from linear codes and fine quantization: general continuous sources and channels*, to be submitted to IEEE Transactions on Information Theory (earlier version appeared in [C8,24]).

Conference Publications

[C1] S. Shahsavari, **F. Shirani Chaharsooghi**, A. Khojastepour, E. Erkip, *Opportunistic Temporal Fair Mode Selection and User Scheduling for Full-duplex Systems*, 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Accepted: June 2019.

[C2] **F. Shirani Chaharsooghi**, S. Garg, E. Erkip, *A Concentration of Measure Approach to Database De-anonymization*, 2019 IEEE International Symposium on Information Theory (ISIT), pp. 2748-2752, 2019.

[C3] A. Khalili, **F. Shirani Chaharsooghi**, E. Erkip, Y. C. Eldar, *Tradeoff Between Delay and High SNR Capacity in Quantized MIMO Systems*, 2019 IEEE International Symposium on Information Theory (ISIT), pp. 597-601, 2019.

[C4] A. Khalili, **F. Shirani Chaharsooghi**, E. Erkip, Y. C. Eldar, *On Multiterminal Communication over MIMO Channels with One-bit ADCs at the Receivers*, 2019 IEEE International Symposium on Information Theory (ISIT), pp. 602-606, 2019.

[C5] S. Shahsavari, **F. Shirani Chaharsooghi**, E. Erkip, *On the Fundamental Limits of Multi-user Scheduling under Short-term Fairness Constraints*, 2019 IEEE International Symposium on Information Theory (ISIT), pp. 408-422, 2019.

[C6] **F. Shirani Chaharsooghi**, S. Garg, E. Erkip, *Matching graphs with community structure: a concentration of measure approach*, 56th IEEE Annual Allerton Conference on Communication, Control, and Computing, pp. 1028-1035, 2018

[C7] S. Shahsavari, **F. Shirani Chaharsooghi**, E. Erkip, *Opportunistic temporal fair scheduling for non-orthogonal multiple access*, 56th IEEE Annual Allerton Conference on Communication, Control, and Computing, pp. 391-398, 2018

[C8] **F. Shirani Chaharsooghi**, S. Pradhan, *Lattices from linear codes and fine quantization: general continuous sources and channels*, IEEE International Symposium on Information Theory (ISIT), pp. 2356-2360, 2018.

[C9] **F. Shirani Chaharsooghi**, S. Garg, E. Erkip, *Typicality matching for pairs of correlated graphs*, IEEE International Symposium on Information Theory (ISIT), pp. 221-225, 2018.

[C10] M. Heidari, **F. Shirani Chaharsooghi**, S. Pradhan, *Bounds on the effective-length of optimal codes for interference channel with feedback*, IEEE International Symposium on Information Theory (ISIT), pp. 1126-1130, 2018.

[C11] **F. Shirani Chaharsooghi**, S. Garg, E. Erkip, *Optimal active social network de-anonymization using information thresholds*, IEEE International Symposium on Information Theory (ISIT), pp. 1445-1449, 2018.

[C12] **F. Shirani Chaharsooghi**, S. Garg, E. Erkip, *Seeded graph matching: efficient algorithms and theoretical guarantees*, 51st Asilomar Conference on Signals, Systems, and Computers, pp. 253-257, 2017.

[C13] **F. Shirani Chaharsooghi**, S. Garg, E. Erkip, *An information theoretic framework for active de-anonymization in social networks based on group memberships*, 55th Annual Allerton Conference on Communication, Control, and Computing, pp. 470-477, 2017.

[C14] **F. Shirani Chaharsooghi**, S. Pradhan, *On the sub-optimality of single-letter coding in multi-termianl communications*, IEEE International Symposium on Information Theory (ISIT), pp. 1823-1827, 2017.

[C15] **F. Shirani Chaharsooghi**, S. Pradhan, *On the correlation between boolean functions of random variables*, IEEE International Symposium on Information Theory (ISIT), pp. 1301-1305, 2017.

[C16] M. Heidari, **F. Shirani Chaharsooghi** , S. Pradhan, *A new achievable rate region for the multiple-access channel with states*, IEEE International Symposium on Information Theory (ISIT), pp. 36-40, 2017.

[C17] M. Heidari, **F. Shirani Chaharsooghi** , S. Pradhan, *On the necessity of structured codes for communication over MAC with feedback*, IEEE International Symposium on Information Theory (ISIT), pp. 2298-2302, 2017.

[C18] **F. Shirani Chaharsooghi** , S. Pradhan, *Trade-off between communication and cooperation in the interference channel*, IEEE International Symposium on Information Theory (ISIT), pp. 2214-2218, 2016.

[C19] **F. Shirani Chaharsooghi** , M. Heidari, S. Pradhan, *Quasi linear codes: application to point-to-point and multi-terminal source coding*, IEEE International Symposium on Information Theory (ISIT), pp. 730-734, 2016.

[C20] M. Heidari, **F. Shirani Chaharsooghi** , S. Pradhan, *New sufficient conditions for multiple-access channel with correlated sources*, IEEE International Symposium on Information Theory (ISIT), pp. 2019-2023, 2016.

[C21] M. Heidari, **F. Shirani Chaharsooghi** , S. Pradhan, *Beyond group capacity in multi-terminal communications*, IEEE International Symposium on Information Theory (ISIT), pp. 2081-2085, 2015.

[C22] **F. Shirani Chaharsooghi** , M. Heidari, S. Pradhan, *New lattices for multiple-descriptions*, IEEE International Symposium on Information Theory (ISIT), pp. 1580-1584, 2015.

[C23] **F. Shirani Chaharsooghi**, S. Pradhan, *Finite-length gains in distributed source coding*, IEEE International Symposium on Information Theory (ISIT), pp. 1702-1706, 2014.

[C24] **F. Shirani Chaharsooghi** , S. Pradhan, *An achievable rate-distortion region for the multiple-descriptions problem*, IEEE International Symposium on Information Theory (ISIT), pp. 576-580, 2014.

[C25] **F. Shirani Chaharsooghi** , A. Ghasemian Sahebi, S. Pradhan, *Distributed source coding in absence of common components*, IEEE International Symposium on Information Theory (ISIT), pp. 1362-1366, 2013.

[C26] **F. Shirani Chaharsooghi** , M. Emadi, M. Zamanighomi and M. R. Aref, *A new method for variable elimination in systems of inequations*, IEEE International Symposium on Information theory (ISIT), pp. 1215-1219, 2011.

[C27] M. Zamanighomi, M. Emadi, **F. Shirani Chaharsooghi**, M. R. Aref, *Achievable rate region for multiple access channel with correlated channel states and cooperating encoders*, IEEE Information Theory Workshop (ITW), pp. 628-632, 2011.

On the Sub-Optimality of Single-Letter Coding Over Networks

Farhad Shirani and S. Sandeep Pradhan

Abstract— **In this paper, we establish a new bound tying together the effective length and the maximum correlation between the outputs of an arbitrary pair of Boolean functions which operate on two sequences of correlated random variables. We derive a new upper bound on the correlation between the outputs of these functions. The upper bound may find applications in problems in many areas which deal with common information. We build upon Witsenhausen's result [1] on maximum correlation. The present upper bound takes into account the effective length of the Boolean functions in characterizing the correlation. We use the new bound to characterize the communication-cooperation tradeoff in multi-terminal communications. We investigate binary block-codes (BBC). A BBC is defined as a vector of Boolean functions. We consider an ensemble of BBCs which is randomly generated using single-letter distributions. We characterize the vector of dependency spectrums of these BBCs. We use this vector to bound the correlation between the outputs of two distributed BBCs. Finally, the upper bound is used to show that the large blocklength single-letter coding schemes studied in the literature are sub-optimal in various multi-terminal communication settings.**

Index Terms— **Random coding, source coding, channel coding, maximum correlation.**

I. Introduction

MOST of the coding strategies developed in information theory are based on random code ensembles which are constructed using independent identically distributed (IID) random variables [2]. The codes associated with different nodes in the network are mutually independent. Moreover, the blocklength associated with these codes are asymptotically large. One can use the law of large numbers to characterize their performance in terms of information quantities that are the functionals of the underlying distribution used to construct the codes. They are called single-letter characterizations [3]. Although the original problem is to optimize performance of codes with asymptotically large blocklengths, the solution is characterized by a functional (such as mutual information) of just *one* realization of the source or the channel under consideration. At a high level, this is very similar to the characterizations of the probability of large deviations studied in probability theory [4], the simplest example being the Chernoff Bound. In network source coding problems, one can do better covering in larger dimensions so that source redundancy can be exploited more efficiently, and the sources can be represented and reconstructed with less distortion. In network channel coding problems, better packing can be done in larger dimensions so that the channel noise can be tackled in a better fashion. In summary, the efficiency of fundamental tasks of communication such as covering and packing increases as we increase the dimension more or less all the way to infinity. Recall that in point-to-point communication the key objective is to perform these tasks efficiently. Although the individual codewords are constructed using IID random variables, since the encoding and decoding processes are accomplished in large dimensions using the so-called typical sets, there is memory of arbitrary lengths among the source reconstruction vectors in source coding and channel input vectors in channel coding.

In network communication, one needs to (a) remove redundancy among correlated information sources [5] in a distributed manner in the source coding problems, and (b) induce redundancy among distributed terminals to facilitate [6] cooperation among them. For example, in the network source coding problems such as distributed data compression, the objective is to exploit the statistical correlation of the distributed information sources. Similarly, in the network channel coding problems, such as the interference networks and broadcast networks, correlation of information among different terminals are induced for better cooperation among them [7]. At a high level, efficient information coding strategies in networks exploit statistical correlation among distributed information sources or induce statistical correlation among information accessed by terminals in the network. Of course, the basic tasks such as packing and covering at every terminal need to be accomplished as well. Statistical correlation among information shared by the terminals in the network can be viewed as a resource that needs to be efficiently managed. Distributed statistical correlation can facilitate cooperation among the terminals in networks.

It was first observed by Gács, Körner and Witsenhausen [1], [8] that coding over blocks decreases distributed correlation. Consider a pair of distributed sources X and Y with a joint probability distribution P_{XY}. Let us assume that the joint distribution does not have any zeros. There are two distributed agents who observe the sources as shown in Figure 1. The observations include n memoryless copies of the sources. The objective is to encode the observations into one bit. Let e and f denote the encoding functions associated with the two encoders. Loosely speaking,

Manuscript received April 18, 2017; revised February 27, 2019; accepted April 20, 2019. Date of publication May 17, 2019; date of current version September 13, 2019. This work was supported by NSF under Grant CCF-1422284. This paper was presented in part at the 2017 IEEE International Symposium on Information Theory.

F. Shirani is with the Department of Electrical and Computer Engineering, New York University, New York, NY 10003 USA (e-mail: fshirani@umich.edu).

S. S. Pradhan is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109 USA.

Communicated by V. M. Prabhakaran, Associate Editor for Shannon Theory.
Digital Object Identifier 10.1109/TIT.2019.2917434

0018-9448 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

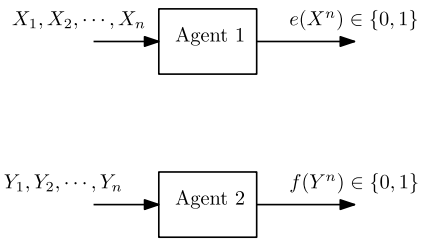

Fig. 1. Correlated Boolean decision functions.

we wish to maximize correlation between the outputs such that $H(e(X^n)) > 0$ and $H(f(Y^n)) > 0$, where $H(\cdot)$ is the entropy function. It was shown that maximum correlation is achieved when the output depends only on one of the input samples at both encoders. In fact any block mapping strictly reduces the correlation between the output bits. In summary, uncoded mappings (mappings with blocklength 1) are optimal in terms of correlation preservation. A second observation that is made in these works is that if the sources have a common component, then and only then the output bits can be made perfectly correlated. In other words, if the objective is to generate one bit at both encoders that match with probability one, then this is possible if and only if the sources have a matching component to begin with. This matching component, if it exists, is called the common information of the two sources.[1] This observation suggests that common information is very fragile. Even a small perturbation of the source distribution can produce a large change in the correlation of the output bits [11]. The study of this setup has had impact on a variety of disciplines, for instance, by taking the agents to be two encoders in the distributed source coding problem [12], or two transmitters in the interference channel problem, or Alice and Bob in a secret key-generation problem [13], [14], or two agents in a distributed control problem [15], [16].

We have taken the fundamental observation made by Gács-Körner-Witsenhausen, and developed a framework for quantitatively characterizing the correlation preserving property of any pair of encoding functions with arbitrary blocklengths. It is harder to preserve distributed correlation in larger dimensions than in smaller dimensions. In other words, short blocklength codes are able to preserve and induce correlation in a distributed fashion in a better way than larger blocklength codes. At this point, it is worth noting that this strange behavior leads to a tension: to perform covering and packing we need large blocklength codes, whereas to preserve and induce correlation we need short blocklength codes. The overall network performance may be optimized by codes whose blocklength is some sweet finite value. Toward a characterization of this trade-off, consider a source encoder at a terminal in a network that maps n samples of an information source into k bits (for some n and k). Then the blocklength of the encoder is n. Suppose that each of the output bits depends only on (αn) samples of the input vector for some $\alpha < 1$. We can then define the *effective length* of the encoder as (αn). It is the conventional wisdom that performance of many coding strategies (characterized by a sequence of encoders and decoders with increasing blocklength) in network communication is super-additive in blocklength (e.g. see [17]). Our results state that the performance is not super-additive in effective length. In fact in network communication problems, to achieve optimality, certain components of the transmission system must have a finite effective length structure. In summary we have new a trade-off between covering and packing efficiency, and the correlation preserving/inducing ability of codes. That is, a trade-off between communication and cooperation in networks. Optimal codes have to straddle this trade-off.

[1]This is also characterized via Rényi maximum correlation [9], [10]. If the sources have a common information then the maximum correlation of the sources is 1.

In this work we make the following three contributions.

- We start with Section III. Consider a discrete memoryless source $X_1, X_2, \ldots$, with finite alphabet $\mathcal{X}$, and a generic distribution P_X. Consider a block encoder (a Boolean function) $e : \mathcal{X}^n \to \{0,1\}$, where n denotes the blocklength (see [8]). Given a pair consisting of a source and an encoder, we define its dependency spectrum (Definition 6) as a (unnormalized) 2^n-dimensional vector that captures the probabilistic as well as the functional memory structure of the pair. For example, for $n = 3$, the dependency spectrum is the following vector $[P_{000}, P_{001}, \ldots, P_{111}]$ charactering the contribution of the constant (P_{000}), single-letter (P_{001}, P_{010}, P_{100}), two-letter (P_{011}, P_{110}, P_{101}), and three-letter (P_{111}) component functions toward constructing e. Note that there are three one-letter and two-letter functions. As another example, for $n = 2$, and logical AND function $e(X^n) = X_1 \wedge X_2$, with binary uniform source, we get $P_{01} = P_{10} = P_{11} = \frac{1}{16}$, and $P_{00} = 0$. Logical AND function is two-thirds a single-letter function and one-third a two-letter function. This is a generalization of the effective length from a number to a vector.
  We use dependency spectrum to study distributed encoding of correlated sources in the following way and provide the first main result (Theorem 1 and 2) of the paper in Section IV. Consider a pair of discrete memoryless correlated sources $(X_1, Y_1), (X_2, Y_2), \ldots$ with finite alphabets $\mathcal{X} \times \mathcal{Y}$ and a generic distribution P_{XY}. Consider a pair of distributed block encoders $e : \mathcal{X}^n \to \{0,1\}$ and $f : \mathcal{Y}^n \to \{0,1\}$. We provide a characterization of the correlation between the outputs of these block encoders. In particular, we give a lower bound on the probability of disagreement between the outputs $P(e(X^n) \neq f(Y^n))$ in terms of the dependency spectra of (P_X, e) and (P_Y, f), and the correlation of the sources given by $P(X \neq Y)$. Roughly speaking, this is a quantitative characterization of the trade-off between the effective length of the encoders and the output correlation.
- We use this characterization to analyze a large class of sequence of code ensembles studied in the information theory literature in Section V. We call this class Single-letter coding ensembles (SLCE) (Definition 8). For example, this class subsumes Shannon-style IID unstructured code ensembles as well as structured linear code ensembles. Most, if not all, of the coding theorems of information theory that characterize asymptotic performance limits are based on this class. In short, a code ensemble is an infinite sequence

of collections of block encoders (indexed by blocklength $n = 1, 2, \ldots$) along with a probability distribution on the collection. We provide the following second main result of the paper (Theorem 3 and 4). For a discrete memoryless source $X_1, X_2, \ldots$, with finite alphabet $\mathcal{X}$ and a generic distribution P_X, the output of the SLCE has the following structure: for any fixed $1 < m < \infty$, the probability that the contribution of m-letter functions toward constructing e is large approaches zero as n tends to infinity. In other words, with high probability SLCE produces encoders which has either a single-letter component or an infinite-letter component. We call this the 1-∞ law. This is a structural deficiency of SLCE. Moreover, when applied on a pair of correlated sources, (X, Y), we provide a high probability upper bound on the correlation of the outputs.

- We study two multi-terminal communication problems in Section VI: transmission of correlated sources over the interference channels and the multiple-access channels. These two problems have been studied in the literature extensively. Inner bounds to the asymptotic performance limits (achievable performance) based on SLCE have been developed in the literature. These bounds have been the de facto performance limits since the 1980s. We provide a novel coding technique based on finite-length codes along with two examples. Using the structural results from the previous section, we show analytically that this coding technique outperforms the inner bounds derived using arbitrarily long codes constructed using SLCE. This is the third main result of the paper (Proposition 5, 7 and 8). In other words, specifically designed finite-length codes can perform better than SLCE.

We discuss some related prior works. In the literature, it has been shown that the loss in correlation caused by the application of large effective-length codes causes a discontinuity in the performance of schemes using such codes in some multi-terminal problems. This was first observed in the Berger-Tung achievable rate-distortion region for the problem of distributed source coding [18] [11]. It was noted that when the common information is available to the two encoders in the distributed source coding problem, the performance is discontinuously better than when the common information is replaced with highly correlated components. In [12], we argued that the discontinuity in performance is due to the fact that the encoding functions in the Berger-Tung scheme preserve common information, but are unable to preserve correlation between highly correlated components. We proposed a new coding scheme, and derived an improved achievable rate-distortion region for the two user distributed source coding problem [19]. The new strategy uses a concatenated coding scheme which consists of one layer of codes with finite effective-length, and one layer of codes with asymptotically large effective-lengths.

II. Notation

In this section, we introduce the notation used in this paper. We represent random variables by capital letters such as X, U. Sets are denoted by calligraphic letters such as $\mathcal{X}, \mathcal{U}$. Particularly, the set of natural numbers and real numbers are shown by $\mathbb{N}$, and $\mathbb{R}$, respectively. For a random variable X, the corresponding probability space is $(\mathcal{X}, \mathbf{F}_X, P_X)$, where $\mathbf{F}$ is the underlying σ-field. The set of all subsets of $\mathcal{X}$ is written as $2^{\mathcal{X}}$. There are three different notations used for different classes of vectors. For random variables, the n-length vector $(X_1, X_2, \cdots, X_n)$, $X_i \in \mathcal{X}$ is denoted by $X^n \in \mathcal{X}^n$. For the vector of functions $(e_1(X), e_2(X), \cdots, e_n(X))$ we use the notation $\underline{e}(X)$. The binary string $(i_1, i_2, \cdots, i_n)$, $i_j \in \{0, 1\}$ is written as $\mathbf{i}$. As an example, the set of functions $\{\underline{e_{\mathbf{i}}}(X^n) | \mathbf{i} \in \{0, 1\}^n\}$ is the set of n-length vectors of functions $(e_{1,\mathbf{i}}, e_{2,\mathbf{i}}, \cdots, e_{n,\mathbf{i}})$ operating on the vector $(X_1, X_2, \cdots, X_n)$ each indexed by an n-length binary string $(i_1, i_2, \cdots, i_n)$. The vector of binary strings $(\mathbf{i}_1, \mathbf{i}_2, \cdots, \mathbf{i}_n)$ denotes the standard basis for the n-dimensional space (e.g. $\mathbf{i}_1 = (0, 0, \cdots, 0, 1)$). The vector of random variables $(X_{j_1}, X_{j_2}, \cdots, X_{j_k})$, $j_i \in [1, n]$, $j_i \neq j_k$, is denoted by $X_{\mathbf{i}}$, where $i_{j_l} = 1, \forall l \in [1, k]$. For example, take $n = 3$, the vector (X_1, X_3) is denoted by X_{101}, and the vector (X_1, X_2) by X_{110}. Particularly, $X_{\mathbf{i}_j} = X_j$, $j \in [1, n]$. Also, for $\mathbf{t} = \underline{1}$, the all-ones vector, $X_{\mathbf{t}} = X^n$. For two binary strings $\mathbf{i}, \mathbf{j}$, we write $\mathbf{i} \leq \mathbf{j}$ if and only if $i_k \leq j_k, \forall k \in [1, n]$. Also, we write $\mathbf{i} < \mathbf{j}$ if $\mathbf{i} \leq \mathbf{j}$ and $\mathbf{i} \neq \mathbf{j}$. For a binary string $\mathbf{i}$ we define $N_{\mathbf{i}} \triangleq \omega_H(\mathbf{i})$, where ω_H denotes the Hamming weight. Lastly, the vector $\sim \mathbf{i}$ is the element-wise complement of $\mathbf{i}$. We use $\oplus_k$ to denote addition modulo k, where $k \in \mathbb{N}$.

III. The *Effective-Length* of an Encoder

In this section, we define a set of parameters which measure the effective-length of an encoding function. We consider general Boolean functions, and find a decomposition of these functions into components which operate over specific subsets of the input sequence. The proposed decomposition builds upon the analysis in [1]. The first subsection summarizes the well-known results. The second subsection contains some new results (Proposition 1 and 3).

A. Mathematical Preliminaries

It turns out that when the input sequence is a vector of independent binary symmetric variables, the decomposition that we provide is equivalent to the Fourier transform of Boolean functions [20]. The Fourier transform does not take into account the underlying probability distribution of the sources. The connections between Fourier transforms and the correlation between outputs of pairs of functions was previously studied in [21], where the decidability of the non-interactive simulation problem was considered. We propose the decomposition for general finite input alphabets with arbitrary input distributions. We only consider encoders with binary outputs.[2] The encoder can be viewed as a vector of Boolean functions. Based on the decomposition, we define a generalization of the effective-length called the '*dependency spectrum*' of a Boolean function.

We proceed by formally defining the problem. We assume that two correlated DMS's are being fed to two arbitrary encoders, and analyze the correlation between the outputs of

[2]The analysis provided in this paper can be generalized to arbitrary finite output alphabets. The interested reader can refer to Section 7 in [1].

these encoders. The following gives the formal definition for DMS's.

Definition 1. *(X, Y) is called a pair of DMS's if we have $P_{X^n,Y^n}(x^n, y^n) = \prod_{i\in[1,n]} P_{X_i,Y_i}(x_i, y_i), \forall n \in \mathbb{N}, x^n \in \mathcal{X}^n, y^n \in \mathcal{Y}^n$, where $P_{X_i,Y_i} = P_{X,Y}, \forall i \in [1, n]$, for some joint distribution $P_{X,Y}$.*

Akin to the results presented in [1] and [8], we restrict our attention to the binary block encoders (BBE), which are defined below.

Definition 2. *A Binary-Block-Encoder is characterized by the triple $(\underline{e}, \mathcal{X}, n)$, where $\underline{e}$ is a mapping $\underline{e} : \mathcal{X}^n \to \{0, 1\}^n$, $\mathcal{X}$ is a finite set, and n is an integer.*

We refer to a BBE by its corresponding mapping $\underline{e}$. The mapping $\underline{e}$ can be viewed as a vector of functions $(e_i)_{i\in[1,n]}$, where $e_i : \mathcal{X}^n \to \{0, 1\}$. We convert the problem of analyzing a BBE into one where the encoder is a binary real-valued function. Converting the discrete-valued encoding function into a real-valued one is crucial since it allows us to use the rich set of tools available in functional analysis. We present a summary of the functional analysis apparatus used in this work.

Definition 3. *Fix a discrete memoryless source X, and a BBE $\underline{e} : \mathcal{X}^n \to \{0, 1\}^n$. Let $P\ (e_i(X^n) = 1) = q_i$. For each Boolean function $e_i, i \in [1, n]$, the real-valued function corresponding to e_i is defined as follows*:

$$\tilde{e}_i(X^n) = \begin{cases} 1 - q_i, & \text{if } e_i(X^n) = 1, \\ -q_i. & \text{otherwise.} \end{cases} \tag{1}$$

Remark 1. *Note that $\tilde{e}_i, i \in [1, n]$ has zero mean and variance $q_i(1 - q_i)$.*

The random variable $\tilde{e}_i(X^n)$ has finite variance on the probability space $(\mathcal{X}^n, 2^{\mathcal{X}^n}, P_{X^n})$. The set of all such functions is denoted by $\mathcal{H}_{X,n}$. More precisely, we define $\mathcal{H}_{X,n} \triangleq L_2(\mathcal{X}^n, 2^{\mathcal{X}^n}, P_{X^n})$ as the separable Hilbert space of all functions $\tilde{h} : \mathcal{X}^n \to \mathbb{R}$ with inner product given by $\tilde{h} \cdot \tilde{g} = \sum_{x^n} \tilde{h}(x^n)\tilde{g}(x^n)P_{X^n}(x^n)$. Since X is a DMS, the isomorphism relation

$$\mathcal{H}_{X,n} = \mathcal{H}_{X,1} \otimes \mathcal{H}_{X,1} \cdots \otimes \mathcal{H}_{X,1} \tag{2}$$

holds [22], where $\otimes$ indicates the tensor product.

Example 1. Let $n = 1$. Let $\mathcal{X} = \{0, 1\}$. The Hilbert space $\mathcal{H}_{X,1}$ is the space of all functions $\tilde{h} : \mathcal{X} \to \mathbb{R}$. The space is spanned by the two linearly independent functions $\tilde{h}_1(X) = \mathbb{1}_{\{X=1\}}$ and $\tilde{h}_2(X) = \mathbb{1}_{\{X=0\}}$. We conclude that the space is two-dimensional.

As a reminder, the following defines the tensor product of vector spaces.

Definition 4 ([22])**.** *Let $\mathcal{H}_i, i \in [1, n]$ be vector spaces over a field F. Also, let $\mathcal{B}_i = \{v_{i,j} | j \in [1, d_i]\}$ be the basis for $\mathcal{H}_i$ where d_i is the dimension of $\mathcal{H}_i$. Then, the tensor product space $\otimes_{i\in[1,n]}\mathcal{H}_i$ is defined as the set of elements $v = \sum_{j_1\in[1,d_1]} \sum_{j_2\in[1,d_2]} \cdots \sum_{j_n\in[1,d_n]} c_{j_1,j_2,\cdots,j_n} v_{j_1} \otimes v_{j_2} \cdots \otimes v_{j_n}$.*

Remark 2. *The tensor product operation in $\mathcal{H}_{X,n}$ is real multiplication (i.e. $f_1, f_2 \in \mathcal{H}_{X,1} : f_1(X_1) \otimes f_2(X_2) \triangleq f_1(X_1)f_2(X_2)$). So, if $\{f_i(X) | i \in [1, d]\}$ is a basis for $\mathcal{H}_{X,1}$ when $|\mathcal{X}| = d$, a basis for $\mathcal{H}_{X,n}$ would be the set of all the real multiplications of these basis elements: $\{\Pi_{j\in[1,n]} f_{i_j}(X_j), i_j \in [1, d]\}$.*

Example 1 gives a decomposition of the space $\mathcal{H}_{X,1}$ for binary input alphabets. Next, we introduce a decomposition of $\mathcal{H}_{X,1}$ for general alphabets which turns out to be very useful. Particularly, we argue that every Boolean function $\tilde{e}(X) \in \mathcal{H}_{X,1}$ can be written as a summation of two functions, one function whose expected value is 0, and a constant function. More precisely, let $\mathcal{I}_{X,1}$ be the subset of all functions of X which have 0 mean, and let $\gamma_{X,1}$ be the set of constant real functions of X. $\mathcal{I}_{X,1}$ and $\gamma_{X,1}$ are linear subspaces of $\mathcal{H}_{X,1}$. $\mathcal{I}_{X,1}$ is the null space of the functional which takes an arbitrary function $\tilde{f} \in \mathcal{H}_{X,1}$ to its expected value $\mathbb{E}_X(\tilde{f})$. The null space of any non-zero linear functional is a hyper-space in $\mathcal{H}_{X,1}$. So, $\mathcal{I}_{X,1}$ is a $(|\mathcal{X}| - 1)$-dimensional subspace of $\mathcal{H}_{X,1}$. On the other hand, $\gamma_{X,1}$ is a one dimensional subspace which is not contained in $\mathcal{I}_{X,1}$. It is spanned by the function $\tilde{g}(X) \equiv 1$. Consider an arbitrary element $\tilde{f} \in \mathcal{H}_{X,1}$. One can write $\tilde{f} = \tilde{f}_1 + \tilde{f}_2$ where $\tilde{f}_1 = \tilde{f} - \mathbb{E}_X(\tilde{f}) \in \mathcal{I}_{X,1}$, and $\tilde{f}_2 = \mathbb{E}_X(\tilde{f}) \in \gamma_{X,1}$. Hence, $\mathcal{H}_{X,1} = \mathcal{I}_{X,1} \oplus \gamma_{X,1}$ gives a decomposition of $\mathcal{H}_{X,1}$. Replacing $\mathcal{H}_{X,1}$ with $\mathcal{I}_{X,1} \oplus \gamma_{X,1}$ in (2), we have:

$$\begin{aligned} \mathcal{H}_{X,n} &= \otimes_{i=1}^n \mathcal{H}_{X,1} = \otimes_{i=1}^n (\mathcal{I}_{X,1} \oplus \gamma_{X,1}) \\ &\overset{(a)}{=} \oplus_{\mathbf{i}\in\{0,1\}^n} (\mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}), \end{aligned} \tag{3}$$

where

$$\mathcal{G}_j = \begin{cases} \gamma_{X,1} & j = 0, \\ \mathcal{I}_{X,1} & j = 1, \end{cases}$$

and, in (a), we have used the distributive property of tensor products over direct sums. Using equation (3) we can define the following:

Definition 5. *For any $\tilde{e} \in \mathcal{H}_{X,n}, n \in \mathbb{N}$, define the decomposition $\tilde{e} = \sum_{\mathbf{i}} \tilde{e}_{\mathbf{i}}$, where $\tilde{e}_{\mathbf{i}} \in \mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}$. Then, $\tilde{e}_{\mathbf{i}}$ is the component of $\tilde{e}$ which is only a function of $\{X_{i_j} | i_j = 1\}$. The collection $\{\tilde{e}_{\mathbf{i}} | \sum_{j\in[1,n]} i_j = k\}$, is called the set of k-letter components of $\tilde{e}$. The vector $(\tilde{e}_{\mathbf{i}})_{\mathbf{i}\in\{0,1\}^n}$ is called the real decomposition vector corresponding to $\tilde{e}$.*

In order clarify the notation, we provide the following two examples.

Example 2. Let (X_1, X_2) be two independent symmetric binary random variables. Assume $e(X_1, X_2) = X_1 \oplus X_2$ is the binary addition function. In this example $P(e = 1) = \frac{1}{2}$. The corresponding real function is given as follows:

$$\tilde{e}(X_1, X_2) = \begin{cases} -\frac{1}{2} & X_1 + X_2 \in \{0, 2\}, \\ \frac{1}{2} & X_1 + X_2 = 1, \end{cases}$$

Using Lagrange interpolation [23], we can write $\tilde{e}$ as follows:

$$\tilde{e} = -\frac{1}{2}(X_1 + X_2 - 2)(X_1 + X_2) - \frac{1}{4}(X_1 + X_2 - 1)(X_1 + X_2 - 2) - \frac{1}{4}(X_1+X_2)(X_1+X_2 - 1) = -X_1^2 - X_2^2 - 2X_1X_2 + 2X_1 + 2X_2 - \frac{1}{2}.$$

The decomposition of $\tilde{e}$ in the form given in (3) is

$$\tilde{e}_{1,1} = X_1 + X_2 - 2X_1X_2 - \frac{1}{2} = -\frac{1}{2}(1 - 2X_1)(1 - 2X_2),$$
$$\tilde{e}_{1,0} = -X_1^2 + X_1 = X_1(1 - X_1) \overset{(a)}{=} 0,$$
$$\tilde{e}_{0,1} = -X_2^2 + X_2 = X_2(1 - X_2) \overset{(a)}{=} 0,$$
$$\tilde{e}_{0,0} = 0.$$

where (a) holds since the input is chosen from $\{0, 1\}$. Note that $\tilde{e}$ has a single non-zero component in its decomposition. This component is the two-letter function $\tilde{e}_{1,1} \in \mathcal{I}_{X,1} \otimes \mathcal{I}_{X,1}$. This is to be expected since the binary addition of two symmetric variables is independent of each variable. So there are no single-letter components. In fact one can verify this directly as follows:

$$\mathbb{E}_{X_2|X_1}(\tilde{e}|X_1) = X_1 - X_1 = 0, \quad \mathbb{E}_{X_1|X_2}(\tilde{e}|X_2) = X_2 - X_2 = 0.$$

Remark 3. *In the previous example, we found that the binary summation of two independent binary symmetric variables is a two-letter function (i.e. it only has a two-letter component). However, this is not true when the source is not symmetric. When $P(X = 1) \neq P(X = 0)$, the output of the summation is not independent of each of the inputs. One can show that the single-letter components of the summation are non-zero in this case.*

Example 3. Let $e(X_1, X_2) = X_1 \wedge X_2$ be the binary logical AND function. The corresponding real function is:

$$\tilde{e}(X_1, X_2) = \begin{cases} -\frac{1}{4} & (X_1, X_2) \neq (1, 1), \\ \frac{3}{4} & (X_1, X_2) = (1, 1). \end{cases}$$

Lagrange interpolation gives $\tilde{e} = X_1X_2 - \frac{1}{4}$. The decomposition is given by:

$$\tilde{e}_{1,1} = (X_1 - \frac{1}{2})(X_2 - \frac{1}{2}), \qquad \tilde{e}_{1,0} = \frac{1}{2}(X_1 - \frac{1}{2}),$$
$$\tilde{e}_{0,1} = \frac{1}{2}(X_2 - \frac{1}{2}), \qquad \tilde{e}_{0,0} = 0.$$

The variances of these functions are given below:

$$Var(\tilde{e}) = \frac{3}{16}, \qquad Var(\tilde{e}_{0,1}) = Var(\tilde{e}_{1,0}) = Var(\tilde{e}_{1,1}) = \frac{1}{16}.$$

As we shall see in the next sections, these variances play a major role in determining the correlation preserving properties of $\tilde{e}$. In the perspective of the effective-length, the function $\tilde{e}$ has $\frac{2}{3}$ of its variance distributed between $\tilde{e}_{0,1}$, and $\tilde{e}_{1,0}$ which are single-letter functions, and $\frac{1}{3}$ of the variance is on $\tilde{e}_{1,1}$ which is a two-letter function.

Similar to the previous examples, for arbitrary $\tilde{e} \in \mathcal{H}_{X,n}, n \in \mathbb{N}$, we can find a decomposition $\tilde{e} = \sum_{\mathbf{i}} \tilde{e}_{\mathbf{i}}$, where $\tilde{e}_{\mathbf{i}} \in \mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}$. We can characterize $\tilde{e}_{\mathbf{i}}$ in terms of products of the basis elements of $\mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}$ as follows.

Lemma 1. *For an arbitrary input alphabet $\mathcal{X}$, let $\tilde{h}_l(X), l \in \{1, 2, \cdots, |\mathcal{X}| - 1\}$ be an orthogonal basis for $\mathcal{I}_{X,1}$, such that $E(\tilde{h}_l^2(X)) = q(1 - q), \forall l \in \{1, 2, \cdots, |\mathcal{X}| - 1\}$, where $q = P(X \neq 0)$. Let $\tau = \{t : i_t = 1\}$, then*:

$$\tilde{e}_{\mathbf{i}}(X^n) = \sum_{\forall t \in \tau : l_t \in [1, |\mathcal{X}|-1]} c_{\mathbf{i},(l_t)_{t\in\tau}} \prod_{t \in \tau} \tilde{h}_{l_t}(X_t), \tag{4}$$

where $c_{\mathbf{i}}, (l_t)_{t\in\tau} \in \mathbb{R}$, and $(l_t)_{t\in\tau}$ is the sequence of l_t's for $t \in \tau$.

Proof. Follows from Definition 4. □

Example 4. Let $\mathcal{X} = \{0, 1\}$. Since $\mathcal{G}_{i_j}$'s, $j \in [1, n]$ take values from the set $\{\mathcal{I}_{X,1}, \gamma_{X,1}\}$, they are all one-dimensional. Let $\tilde{h}$ be defined as follows:

$$\tilde{h}(X) = \begin{cases} 1 - q, & \text{if } X = 1, \\ -q. & \text{if } X = 0, \end{cases} \tag{5}$$

where $q \triangleq P(X = 1)$. Then, the single element set $\{\tilde{h}(X)\}$ is a basis for $\mathcal{I}_{X,1}$. Hence, using the previous lemma:

$$\tilde{e}_{\mathbf{i}}(X^n) = c_{\mathbf{i}} \prod_{t : i_t = 1} \tilde{h}(X_t), \tag{6}$$

where $c_{\mathbf{i}} \in \mathbb{R}$.

B. Properties of the Real Decomposition

The dependency spectrum and effective length of an arbitrary Boolean function are defined below.

Definition 6. *For a function $e : \mathcal{X}^n \to \{0, 1\}$, with real decomposition vector $(\tilde{e}_{\mathbf{i}})_{\mathbf{i}\in\{0,1\}^n}$, the dependency spectrum is defined as the vector $(\mathbf{P_i})_{\mathbf{i}\in\{0,1\}^n}$ of the variances, where $\mathbf{P_i} = Var(\tilde{e}_{\mathbf{i}}), \mathbf{i} \in \{0, 1\}^n$. The effective length is defined as the expected value $\widetilde{\mathbf{L}} = \frac{1}{n}\sum_{\mathbf{i}\in\{0,1\}^n} w_H(\mathbf{i}) \cdot \mathbf{P_i}$, where $w_H(\cdot)$ is the Hamming weight.*

Remark 4. *The dependency spectrum $(\mathbf{P_i})_{\mathbf{i}\in\mathbb{N}}$ characterizes the 'effect' of each component $\tilde{e}_{\mathbf{i}}$ on the output of the function $\tilde{e}$. A relevant work can be found in [24] where the output correlation of two functions with i.i.d inputs is characterized using the singular values vector of the matrix $P_X^{-\frac{1}{2}\otimes_n} P_{X,Y}^{\otimes_n} P_Y^{-\frac{1}{2}\otimes_n}$.*

In the next proposition, we show that the $\tilde{e}_{\mathbf{i}}$'s are uncorrelated and we derive an expression for $\mathbf{P_i}$ using the notation in Lemma 1.

Proposition 1. *Let X^n be a sequence of independent and identically distributed (i.i.d.) random variables and let $(\tilde{e}_{\mathbf{i}})_{\mathbf{i}\in\{0,1\}^n}$ be the real decomposition vector corresponding to the Boolean function $e(X^n)$. Define $\mathbf{P_i}$ as the variance of $\tilde{e}_{\mathbf{i}}(X_{\mathbf{i}})$. The following hold:*
1) $\mathbb{E}(\tilde{e}_{\mathbf{i}}\tilde{e}_{\mathbf{j}}) = 0, \mathbf{i} \neq \mathbf{j}$, in other words $\tilde{e}_{\mathbf{i}}$'s are uncorrelated.
2) $\mathbf{P_i} = \mathbb{E}(\tilde{e}_{\mathbf{i}}^2) = \sum_{\forall t\in\tau : l_t \in [1,|\mathcal{X}|-1]} c^2_{\mathbf{i},(l_t)_{t\in\tau}} (q(1 - q))^{w_H(\mathbf{i})}$, where w_H is the Hamming weight function. Particularly, if $\mathcal{X} = \{0, 1\}$, then $\mathbf{P_i} = \mathbb{E}(\tilde{e}_{\mathbf{i}}^2) = c_{\mathbf{i}}^2 (q(1 - q))^{w_H(\mathbf{i})}$.

Proof. 1) follows by direct calculation. 2) holds from the independence of X_i's. □

In the next lemma we find a characterization of $\tilde{e}_{\mathbf{i}}, \mathbf{i} \in \{0,1\}^n$ for general $\tilde{e}$.

Proposition 2. *Let X^n be a sequence of i.i.d. random variables and let $(\tilde{e}_{\mathbf{i}})_{\mathbf{i}\in\{0,1\}^n}$ be the real decomposition vector corresponding to the Boolean function $e(X^n)$. $\tilde{e}_{\mathbf{i}} = \mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}} \tilde{e}_{\mathbf{j}}$ gives the orthogonal decomposition of $\tilde{e}$ into the Hilbert spaces $\mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \cdots \otimes \mathcal{G}_{i_n}, \mathbf{i} \in \{0,1\}^n$.*

Proof. We prove that the $\tilde{e}_{\mathbf{i}}$ given in the lemma are indeed the decomposition into the components of the direct sum. Equivalently, we show that 1) $\tilde{e} = \sum_{\mathbf{i}} \tilde{e}_{\mathbf{i}}$, and 2) $\tilde{e}_{\mathbf{i}} \in \mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}, \forall \mathbf{i} \in \{0,1\}^n$.

First we check the equality $\tilde{e} = \sum_{\mathbf{i}} \tilde{e}_{\mathbf{i}}$. Let $\mathbf{t}$ denote the n-length vector whose elements are all ones. We have:

$$\tilde{e}_{\mathbf{t}} = \mathbb{E}_{X^n|X_{\mathbf{t}}}(\tilde{e}|X_{\mathbf{t}}) - \sum_{\mathbf{i}<\mathbf{t}} \tilde{e}_{\mathbf{i}} \overset{(a)}{\Rightarrow} \tilde{e}_{\mathbf{t}} + \sum_{\mathbf{i}<\mathbf{t}} \tilde{e}_{\mathbf{i}} = \tilde{e} \overset{(b)}{\Rightarrow} \tilde{e} = \sum_{\mathbf{i}\in\{0,1\}^n} \tilde{e}_{\mathbf{i}},$$

where in (a) we have used 1) $X_{\mathbf{t}} = X^n$ and 2) for any function $\tilde{f}$ of X^n, $\mathbb{E}_{X^n|X^n}(\tilde{f}|X^n) = \tilde{f}$, and (b) holds since $\mathbf{i} < \mathbf{t} \Leftrightarrow \mathbf{i} \neq \mathbf{t}$. It remains to show that $\tilde{e}_{\mathbf{i}} \in \mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}, \forall \mathbf{i} \in \{0,1\}^n$. The next lemma provides a means to verify this property.

Lemma 2. *Fix $\mathbf{i} \in \{0,1\}^n$, define $\mathcal{A}_0 \triangleq \{s|i_s = 0\}$, and $\mathcal{A}_1 \triangleq \{s|i_s = 1\}$. Then, $\tilde{f}$ is an element of $\mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}$ if and only if (1) it is constant in all X_s, $s \in \mathcal{A}_0$, and (2) $\mathbb{E}_{X^n|X_{\sim \mathbf{i}_s}}(\tilde{f}|X_{\sim \mathbf{i}_s}) = 0$ for all s, when $s \in \mathcal{A}_1$.*

Proof. Please refer to the appendix. □

Returning to the original problem, it is enough to show that $\tilde{e}_{\mathbf{i}}$'s satisfy the conditions in Lemma 2. We prove the stronger result presented in the next lemma.

Lemma 3. *Let X^n be a sequence of i.i.d. random variables and let $(\tilde{e}_{\mathbf{i}})_{\mathbf{i}\in\{0,1\}^n}$ be the real decomposition vector corresponding to the Boolean function $e(X^n)$. The following hold:*
1) $\forall \mathbf{i}, \mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}) = 0$.
2) $\forall \mathbf{i} \leq \mathbf{k}$, we have $\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{i}}|X_{\mathbf{k}}) = \tilde{e}_{\mathbf{i}}$.
3) $\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}\tilde{e}_{\mathbf{k}}) = 0$, for $\mathbf{i} \neq \mathbf{k}$.
4) $\forall \mathbf{k} \leq \mathbf{i} : \mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{i}}|X_{\mathbf{k}}) = 0$.

Proof. Please refer to the appendix. □

The second condition in Lemma 3 is equivalent to condition (2) in Lemma 2. The fourth condition in Lemma 3 is equivalent to condition (1) in Lemma 2. Using Lemma 2 and 3, we conclude that $\tilde{e}_{\mathbf{i}} \in \mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}, \forall \mathbf{i} \in \{0,1\}^n$. This completes the proof of Proposition 2. □

The following example clarifies the notation used in Proposition 2.

Example 5. Consider the case where $n = 2$. We have the following decomposition of $\mathcal{H}_{X,2}$:

$$\mathcal{H}_{X,2} = (\mathcal{I}_{X,1} \otimes \mathcal{I}_{X,1}) \oplus (\mathcal{I}_{X,1} \otimes \gamma_{X,1}) \oplus (\gamma_{X,1} \otimes \mathcal{I}_{X,1}) \oplus (\gamma_{X,1} \otimes \gamma_{X,1}). \tag{7}$$

Let $\tilde{e}(X_1, X_2)$ be an arbitrary function in $\mathcal{H}_{X,2}$. The decomposition of $\tilde{e}$ in the form given in (7) is as follows:

$$\begin{aligned}
\tilde{e} &= \tilde{e}_{1,1} + \tilde{e}_{1,0} + \tilde{e}_{0,1} + \tilde{e}_{0,0},\\
\tilde{e}_{1,1} &= \tilde{e} - \mathbb{E}_{X_2|X_1}(\tilde{e}|X_1) - \mathbb{E}_{X_1|X_2}(\tilde{e}|X_2)\\
&\quad + \mathbb{E}_{X_1,X_2}(\tilde{e}) \in \mathcal{I}_{X,1} \otimes \mathcal{I}_{X,1},\\
\tilde{e}_{1,0} &= \mathbb{E}_{X_2|X_1}(\tilde{e}|X_1) - \mathbb{E}_{X_1,X_2}(\tilde{e}) \in \mathcal{I}_{X,1} \times \gamma_{X,1},\\
\tilde{e}_{0,1} &= \mathbb{E}_{X_1|X_2}(\tilde{e}|X_2) - \mathbb{E}_{X_1,X_2}(\tilde{e}) \in \gamma_{X,1} \otimes \mathcal{I}_{X,1},\\
\tilde{e}_{0,0} &= \mathbb{E}_{X_1,X_2}(\tilde{e}) \in \gamma_{X,1} \otimes \gamma_{X,1}.
\end{aligned}$$

It is straightforward to show that each of the $\tilde{e}_{i,j}$'s, $i, j \in \{0,1\}$, belong to their corresponding subspaces. For instance, $\tilde{e}_{0,1}$ is constant in X_1, and is a 0 mean function of X_2 (i.e. $\mathbb{E}_{X_2}\left(\tilde{e}_{0,1}(x_1, X_2)\right) = 0, x_1 \in \mathcal{X}$), so $\tilde{e}_{0,1} \in \gamma_{X,1} \otimes \mathcal{I}_{X,1}$.

Lastly, we derive an expression for $\mathbf{P}_{\mathbf{i}}$ using Proposition 2:

Proposition 3. *For arbitrary $e : \mathcal{X}^n \to \{0,1\}$, let $\tilde{e}$ be the corresponding real-valued function, and let $\tilde{e} = \sum_{\mathbf{i}} \tilde{e}_{\mathbf{i}}$ be the decomposition in the form of Equation (3). The variance of each component in the decomposition is given by the following recursive formula $\mathbf{P}_{\mathbf{i}} = \mathbb{E}_{X_{\mathbf{i}}}(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})) - \sum_{\mathbf{j}<\mathbf{i}} \mathbf{P}_{\mathbf{j}}, \forall \mathbf{i} \in \{0,1\}^n$, where $\mathbf{P}_{\underline{0}} \triangleq 0$.*

Proof. Please refer to the appendix. □

Corollary 1. *For an arbitrary $e : \mathcal{X}^n \to \{0,1\}$ with corresponding real function $\tilde{e}$, and decomposition $\tilde{e} = \sum_{\mathbf{i}} \tilde{e}_{\mathbf{i}}$. Let the variance of $\tilde{e}$ be denoted by $\mathbf{P}$. Then, $\mathbf{P} = \sum_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}$.*

The corollary is a special case of Proposition 3, where we have taken $\mathbf{i}$ to be the all ones vector.

IV. Correlation Preservation in Arbitrary Encoders

Our objective is to bound the correlation preserving properties of general n-length encoding functions. As a first step, we derive bounds on the correlation between the outputs of two arbitrary Boolean functions (i.e. functions whose output is a binary scalar). For pedagogical reasons we present the results of this section in two parts. First, we consider binary input alphabets, and derive bounds on the probability of agreement of Boolean functions. Then, we extend these results to the case of non-binary input alphabets.

A. Binary Input Alphabets

We proceed with presenting the main result of this section. Let (X, Y) be a pair of binary DMS's. Consider two arbitrary Boolean functions $e : \{0,1\}^n \to \{0,1\}$ and $f : \{0,1\}^n \to \{0,1\}$. The following theorem provides an upper-bound on the probability of equality between the functions $e(X^n)$ and $f(Y^n)$.

Theorem 1. *Let $\epsilon \triangleq P(X \neq Y)$, the following bound holds:*

$$\begin{aligned}
&2\sqrt{\sum_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}}\sqrt{\sum_{\mathbf{i}} \mathbf{Q}_{\mathbf{i}}} - 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \leq P(e(X^n) \neq f(Y^n))\\
&\leq 1 - 2\sqrt{\sum_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}}\sqrt{\sum_{\mathbf{i}} \mathbf{Q}_{\mathbf{i}}} + 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}},
\end{aligned}$$

where $N_{\mathbf{i}} \triangleq w_H(\mathbf{i})$, $\mathbf{P}_{\mathbf{i}}$ is the variance of $\tilde{e}_{\mathbf{i}}$, and $\underline{\tilde{e}}$ is the real function corresponding to $\underline{e}$, and $\mathbf{Q}_{\mathbf{i}}$ is the variance of $\tilde{f}_{\mathbf{i}}$, and finally, $C_{\mathbf{i}} \triangleq (1-2\epsilon)^{N_{\mathbf{i}}}$.

Proof. Please refer to the appendix. □

Remark 5. *The value $C_{\mathbf{i}} = (1-2\epsilon)^{N_{\mathbf{i}}}$ is decreasing with $N_{\mathbf{i}}$. So, in order to increase $P(e(X^n) \neq f(Y^n))$, most of the variance $\mathbf{P_i}$ should be distributed on $\tilde{e}_{\mathbf{i}}$ which have lower $N_{\mathbf{i}}$ (i.e. operate on smaller blocks). Particularly, the lower bound is minimized by setting*

$$\frac{\mathbf{P_i}}{\sqrt{Var(X)}} = \frac{\mathbf{Q_i}}{\sqrt{Var(Y)}} = \begin{cases} 1 & \mathbf{i} = \mathbf{i}_1, \\ 0 & otherwise. \end{cases} \tag{8}$$

This recovers the result in [1]. More precisely, if we replace the dependency spectrum in Theorem 1 by the values in Equation (8)*, we get*:

$$2(1-C_{\mathbf{i}_1})\sqrt{Var(X)Var(Y)} \leq P(e(X^n) \neq f(Y^n)).$$

This is the bound given in Theorem 2 in [1], where $cos(\theta) = C_{\mathbf{i}_1}$.[3]

Remark 6. *For fixed $\mathbf{P_i}$, the lower-bound is minimized by taking $\tilde{e}$, and $\tilde{f}$ to be the same functions.*

Corollary 2. *We can relax the bound in Theorem 1 as follows*:

$$2\sum_{\mathbf{i}}(1-C_{\mathbf{i}})\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \leq P(e(X^n) \neq f(Y^n)) \leq 1-2\sum_{\mathbf{i}}(1-C_{\mathbf{i}})\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}$$

Proof.

$$\begin{aligned} \sigma &\geq 2\sqrt{\sum_{\mathbf{i}}\mathbf{P_i}}\sqrt{\sum_{\mathbf{i}}\mathbf{Q_i}} - 2\sum_{\mathbf{i}} C_{\mathbf{i}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \\ &\overset{(a)}{\Rightarrow} \sigma \geq 2\sum_{\mathbf{i}}\mathbf{P}_i^{\frac{1}{2}}\mathbf{Q}_i^{\frac{1}{2}} - 2\sum_{\mathbf{i}} C_{\mathbf{i}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \\ &\Rightarrow \sigma \geq 2\sum_{\mathbf{i}}(1-C_{\mathbf{i}})\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}. \end{aligned}$$

In (a) we have used the Cauchy-Schwarz inequality. □

B. Arbitrary Input Alphabets

So far, we have only considered Boolean functions with binary input alphabets. Next, we extend Theorem 1; and derive a new bound on the correlation between the outputs of Boolean functions with arbitrary (finite) input alphabets. Similar to the previous part, let (X, Y) be a pair of DMS's with joint distribution $P_{X,Y}$. Assume that the alphabets $\mathcal{X}$ and $\mathcal{Y}$ are finite sets. Consider two arbitrary Boolean functions $e : \mathcal{X}^n \to \{0, 1\}$ and $f : \mathcal{Y}^n \to \{0, 1\}$. We prove the following extension of Theorem 1.

Theorem 2. *Let $\psi \triangleq \sup(E(h(X)g(Y))$, where the supremum is taken over all single-letter functions $h : \mathcal{X} \to \mathbb{R}$, and $g : \mathcal{Y} \to \mathbb{R}$ such that $h(X)$ and $g(Y)$ have unit variance and zero mean. the following bound holds*:

$$\begin{aligned} &2\sqrt{\sum_{\mathbf{i}}\mathbf{P_i}}\sqrt{\sum_{\mathbf{i}}\mathbf{Q_i}} - 2\sum_{\mathbf{i}} C_{\mathbf{i}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \leq P(e(X^n) \neq f(Y^n)) \\ &\leq 1 - 2\sqrt{\sum_{\mathbf{i}}\mathbf{P_i}}\sqrt{\sum_{\mathbf{i}}\mathbf{Q_i}} + 2\sum_{\mathbf{i}} C_{\mathbf{i}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}, \end{aligned}$$

[3]For a definition of θ please refer to [1].

where 1) $C_{\mathbf{i}} \triangleq \psi^{N_{\mathbf{i}}}$, 2) $\mathbf{P_i}$ is the variance of $\tilde{e}_{\mathbf{i}}$, 3) $\underline{\tilde{e}}$ is the real function corresponding to $\underline{e}$, 4) $\mathbf{Q_i}$ is the variance of $\tilde{f}_{\mathbf{i}}$, and 5) $N_{\mathbf{i}} \triangleq w_H(\mathbf{i})$.

Proof. Pleas refer to the Appendix. □

Remark 7. *In Lemma 9 which was used in the proof of Theorem 1 in the Appendix, it was shown that for binary random variables X and Y, with $P(X \neq Y) = \epsilon$, we have $\psi = 1 - 2\epsilon$. So, the bounds in Theorem 1 and Theorem 2 are the same for binary inputs.*

Remark 8. *The value of ψ is in the interval $[0, 1]$. ψ is equal to one if and only if $X = Y$. The proof is straightforward and follows from the Cauchy-Schwarz inequality.*

C. Discontinuity of the Output Correlation at Asymptoticly Large Effective Lengths

In [11], it was shown that an extension of the Berger-Tung achievable region with common components for the distributed source coding problem is discontinuous in the source distribution. We argue that this is a widespread phenomenon in current coding strategies in multi-terminal communications and that it is an artifact of the discontinuity in the correlation between the outputs of functions with asymptotically large effective lengths.

Lemma 4. *Let (X^n, Y^n) be a sequence pairs of i.i.d. binary random variables and let $(\tilde{e}_{\mathbf{i}}^n)_{\mathbf{i}}$ and $(\tilde{f}_{\mathbf{i}}^n)_{\mathbf{i}\in\{0,1\}^n}$ be the real decomposition vector corresponding to the Boolean function $e^n(X^n)$ and $f^n(Y^n)$, respectively, where $(e^n(X^n), f^n(Y^n))_{n\in\mathbf{N}}$ is a sequence of pairs of Boolean functions such that:*

$$\frac{\mathbf{P}_{\mathbf{i}}^n}{\sqrt{Var(X)}} = \frac{\mathbf{Q}_{\mathbf{i}}^n}{\sqrt{Var(Y)}} = \begin{cases} 1 & \mathbf{i} = \underline{1}, \\ 0 & otherwise. \end{cases} \tag{9}$$

Then, if $\epsilon = P(X \neq Y) \neq 0$,

$$2\sqrt{\mathbf{P}_{\underline{1}}}\sqrt{\mathbf{Q}_{\underline{1}}} \leq \liminf_{n\to\infty} P(e^n(X^n) \neq f^n(Y^n)), \tag{10}$$

whereas for $\epsilon = 0$ and $e^n(\cdot) = f^n(\cdot)$, we have $P(e^n(X^n) \neq f^n(Y^n)) = 0$.

The proof of Equation (10) follows directly from Theorem 1. For $\epsilon = 0$, note that $P(X = Y) = 1$, so, given that the two Boolean function are the same, their outputs are equal with probability one.

Lemma 4 shows that functions with asymptotically large effective lengths produce outputs whose correlation is discontinuous as a function of the input distribution. In the next section, we show that single letter coding strategies produce functions with asymptotically large effective lengths. We use the discontinuity in correlation proved in Lemma 4 to show that these coding strategies are sub-optimal in various communication scenarios.

V. Correlation in Single Letter Coding Ensembles

In this section, we investigate the coding ensembles used in multi-terminal communication schemes. Deriving computable characterizations of the optimal achievable performance limits of communication networks has been a topic of significant

interest in multi-terminal information theory. One of the main instruments used in the information theoretic analysis of communication schemes is the concentration of measure properties which manifests when considering SLCE. These coding ensembles are used in schemes such as Shannon's point-to-point (PtP) source coding scheme, the Berger-Tung coding scheme for distributed source coding [25], the Zhang-Berger multiple-descriptions coding scheme [26], the Cover-El Gamal-Salehi coding scheme [6] for transmission of correlated sources over the multiple-access channel, and the Salehi-Kurtas scheme [27] for the transmission of sources over the interference channel. As a first step, it is shown that SLCEs produce encoding functions which have most of their variance either on the single-letter components or on the components with asymptotically large blocklengths. This along with Theorem 2 are used to prove that such schemes are inefficient in preserving correlation. In the next step, we provide several examples of multi-terminal scenarios where in order to achieve the optimal performance, the correlation between the outputs of the encoding functions used in different terminals must satisfy specific lower bounds which cannot be satisfied using SLCEs.

A. Single Letter Coding Ensembles

Traditionally, the probabilistic method has been used to investigate the performance of coding schemes in multi-terminal communications. The coding scheme is designed by providing a stochastic rule which chooses the encoding function from the set of all possible encoding functions. A 'good' coding scheme is one which produces 'good' encoding functions with high probability. A coding ensemble consists of a probability distribution on the set of all encoding functions:

Definition 7. *For a fixed $t \in \mathbb{N}$, let $(r_k^i)_{i\in\mathbb{N}}, k \in [1,t]$ be sequences of natural numbers which go to infinity as $i \to \infty$. Define sets of encoding functions $\mathcal{E}_k^i = \{\underline{e}_k^i : \mathcal{X}^i \to \{0,1\}^{r_k^i}\}, k \in [1,t], i \in \mathbb{N}$. A coding ensemble $\mathbb{S}$ is characterized by a sequence of probability measures $P_{\mathbb{S},i}(\underline{e}_1^i, \underline{e}_2^i, \cdots, \underline{e}_t^i), i \in \mathbb{N}$ on the set of encoding functions $\mathcal{E}_1^i \times \mathcal{E}_2^i \times \cdots \mathcal{E}_t^i$. The variable i is called the blocklength.*

Remark 9. *Whenever the choice of the coding ensemble and the blocklength is clear, we denote the distribution $P_{\mathcal{S},i}$ by $P_{\underline{E}_1,\underline{E}_1,\cdots,\underline{E}_t}(\underline{e}_1, \underline{e}_2, \cdots, \underline{e}_t)$.*

In a multi-terminal scenario with t encoders, for a given blocklength n, the coding ensemble chooses t encoding functions $\underline{E}_k^n, k \in [1,t]$ randomly and based on the joint distribution $P_{\underline{E}_1,\underline{E}_1,\cdots,\underline{E}_t}(\underline{e}_1, \underline{e}_2, \cdots, \underline{e}_t)$. Let X_k^n be the input of the kth encoder. The output of the encoder is the binary sequence $\underline{E}_k^n(X_k^n)$. The length of the output sequence is r_k^n. As an example, in Shannon's point-to-point coding ensemble, the probability distribution $P_{\underline{E}_1}(\underline{e}_1)$ on the set of encoding functions is determined by using single-letter distributions to assign probabilities to the corresponding codebooks. Shannon's method of assigning probabilities to encoding functions leads to specific properties which are shared among the coding ensembles used in many multi-terminal communication scenarios. These properties are described below. For simplicity of notation, in presenting these conditions we write $P_{\underline{E}}(\underline{e})$ instead of $P_{\underline{E}_k}(\underline{e}_k)$ when the notation does not cause ambiguity:

Definition 8. *The coding ensemble characterized by $P_{\mathbb{S},i}, i \in \mathbb{N}$ is called an SLCE if the following properties hold for every $k \in [1,t]$. Fix $k \in [1,t]$, let $\underline{E} = \underline{E}_k = (E_1, E_2, \cdots, E_n)$, then*[4]

*1) **Asymptotically Independent Codewords:** $\exists \delta_X > 0$ such that $\forall x^n, \exists \mathcal{B}_n(x^n) \subset \mathcal{X}^n$ such that the following holds:*

$$Pr(X^n \in \mathcal{B}_n(x^n)) \le 2^{-n\delta_X}, \quad \text{and}$$
$$\forall \tilde{x}^n \notin \mathcal{B}_n(x^n), e^r, \tilde{e}^r \in \{0,1\}^r :$$
$$(1 - 2^{-n\delta_X}) P_{\underline{E}(x^n)}(e^r) P_{\underline{E}(\tilde{x}^n)}(\tilde{e}^r) < P_{\underline{E}(x^n),\underline{E}(\tilde{x}^n)}(e^r, \tilde{e}^r)$$
$$< (1 + 2^{-n\delta_X}) P_{\underline{E}(x^n)}(e^r) P_{\underline{E}(\tilde{x}^n)}(\tilde{e}^r).$$

*2) **Asymptotically Independent Output Bits:** $\forall \delta > 0, \exists m \in \mathbb{N}$ such that $\forall n > m, \forall x^n \in \{0,1\}^n, \upsilon \in \{0,1\}, \forall i \in [1,n]$: $|P(E_i(X^n) = \upsilon | X^n = x^n) - P(E_i(X^n) = \upsilon | X_i = x_i)| < \delta$.*

*3) **Typicality Encoding:** $\forall \pi \in S_n : P_{\underline{E}}(\underline{E}) = P_{\underline{E}}(\underline{E}_\pi)$, where $\underline{E}_\pi(X^n) = \pi^{-1}(\underline{E}(\pi(X^n)))$, where S_n is the symmetric group of length n.*

The properties of SLCE codebooks can be explained as follows:

1) **Asymptotically Independent Codewords:** Take an arbitrary vector x^n. The condition requires that the codewords $E(x^n)$ and $E(\tilde{x})^n, \tilde{x}^n \in \{0,1\}^r$ be independently generated except for the set of vectors $\tilde{x}^n \in \mathcal{B}_n(x^n)$, where the probability of the set $\mathcal{B}_n(x^n)$ goes to 0 exponentially fast as $n \to \infty$.

An interpretation for this property is that codewords are chosen pairwise independently as the blocklength goes to infinity. For instance, let us investigate the property in the conventional Shannon code ensembles, where codewords are chosen pairwise independently. In order for $E(x^n)$ and $E(\tilde{x})^n$ to be correlated, they must be mapped to the same codeword. This requires that $\tilde{x}^n \in \mathcal{B}_n(x^n)$, where $\mathcal{B}_n(x^n)$ is the set of all vectors $\tilde{x}^n$ which are jointly typical with x^n with respect to the distribution $P_{X,\tilde{X}}$, where $P_{Y,X,\tilde{X}} = P_Y P_{X|Y} P_{\tilde{X}|Y}$.

2) **Asymptotically Independent Output Bits:** The property requires that the joint distribution of the input sequence and the output sequence of the encoding function averaged over all possible encoding functions approaches a product distribution in variational distance as $n \to \infty$ (i.e. the output bits 'look' independent.). It is well known that the property holds for conventional Shannon coding ensembles (e.g. [28]).

3) **Typicality Encoding:** The explanation for the third condition is that the probability that a vector x^n is mapped to y^n depends only on their joint type and is equal to the probability that the permuted sequence $\pi(x^n)$ is mapped to $\pi(y^n)$. As an example typicality encoding satisfies this condition.

B. Examples of Single-Letter Coding Ensembles

In the following examples, we show that the coding ensembles used in Shannon's point-to-point source coding

[4]Recall that the ith component of the vector of encoding functions $\underline{E}$ is denoted by E_i.

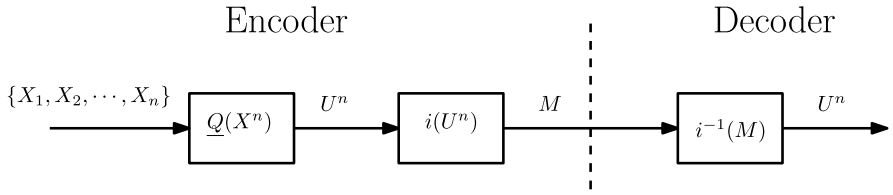

Fig. 2. Point-to-point source coding example

scheme [29] and the Cover-El Gamal-Salehi (CES) [6] scheme for the transmission of correlated sources over the multiple access channel are SLCEs.

1) Point-to-Point Source Coding: Consider the PtP source coding problem depicted in Figure 2. A discrete memoryless source X is fed to an encoder. The encoder uses the mapping $\underline{E} : \mathcal{X}^n \to \mathcal{U}^n$ to compress the source sequence. The codebook is defined as the image of $\underline{E}$. The codebook is indexed by the bijection $i : Im(\underline{E}) \to [1, |Im(\underline{E})|]$. The index $M \triangleq i(E(X^n))$ is sent to the decoder. The decoder reconstructs the compressed sequence $U^n \triangleq i^{-1}(M) = \underline{E}(X^n)$. The efficiency of the reconstruction is evaluated based on the separable distortion criteria $d_n : \mathcal{X}^n \times \mathcal{U}^n \to [0, \infty)$, where separability property means that $d_n(x^n, u^n) = \sum_{i\in[1,n]} d_1(x_i, u_i)$. We assume that the alphabets $\mathcal{X}$ and $\mathcal{U}$ are both binary. The rate of transmission is defined as $R \triangleq \frac{1}{n}\log|Im(\underline{E})|$, and the average distortion is defined as $\frac{1}{n}\mathbb{E}(d_n(X^n, U^n))$. The goal is to choose $\underline{E}$ such that the rate-distortion tradeoff is optimized. Note that the choice of the bijection 'i' does not affect the performance of the coding scheme. It is well-known that for a source X and distortion criteria $d_1 : \{0,1\} \times \{0,1\} \to [0, \infty)$, the rate-distortion pair $(R, D) = \big(r, \mathbb{E}_{X,U}(d_1(X, U))\big)$ is achievable for all $r > I(U; X)$ and conditional distributions $P_{U|X}$. The conventional proof [29] uses SLCE's to construct the coding scheme. In order to verify the properties of the SLCE's in the coding ensemble in [29], we provide an outline of the scheme. Fix $n \in \mathbb{N}$, and $\epsilon > 0$. Define $P_U(u) = \mathbb{E}_X\{P_{U|X}(u|X))\}$. In [29], a randomly generated encoding function is constructed with the aid of a set of vectors called the codebook, and typicality encoding. The codebook $\mathcal{C}$ is constructed as follows. Let $A_\epsilon^n(U) \triangleq \{u^n \big| |\frac{1}{n}w_H(u^n) - P_U(1)| < \epsilon\}$ be the set of n-length binary vectors which are ϵ-typical with respect to P_U. The codebook $\mathcal{C}$ is constructed by choosing $\lceil 2^{nR}\rceil$ vectors from $A_\epsilon^n(U)$ randomly and uniformly. For an arbitrary sequence $x^n \in \{0,1\}^n$, define $A_\epsilon^n(U|x^n)$ as the set of vectors in $\mathcal{C}$ which are jointly ϵ-typical with x^n with respect to $P_{U|X}$. The vector $\underline{E}(x^n)$ is chosen randomly and uniformly from $A_\epsilon^n(U|x^n) \cap \mathcal{C}$.

Remark 10. *The codebook generation process could be altered in the following way: instead of choosing the codewords randomly and uniformly from the set of typical sequences $A_\epsilon^n(U)$, the encoder can produce each codeword independent of the others and with the distribution $P_{U^n}(u^n) = \Pi_{i\in[1,n]}P_U(u_i)$. However, the discussion that follows remains unchanged regardless of which of these codebook generation methods are used.*

Lemma 5. *The ensemble described above is a SLCE.*

Proof. Please refer to the Appendix. □

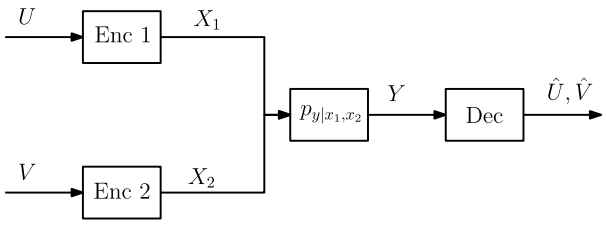

Fig. 3. Transmission of Sources over MAC

2) Transmission of Correlated Sources Over the Multiple Access Channel (CS-MAC): Consider the problem of the lossless transmission of the sources U and V over a MAC depicted in Figure 3. The largest known transmissible region for this problem is achieved using the CES scheme. The following lemma gives the transmissible region using the CES scheme in absence of common components (i.e. when there is no random variable W such that (a) $H(W) > 0$, (b) $W = f(U) = g(V)$.)

Lemma 6. *[6] The sources U, and V are transmissible over a CS-MAC with channel input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and output alphabet $\mathcal{Y}$, and channel transition probability $p(y|x_1, x_2)$, if there exists a probability mass function $p(x_1|u)p(x_2|v)$ such that*:

$$H(U|V) < I(X_1; Y|X_2, V),$$
$$H(V|U) < I(X_2; Y|X_1, U),$$
$$H(U, V) < I(X_1, X_2; Y),$$

where $p(u, v, x_1, x_2) = p(u, v)p(x_1|u)p(x_2|v)$.

Similar to the previous example achievability is proved by providing a coding ensemble which specifies a probability distribution $P_{\mathbb{S}}(\mathbf{e}_1, \mathbf{e}_2)$ on the set of pairs of encoding functions at the two transmitters. The CES scheme generates the encoding functions independently (i.e. $P_{\mathbb{S}}(\mathbf{e}_1, \mathbf{e}_2) = P_{\mathbb{S}}(\mathbf{e}_1)P_{\mathbb{S}}(\mathbf{e}_2)$). Each of the encoding functions is generated by a method similar to the previous example. Hence, the marginals $P_{\mathbb{S}}(\mathbf{e}_i), i \in \{1, 2\}$ each satisfy the conditions in Definition 8. So, the coding ensemble is a SLCE.

C. Bounds on Output Correlation for SLCEs: The 1-∞ Law

Our objective is to analyze the correlation preserving properties of SLCE's. For a randomly generated encoding function $\underline{E} = (E_1, E_2, \cdots, E_n)$, denote the decomposition of the real function corresponding to the kth element into the form in Equation (3) as $\tilde{E}_k = \sum_{\mathbf{i}} \tilde{E}_{k,\mathbf{i}}, k \in [1, n]$. Let $\mathbf{P}_{k,\mathbf{i}}$ be the variance of $\tilde{E}_{k,\mathbf{i}}$. For a fixed $m \in \mathbb{N}$, we are interested in the quantity $\sum_{\mathbf{i}:N_{\mathbf{i}}\le m, \mathbf{i}\neq 00\cdots 01} \mathbf{P}_{k,\mathbf{i}}$ which is the total variance allocated to components of the decomposition

which operate on at most m elements of the input except for the single-letter component. From Theorem 1 we know that if $\sum_{\mathbf{i}:N_{\mathbf{i}}\leq m,\mathbf{i}\neq 00\cdots 01}\mathbf{P}_{k,\mathbf{i}}$ is small, then the encoding function preserves less correlation. The following proposition shows that the probability $P_{\mathcal{S}}(\sum_{\mathbf{i}:N_{\mathbf{i}}\leq m,\mathbf{i}\neq\mathbf{i}_k}\mathbf{P}_{k,\mathbf{i}}\geq\gamma)$ is independent of the index k. This is due to property 3) in the Definition 8 of SLCE's.

Proposition 4. *$P_{\mathcal{S}}(\sum_{\mathbf{i}:N_{\mathbf{i}}\leq m,\mathbf{i}\neq 00\cdots 01}\mathbf{P}_{k,\mathbf{i}}\geq\gamma)$ is constant as a function of k.*

Proof. Please refer to the Appendix. □

The next theorem shows that most of the variance in the components of the decomposition of $\tilde{E}_k$ is concentrated in the single-letter component $\tilde{E}_{k,\mathbf{i}_k}$ and the large effective length components of the decomposition. We refer to this as the 1-∞ law. The proof of the theorem is provided in the Appendix.

Theorem 3. *For any $k\in\mathbb{N}, m\in\mathbb{N}, \gamma>0$, $P_{\mathcal{S}}(\sum_{\mathbf{i}:N_{\mathbf{i}}\leq m,\mathbf{i}\neq\mathbf{i}_k}\mathbf{P}_{k,\mathbf{i}}\geq\gamma)\to 0$, as $n\to\infty$, where, $\mathbf{i}_k$ is the kth standard basis element.*

Remark 11. *Theorem 3 shows that SLCE's distribute most of the variance of $\tilde{E}_k$ on $\tilde{E}_{k,\mathbf{i}}$'s which operate on large blocks. Hence, the encoders generated using such ensembles have high expected effective-lengths. This along with Theorem 1 gives an upper bound on the correlation preserving properties of SLCE's. This is stated in the following theorem.*

Theorem 4. *Let (X,Y) be a pair of DMS's, with $P(X=Y)=1-\epsilon$. Also, assume that the pair of BBE's $\underline{E},\underline{F}$ are produced using SLCE's. Define $E\triangleq E_1$, and $F\triangleq F_1$. Then,*

$$\forall\delta>0: P_{\mathcal{S}}\left(P_{X^n,Y^n}\left(E(X^n)\neq F(Y^n)\right)>\zeta\right)\to 1,$$

as $n\to\infty$, where $\zeta=2\mathbf{P}^{\frac{1}{2}}\mathbf{Q}^{\frac{1}{2}}-2(1-2\epsilon)\mathbf{P}_{\mathbf{i}_1}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}_1}^{\frac{1}{2}}-\delta$, $\mathbf{P}_{\mathbf{i}}\triangleq Var(\tilde{E}_{\mathbf{i}})$, $\mathbf{Q}_{\mathbf{i}}\triangleq Var(\tilde{F}_{\mathbf{i}})$, $\mathbf{P}\triangleq Var(\tilde{E})$, and $\mathbf{Q}\triangleq Var(\tilde{F})$.

The proof is provided in the Appendix.

Remark 12. *Note that in this theorem we consider a pair of BBEs produced using SLCEs. The bound is presented as function of the dependency spectra of the two BBEs. The two SLCEs can have arbitrary correlation. As an example, E and F can be taken to be either independent or exactly equal to each other.*

Remark 13. *The previous theorem gives a bound on the correlation preserving properties on SLCE's. The theorem shows that in order to increase correlation in these schemes the encoder needs to put more variance on the element $\tilde{E}_{k,\mathbf{i}_k}, k\in[1,n]$. This would require more correlation between the input and output of the encoder, which itself would require more rate. As an example consider the extreme case where $Var(\tilde{E}_k)=Var(\tilde{E}_{k,\mathbf{i}_k})$, which requires $E_k(X^n)=X_k$. This means that in order to achieve maximum correlation, the encoder must use uncoded transmission.*

Remark 14. *In the case when $X=Y$, there is common-information [8] available at the encoders. If the encoders use the same encoding function E, their outputs would be equal. Whereas from theorem 4, for any non-zero ϵ, the output correlation is bounded away from 0 (except when doing uncoded transmission). So, the correlation between the outputs of SLCE's is discontinuous as a function of ϵ.*

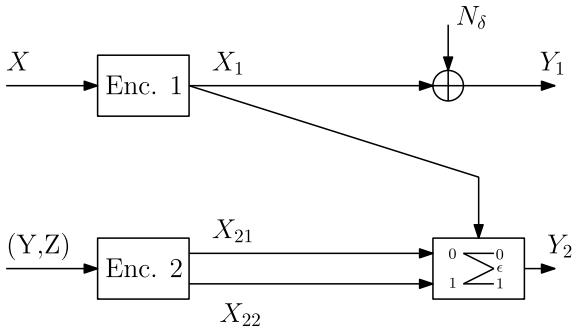

Fig. 4. An CS-IC example where SLCEs are suboptiomal.

VI. Multi-Terminal Communication Examples

In this section, we provide two examples of multi-terminal communication problems where SLCEs have suboptimal performance. We use the discontinuity mentioned in the previous section to show the sub-optimality of SLCEs.

A. Transmission of Correlated Sources Over the Interference Channel

Consider the problem of transmission of correlated sources over the interference channel (CS-IC) described in [27]. We examine the specific CS-IC setup shown in Figure 4. We are restricting our attention to bandwidth expansion factor equal to one. Here, the sources X and Y are Bernoulli random variables with parameters α_X and α_Y, and Z is a q-ary random variable with distribution P_Z. X and Z are independent. Y and Z are also independent. Finally, X and Y are correlated, and $P(X\neq Y)=\epsilon$. The random variable N_δ is Bernoulli with parameter δ. Decoder one reconstructs X and decoder two reconstructs Z losslessly. The first transmitter transmits the binary input X_1, and the second transmitter transmits the pair of inputs (X_{21},X_{22}), where X_{21} is q-ary and X_{22} is binary. Receiver 1 receives $Y_1=X_1\oplus_2 N_\delta$, and receiver 2 receives Y_2 which is given below:

$$Y_2=\begin{cases}X_{21}, & \text{if } X_{22}=X_1,\\ e, & otherwise.\end{cases}\tag{11}$$

So, the second channel outputs X_{21} noiselessly if the second encoder 'guesses' the first encoder's output correctly (i.e. $X_{22}=X_1$), otherwise an erasure is produced. The following proposition gives a set of sufficient conditions for the transmission of correlated sources over this interference channel:

Proposition 5. *The sources X and Z are transmissible if there exist $\epsilon,\gamma,d>0$, and $n\in\mathbb{N}$ such that:*

$$H(X)\leq(1-h_b(\delta))\left(1-\frac{h_b(\gamma+d)}{1-h_b(\delta)}\right)+O\left(\frac{1+\sqrt{nV+k\mathcal{V}(d)}Q^{-1}(\gamma)}{\sqrt{n}}\right),$$
$$H(Z)\leq\left((1-\epsilon)^k\log q\right)\left(1-\frac{h_b(\gamma+d)}{1-h_b(\delta)}\right),$$

where $h_b(\cdot)$ is the binary entropy function, $V = \delta(1-\delta)log_2(\frac{1-\delta}{\delta})$ is the channel dispersion, and $\mathcal{V}(d)$ is the rate-dispersion function as in [30], and $Q(.)$ is the Gaussian complementary cumulative distribution function.

For a fixed n, ϵ and γ, we denote the set of pairs $(H(X), H(Z))$ which satisfy the bounds by $S(n, \epsilon, \gamma)$.

Proof. First we provide an outline of the coding strategy. Fix $n, m \in \mathbb{N}, d, \gamma \in \mathbb{R}$, where $n \ll m$. Let $k = n\left(1 - \frac{h_b(d+\gamma)}{1-h_b(\delta)}\right)^{-1}$. The encoders send km bits of the compressed input at each block of transmission. The first encoder transmits its source in two steps. First, it uses a fixed blocklength source-channel code [30] with parameters (k, n, d, γ). The code maps k-length blocks of the source to n-length blocks of the channel input, and the average distortion resulting from the code is less than $d + \gamma$. In this step, the encoder transmits the source in m blocks of length k. A total of nm channel uses are needed (note that n<k). In the second step, the encoder uses a large blocklength code to correct the errors in the previous step. The code has rate close to $\frac{h_b(\gamma+d)}{1-h_b(\delta)}$, and its input length is equal to km.

The second encoder only transmits messages in the first step of transmission. It uses the same fixed blocklength code as the first encoder and the source sequence Y^k to estimate the outcome of the first encoder. It sends this estimate of the first encoder's output on X_{22}^n. Since $P(X^k = Y^k) = (1-\epsilon)^k$, we conclude that X_1^k and X_{22}^k are equal at least with probability $(1-\epsilon)^k$. The encoder sends the source Z using X_{21} over the resulting q-ary erasure channel which has probability of erasure at most $(1-\epsilon)^k$. The following provides a detailed descriptions of the coding strategy:

Codebook Generation: Fix n, ϵ, d. Let $k = n\left(1 - \frac{h_b(d+\gamma)}{1-h_b(\delta)}\right)^{-1}$. Let C_k be the optimal source-channel code with parameters (k, n, d, γ) for the point-to-point transmission of a binary source over the binary symmetric channel, as described in [30]. The code transmits k-length blocks of the source using n-length blocks of the channel input; and guarantees that the resulting distortion at each block is less than d with probability $(1-\epsilon)$ (i.e $P(d_H(X^n, \hat{X}^n) > d) \leq \gamma$, where $\hat{X}$ is the reconstruction of the binary source X at the decoder). In [30], it is shown that the parameters of the code satisfy:

$$n(1-h_b(\delta)) - k\,(H(X) - h_b(\alpha_X * d)) = \sqrt{nV + k\mathcal{V}(d)}\,Q^{-1}(\gamma) + O(log(n)).$$

Since $P(d_H(X^n, \hat{X}^n) > d) \leq \gamma$, it is straightforward to show that the average distortion is less than or equal to $\gamma + d$. Also, construct a family of good channel codes $C'_m, m \in \mathbb{N}$ for the binary symmetric channel with rate $R_m = 1 - h_b(\delta) - \lambda_m$, where $\lambda_m \to 0$ as $m \to \infty$. Next, construct a family of good channel codes $C''_m, m \in \mathbb{N}$ for the q-ary erasure channel with rate $R_m = (1-\epsilon)^k log(q) - \lambda_m$. Finally, randomly and uniformly bin the space of binary vectors of length kn with rate $R' = h_n(d+\gamma)$. More precisely, generate a binning function $B : \{0,1\}^{km} \to \{0,1\}^{kmR'}$, by mapping any vector $\mathbf{i}$ to a value chosen uniformly from $\{0,1\}^{kmR'}$.

Encoding: Fix m. At each block the encoders transmit km symbols of the source input. Let the source sequences be denoted by $X(1:k, 1:m), Y(1:k, 1:m), Z(1:k, 1:m)$, where we have broken the source vectors into m blocks of length k. In this notation $X(i, j)$ is the ith element of the jth block, and $X(1:k, j)$, $j \in [1, m]$ is the jth block.

Step 1: Encoder 1 uses the code C_k to transmit each of the blocks $X(1:k, i), i \in [1, m]$ to the decoder. The second encoder finds the output of the code C_k when $Y(1:k, i)$ is fed to the code, and transmits the output vector on $X_{22}(1:n, i)$. The encoder uses an interleaving method similar to the one in [12] to transmit Z. For the sequence $Z(1:k, 1:m)$, it finds the output of C''_{km} for this input and transmits it on $X_{21}(1:n, 1:m)$.

Step 2: The first encoder transmits $B(X(1:k, 1:m))$ to the decoder losslessly using $C'_{kmR'}$.

Decoding: In the first step, the first decoder reconstructs $X(1:k, 1:m)$ with average distortion at most $\gamma + d$. In the second step, using the bin number $B(X(1:k, 1:m))$ it can losslessly reconstruct the source, since $C'_{kmR'}$ is a good channel code. Decoder 2 also recovers $Z(1:k, 1:m)$ losslessly using $Y_2(1:k, 1:m)$ since C''_{km} is a good channel code.

The conditions for successful transmission is given as follows:

$$n(1-h_b(\delta)) - k\,(H(X) - h_b(\alpha_X * d)) \geq \sqrt{nV + k\mathcal{V}(d)}\,Q^{-1}(\gamma) + O(log(n)),$$
$$n(1-\epsilon)^k log(q) \geq kH(Z).$$

Simplifying these conditions by replacing $k = n\left(1 - \frac{h_b(d+\gamma)}{1-h_b(\delta)}\right)^{-1}$ proves the proposition. □

The bound provided in Proposition 5 is not calculable without the exact characterization of the $O(\frac{log(n)}{n})$ term. However, we use this bound to prove the sub-optimality of SLCEs. First, we argue that the transmissible region is 'continuous' as a function of ϵ. Note that for $\epsilon = 0$, sources with parameters $(H(X), H(Z)) = (1 - h_b(\delta), \log q)$ are transmissible. The region in Proposition 5 is continuous in the sense that as ϵ approaches 0, the pairs $(H(X), H(Z))$ in the neighborhood of $(1 - h_b(\delta), \log q)$ satisfy the bounds given in the proposition (i.e. the corresponding sources are transmissible).

Proposition 6. *For all $\lambda > 0$, there exist $\epsilon_0, \gamma_0 > 0$, and $n_0 \in \mathbb{N}$ such that*:

$$\forall \epsilon < \epsilon_0 : (1 - h_b(\delta) - \lambda, \log q - \lambda) \in S(n_0, \epsilon, \gamma_0).$$

Proof. Follows directly from Proposition 5. □

For an arbitrary encoding scheme operating on blocks of length n, let the encoding functions be as follows: $X_1^n = \underline{e}_1(X^n)$, and $(X_{21}^n, X_{22}^n) = (\underline{e}_{21}(Y^n, Z^n), \underline{e}_{22}(Y^n, Z^n))$. The following lemma gives an outer bound on $H(Z)$ as a function of the correlation between the outputs of $\underline{e}_1$ and $\underline{e}_{21}$.

Lemma 7. *For a coding scheme with encoding functions $\underline{e}_1(X^n), \underline{e}_{21}(Y^n, Z^n), \underline{e}_{22}(Y^n, Z^n)$, the following holds*:

$$H(Z) \leq \frac{1}{n}\sum_{i=1}^{n} P(e_{1,i}(X^n) = e_{22,i}(Y^n, Z^n)) + 1. \qquad (12)$$

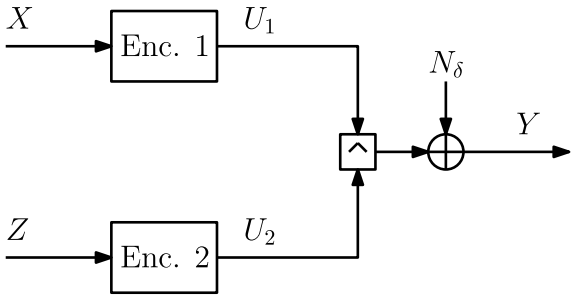

Fig. 5. A CS-MAC example where SLCEs are suboptiomal.

Proof. Since Z^n is reconstructed losslessly at the decoder, by Fano's inequality the following holds:

$$\begin{aligned} H(Z^n) &\approx I(Y_2^n; Z^n) \overset{(a)}{=} I(E^n, Y_2^n; Z^n) \\ &= I(E^n; Z^n) + I(Y_2^n; Z^n|E^n) \\ &\overset{(b)}{\leq} H(E^n) + \sum_{i=1}^{n} P(e_{1,i}(X^n) = e_{22,i}(Y^n, Z^n)) \log q \\ &\overset{(c)}{\leq} n + \sum_{i=1}^{n} P(e_{1,i}(X^n) = e_{22,i}(Y^n, Z^n)) \log q, \end{aligned}$$

where in (a) we have defined E^n as the indicator function of the event that $Y_2 = e$, in (b) we have used Equation (11) and in (c) we have used the fact that E^n is a binary vector. □

Using Theorem 4, we show that if the encoding functions are generated using SLCEs, $P(e_{1,i}(X^n) = e_{22,i}(Y^n, Z^n))$ is discontinuous in ϵ. The next proposition shows that SLCEs are sub-optimal:

Proposition 7. *There exists $\lambda > 0$, and $q \in \mathbb{N}$, such that sources with $(H(X), H(Z)) = (1 - h_b(\delta) - \lambda, \log q - \lambda)$ are not transmissible using SLCEs.*

Proof. Let $X_1^n = \underline{E}_1(X^n)$, and $X_{22^n} = \underline{E}_{22,z^n}(Y^n), z^n \in \{0,1\}^n$ be the encoding functions used in the two encoders to generate X_1 and X_{22}. If $H(Z) \approx \log(q)$, from (12), we must have $P(E_{1,j}(X^n) = E_{22,z^n,j}(Y^n)) \approx 1$ for almost all of the indices $j \in [1, n]$. From Theorem 4, this requires $\mathbf{P}_{j,\mathbf{i}_j} \approx 1$, which requires uncoded transmission (i.e. $X_1^n = \underline{E}(X^n) \approx X^n$). However, uncoded transmission contradicts the lossless reconstruction of the source at the first decoder. □

The proof is not restricted to any particular scheme, rather it shows that any SLCE would have sub-optimal performance.

B. Transmission of Correlated Sources Over the Multiple Access Channel (CS-MAC)

We examine the CS-MAC setup shown in Figure 5. Again, we restrict our attention to bandwidth expansion factor equal to one. Here, the source X is a q-ary source. The source Z is defined as $Z = X \oplus_q N_\epsilon$, where N_ϵ is a q-ary random variable with

$$P(N_\epsilon = i) = \begin{cases} 1-\epsilon, & \text{if } i = 0, \\ \frac{\epsilon}{q-1} & \text{if } i \in \{1, 2, \cdots, q-1\}, \end{cases}$$

and

$$P(N_\delta = i) = \begin{cases} 1-\delta, & \text{if } i = 0, \\ \frac{\delta}{q-1} & \text{if } i \in \{1, 2, \cdots, q-1\}, \end{cases}$$

The output is:

$$Y = U_1 \wedge U_2 \oplus_q N_\delta = \begin{cases} U_2 \oplus_q N_\delta, & \text{if } U_1 = U_2, \\ N_\delta & \text{if } U_1 \neq U_2, \end{cases}$$

where U_1 and U_2 are the outputs of Encoder 1 and Encoder 2, respectively. The goal is to transmit both sources X and Z losslessly to the decoder.

In this setup, there are two strategies available to the encoders. The first strategy is for both encoders to transmit the sources simultaneously. In this case, the encoders must have equal outputs. Otherwise, the decoder receives the noise N_δ. So, in this strategy, the encoders must 'guess' each other's outputs. The second strategy is to make a binary symmetric channel with noise δ for one of the encoders, while the other encoder does not transmit any messages. For example, in order to create such a channel for Encoder 1, encoder two transmits a constant sequence $U_2^n = (j, j, \cdots, j), j \in [1, q-1]$. Then, Encoder 2 can transmit a binary codeword using alphabet $\{0, j\}$. The rates of transmission for this strategy is:

$$\begin{aligned} R_{s,1} &= \max_{p(U_1)} I(U_1; Y) \\ &= h\left(\frac{1}{2}\left(1 - \frac{(q-2)\delta}{q-1}\right), \frac{1}{2}\left(1 - \frac{(q-2)\delta}{q-1}\right), \frac{\delta}{q-1}, \cdots, \frac{\delta}{q-1}\right) \\ &\quad - h\left(1-\delta, \frac{\delta}{q-1}, \cdots, \frac{\delta}{q-1}\right), \\ R_{s,2} &= 0. \end{aligned}$$

The following Proposition gives a condition under which the sources are transmissible:

Proposition 8. *There exists positive reals $\lambda_\epsilon, \epsilon \in (0, \frac{1}{2}]$, with $\lim_{\epsilon \to 0} \lambda_\epsilon = 0$, such that the sources X and Y are transmissible if the following condition is satisfied*:

$$H(X) \leq \log q - H(N_\delta) - \lambda_\epsilon.$$

Proof. The ideas in this proof are similar to the ones in Proposition 5. We provide an outline of the proof here. There are two steps for the transmission of the sources. First, the first strategy described above is used to transmit at a rate close to $\log q - H(N_\delta)$. In this step, the encoders use a finite blocklength code to maximize their probability of agreement. In the second step, the encoders use the second strategy described above to correct the errors from the first step. The errors in the first step vanish as $\epsilon \to 0$, since the sources become equal with probability going to one. So, the rate of transmission approaches the rate of the first step which is close to $\log q - H(N_\delta)$. We provide a more detailed summary of the proof: Fix n. Both encoders use an finite blocklength source-channel code for the q-ary symmetric channel with noise N_δ to transmit the sources. Let the blocklength of this code be equal to n, and the rate be equal to $\log q - H(N_\delta) + O(\frac{1}{\sqrt{n}})$. From the problem statement $P(X^n = Z^n) = P(N_\epsilon^n = 0^n) = (1-\epsilon)^n$. Since U_1^n is a function of X^n, a and U_2^n is a function of Z^n, we conclude

that $P(U_1^n = U_2^n) \geq (1-\epsilon)^n$. The encoders then take turns to send refinements to the decoder. This is done using the second strategy described above. The rate required for this part of the transmission is $\frac{(1-\epsilon)^n}{R_{s,1}} + \frac{H(N_\epsilon)}{R_{s,1}}$. Note that $\frac{(1-\epsilon)^n}{R_{s,1}} + \frac{H(N_\epsilon)}{R_{s,1}}$ goes to 0 as $\epsilon \to 0$. This completes the proof. □

The following lemma provides an upper-bound to the entropy of X as a function of ϵ and the correlation between U_1 and U_2.

Lemma 8. *For a coding scheme with encoding functions $U_1^n = \underline{e}_1(X^n), U_2^n = \underline{e}_2(Z^n)$, the following holds*:

$$H(X) \leq \frac{1}{n}\sum_{i=1}^{n} P(U_{1,i} = U_{2,i})\,(\log q - H(N_\delta)) + 1. \quad (13)$$

Proof. Similar to the proof of Lemma 7, we use Fano's inequality to prove the lemma. Since X^n is reconstructed losslessly at the decoder, by Fano's inequality the following holds:

$$\begin{aligned}
H(X^n) &\approx I(U_1^n U_2^n; Y^n)\\
&\leq \sum_{i=1}^{n} I(U_{1,i}U_{2,i}; Y_i) \overset{(a)}{=} \sum_{i=1}^{n} I(E_i, U_{1,i}U_{2,i}; Y_n)\\
&= \sum_{i=1}^{n} I(E_i; Y_i) + I(U_{1,i}U_{2,i}; Y_i|E_i)\\
&\overset{(b)}{\leq} H(E_i) + \sum_{i=1}^{n} P(U_{1,i} = U_{2,i})(Y^n, Z^n))\,(\log q - H(N_\delta))\\
&\overset{(c)}{\leq} n + \sum_{i=1}^{n} P(U_{1,i} = U_{2,i})\,(\log q - H(N_\delta))\,,
\end{aligned}$$

where in (a) we have defined E_i as the indicator function of the event that $U_{1,i} = U_{2_i}, i \in [1,n]$, in (b) we have used that $I(U_{1,i}U_{2,i}; Y_i|E_i) = P(E_i = 0)\cdot 0 + P(E_i = 1)I(U_{1,i}; Y|U_{1,i} = U_{2,i})$ and in (c) we have used the fact that E^n is binary.

□

Since for SLCE's $P(U_{1,i} = U_{2,i})$ is bounded away from 1 for $\epsilon \neq 0$, we conclude that there exists q and N_δ such that $\frac{1}{n}\sum_{i=1}^{n} P(U_{1,i} = U_{2,i})\,(\log q - H(N_\delta)) + 1 \leq \log q - H(N_\delta)$. So, SLCE's are suboptimal in this example as well.

VII. Conclusion

We derived a new bound on the maximum correlation between Boolean functions operating on pairs of sequences of random variable. The bound was presented as a function of the dependency spectrum of the functions. We developed a new mathematical apparatus for analyzing Boolean functions, provided formulas for decomposing the Boolean function into additive components, and for calculating the dependency spectrum of these functions. The new bound may find applications in security, control and information theory.

Next, we characterized a set of properties which are shared between the SLCEs used in the literature. We showed that ensembles which have these properties produce encoding functions which are inefficient in preserving correlation. We derived a probabilistic upper-bound on the correlation between the outputs of random encoders generated using SLCEs. We showed that the correlation between the outputs of such encoders is discontinuous with respect to the input distribution. We used this discontinuity to show that all SLCSs are sub-optimal in two specific multi-terminal communications problem involving the transmission of correlated source.

Appendix

A. Proof of Lemma 2

Proof. By definition, any element of $\mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}$ satisfies the conditions in the proposition. Conversely, we show that any function satisfying the conditions (1) and (2) is in the tensor product. Let $\tilde{f} = \sum_{\mathbf{j}} \tilde{f}_{\mathbf{j}}$, $\tilde{f}_{\mathbf{j}} \in \mathcal{G}_{j_1} \otimes \mathcal{G}_{j_2} \otimes \cdots \otimes \mathcal{G}_{j_n}$ be an arbitrary function satisfying conditions (1) and (2). Assume $i_k = 1$ for some $k \in [1,n]$. Then:

$$\begin{aligned}
0 &\overset{(2)}{=} \mathbb{E}_{X^n|X_{\sim \mathbf{i}_k}}\Big(\sum_{\mathbf{j}} \tilde{f}_{\mathbf{j}}|X_{\sim \mathbf{i}_k}\Big) \overset{(a)}{=} \sum_{\mathbf{j}} \mathbb{E}_{X^n|X_{\sim \mathbf{i}_k}}(\tilde{f}_{\mathbf{j}}|X_{\sim \mathbf{i}_k})\\
&\overset{(1)}{=} \sum_{\mathbf{j}:j_k=0} \mathbb{E}_{X^n|X_{\sim \mathbf{i}_k}}(\tilde{f}_{\mathbf{j}}|X_{\sim \mathbf{i}_k}) \overset{(2)}{=} \sum_{\mathbf{j}:j_k=0} \tilde{f}_{\mathbf{j}},
\end{aligned}$$

where we have used linearity of expectation in (a), and the last two equalities use the fact that $\tilde{f}_{\mathbf{j}} \in \mathcal{G}_{j_1} \otimes \mathcal{G}_{j_2} \otimes \cdots \otimes \mathcal{G}_{j_n}$ which means it satisfies properties (1) and (2). So far we have shown that $\tilde{f} = \sum_{\mathbf{j} \geq \mathbf{i}} \tilde{f}_{\mathbf{j}}$. Recall that $\mathbf{i}$ is given in the statement of the proposition. Now assume $i_{k'} = 0$. Then:

$$\begin{aligned}
\sum_{\mathbf{j}\geq\mathbf{i}} \tilde{f}_{\mathbf{j}} = \tilde{f} &\overset{(1)}{=} \mathbb{E}_{X^n|X_{\sim \mathbf{i}_{k'}}}\Big(\sum_{\mathbf{j}\geq\mathbf{i}} \tilde{f}_{\mathbf{j}}|X_{\sim \mathbf{i}_{k'}}\Big)\\
&= \sum_{\mathbf{j}\geq\mathbf{i}} \mathbb{E}_{X^n|X_{\sim \mathbf{i}_{k'}}}(\tilde{f}_{\mathbf{j}}|X_{\sim \mathbf{i}_{k'}}) = \sum_{\mathbf{j}\geq\mathbf{i}:j_{k'}=0} \tilde{f}_{\mathbf{j}} \Rightarrow \sum_{\mathbf{j}\geq\mathbf{i}:j_{k'}=1} \tilde{f}_{\mathbf{j}} = 0.
\end{aligned}$$

So, $\tilde{f} = \sum_{\mathbf{i}\geq\mathbf{j}\geq\mathbf{i}} \tilde{f}_{\mathbf{j}} = \tilde{f}_{\mathbf{i}}$. By assumption we have $\tilde{f}_{\mathbf{i}} \in \mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}$. □

B. Proof of Lemma 3

Proof. 1) For two n-length binary vectors $\mathbf{i}$, and $\mathbf{j}$, we write $\mathbf{i} \leq \mathbf{j}$ if $i_k \leq j_k, \forall k \in [1,n]$. The set $\{0,1\}^n$ equipped with $\leq$ is a well-founded set (i.e. any subset of $\{0,1\}^n$ has at least one minimal element). The following presents the principle of Noetherian induction on well-founded sets:

Proposition 9 (Principle of Noetherian Induction [31])**.** *Let $(A, \preccurlyeq)$ be a well-founded set. To prove the property $P(x)$ is true for all elements x in A, it is sufficient to prove the following*

*1) **Induction Basis:** $P(x)$ is true for all minimal elements in A.*

*2) **Induction Step:** For any non-minimal element x in A, if $P(y)$ is true for all minimal y such that $y \prec x$, then it is true for x.*

We will use Noetherian induction to prove the result. Let $\mathbf{i}_j, j \in [1,n]$ be the jth element of the standard basis. Then $\tilde{e}_{\mathbf{i}_j} = \mathbb{E}_{X^n|X_j}(\tilde{e}|X_j)$. By the smoothing property of expectation, $\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}_j}) = \mathbb{E}_{X^n}(\tilde{e}) = 0$. Assume that $\forall \mathbf{j} < \mathbf{i}$,

$\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}) = 0$. Then,

$$\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}) = \mathbb{E}_{X^n}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}} \tilde{e}_{\mathbf{j}}\right) = \mathbb{E}_{X^n}(\tilde{e}) - \sum_{\mathbf{j}<\mathbf{i}} \mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}) = 0 - \sum_{\mathbf{j}<\mathbf{i}} 0 = 0.$$

2) This statement is also proved by induction. $\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})$ is a function of $X_{\mathbf{i}}$, so by induction $\tilde{e}_{\mathbf{i}} = \mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}} \tilde{e}_{\mathbf{k}}$ is also a function of $X_{\mathbf{i}}$.

3) Let $\mathbf{i}_k, k \in [1, n]$ be defined as the kth element of the standard basis, and take $j, j' \in [1, n]$, $j \neq j'$. We have:

$$\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}_j}\tilde{e}_{\mathbf{i}_{j'}}) = \mathbb{E}_{X^n}(\mathbb{E}_{X^n|X_j}(\tilde{e}|X_j)\mathbb{E}_{X^n|X_{j'}}(\tilde{e}|X_{j'})) \overset{(a)}{=} \mathbb{E}_{X^n}(\mathbb{E}_{X^n|X_j}(\tilde{e}|X_j))\mathbb{E}_{X^n}(\mathbb{E}_{X^n|X_{j'}}(\tilde{e}|X_{j'})) \overset{(b)}{=} \mathbb{E}^2_{X^n}(\tilde{e}) = 0,$$

where we have used the memoryless property of the source in (a) and (b) results from the smoothing property of expectation. We extend the argument by Noetherian induction. Fix $\mathbf{i}, \mathbf{k}$. Assume that $\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}\tilde{e}_{\mathbf{j}'}) = \mathbb{1}(\mathbf{j} = \mathbf{j}')\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}), \forall \mathbf{j} < \mathbf{i}, \mathbf{j}' \leq \mathbf{k}$, and $\forall \mathbf{j} \leq \mathbf{i}, \mathbf{j}' \leq \mathbf{k}$. Then, we have

$$\begin{aligned}
&\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}\tilde{e}_{\mathbf{k}}) \\
&= \mathbb{E}_{X^n}\left(\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}} \tilde{e}_{\mathbf{j}}\right)\left(\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}}) - \sum_{\mathbf{j}'<\mathbf{k}} \tilde{e}_{\mathbf{j}'}\right)\right) \\
&= \mathbb{E}_{X_n}\big(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})\big) - \sum_{\mathbf{j}<\mathbf{i}} \mathbb{E}_{X^n}\big(\tilde{e}_{\mathbf{j}}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})\big) \\
&- \sum_{\mathbf{j}'<\mathbf{k}} \mathbb{E}_{X^n}\left(\tilde{e}_{\mathbf{j}'}\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) + \sum_{\mathbf{j}<\mathbf{i},\mathbf{j}'<\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}\tilde{e}_{\mathbf{j}'}).
\end{aligned}$$

The second and third terms in the above expression can be simplified as follows. First, note that:

$$\tilde{e}_{\mathbf{i}} = \mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}} \tilde{e}_{\mathbf{j}} \Rightarrow \sum_{\mathbf{j}\leq\mathbf{i}} \tilde{e}_{\mathbf{j}} = \mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}). \quad (14)$$

Our goal is to simplify $\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}\mathbb{E}_{X^n|X_{\mathbf{j}'}}(\tilde{e}|X_{\mathbf{j}'}))$. We proceed by considering two different cases:

Case 1: $\mathbf{i} \not\leq \mathbf{k}$ and $\mathbf{k} \not\leq \mathbf{i}$:

Let $\mathbf{j} < \mathbf{i}$:

$$\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})) \overset{(14)}{=} \mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}\sum_{\mathbf{l}\leq\mathbf{k}} \tilde{e}_{\mathbf{l}})) = \sum_{\mathbf{l}\leq\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}}\tilde{e}_{\mathbf{l}}) = \sum_{\mathbf{l}\leq\mathbf{k}} \mathbb{1}(\mathbf{j} = \mathbf{l})\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) = \mathbb{1}(\mathbf{j} \leq \mathbf{k})\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}).$$

By the same arguments, for $\mathbf{j}' \leq \mathbf{k}$:

$$\mathbb{E}_{X^n}\left(\tilde{e}_{\mathbf{j}'}\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) = \mathbb{1}(\mathbf{j}' \leq \mathbf{i})\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}'}).$$

Replacing the terms in the original equality we get:

$$\begin{aligned}
\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}\tilde{e}_{\mathbf{k}}) &= \mathbb{E}_{X^n}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})\right) \quad (15)\\
&- \sum_{\mathbf{j}<\mathbf{i}} \mathbb{1}(\mathbf{j} \leq \mathbf{k})\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) \\
&- \sum_{\mathbf{j}'\leq\mathbf{k}} \mathbb{1}(\mathbf{j}' \leq \mathbf{i})\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}'} + \sum_{\mathbf{j}<\mathbf{i},\mathbf{j}'<\mathbf{k}} \mathbb{1}(\mathbf{j} = \mathbf{j}')\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}).
\end{aligned}$$

Note that:

$$\sum_{\mathbf{j}<\mathbf{i}} \mathbb{1}(\mathbf{j} \leq \mathbf{k})\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) = \sum_{\mathbf{j}<\mathbf{i},\mathbf{j}\leq\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) = \sum_{\mathbf{j}\leq\mathbf{i}\wedge\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}})$$
$$\sum_{\mathbf{j}'\leq\mathbf{k}} \mathbb{1}(\mathbf{j}' \leq \mathbf{i})\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}'} = \sum_{\mathbf{j}'\leq\mathbf{k},\mathbf{j}'\leq\mathbf{i}} \mathbb{E}_{X^n}(\tilde{e}_{\mathbf{j}'} = \sum_{\mathbf{j}\leq\mathbf{i}\wedge\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}})$$
$$\sum_{\mathbf{j}<\mathbf{i},\mathbf{j}'<\mathbf{k}} \mathbb{1}(\mathbf{j} = \mathbf{j}')\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}} = \sum_{\mathbf{j}\leq\mathbf{i}\wedge\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}})$$

Replacing the terms in (15), we have:

$$\begin{aligned}
\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}\tilde{e}_{\mathbf{k}}) &= \mathbb{E}_{X^n}\big(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})\big) - \sum_{\mathbf{j}\leq\mathbf{i}\wedge\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) \\
&\overset{(a)}{=} \mathbb{E}_{X^n}(\mathbb{E}^2_{X^n|X_{\mathbf{i}\wedge\mathbf{k}}}(\tilde{e}(X^n)|X_{\mathbf{i}\wedge\mathbf{k}})) - \sum_{\mathbf{j}\leq\mathbf{i}\wedge\mathbf{k}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) \\
&\overset{(b)}{=} \mathbb{E}_{X^n}(\mathbb{E}^2_{X^n|X_{\mathbf{i}\wedge\mathbf{k}}}(\tilde{e}(X^n)|X_{\mathbf{i}\wedge\mathbf{k}})) - \mathbb{E}_{X^n}\left((\sum_{\mathbf{j}\leq\mathbf{i}\wedge\mathbf{k}} \tilde{e}_{\mathbf{j}})^2\right) \overset{(14)}{=} 0,
\end{aligned}$$

where in (b) we have used that $\tilde{e}_{\mathbf{i}}$'s are uncorrelated, and (a) is proved below:

$$\begin{aligned}
&\mathbb{E}_{X^n}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})\right) \\
&= \sum_{x_{\mathbf{i}\wedge\mathbf{k}}} P(x_{\mathbf{i}\wedge\mathbf{k}})\left(\left(\sum_{x_{|\mathbf{i}-\mathbf{k}|^+}} P(x_{|\mathbf{i}-\mathbf{k}|^+})\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) \times \right. \\
&\left.\left(\sum_{x_{|\mathbf{k}-\mathbf{i}|^+}} P(x_{|\mathbf{k}-\mathbf{i}|^+})\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})\right)\right) \\
&= \sum_{x_{\mathbf{i}\wedge\mathbf{k}}} P(x_{\mathbf{i}\wedge\mathbf{k}})\mathbb{E}^2_{X^n|X_{\mathbf{i}\wedge\mathbf{k}}}(\tilde{e}|x_{\mathbf{i}\wedge\mathbf{k}}) \\
&= \mathbb{E}_{X^n}(\mathbb{E}^2_{X^n|X_{\mathbf{i}\wedge\mathbf{k}}}(\tilde{e}(X^n)|X_{\mathbf{i}\wedge\mathbf{k}})).
\end{aligned}$$

Case 2: Assume $\mathbf{i} \leq \mathbf{k}$:

$$\begin{aligned}
&\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}\tilde{e}_{\mathbf{k}}) \\
&= \mathbb{E}_{X^n}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}})\right) - \sum_{\mathbf{j}<\mathbf{i}} \mathbb{1}(\mathbf{j} \leq \mathbf{k})\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) \\
&- \sum_{\mathbf{j}'<\mathbf{k}} \mathbb{1}(\mathbf{j}' \leq \mathbf{i})\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}'}) + \sum_{\mathbf{j}<\mathbf{i},\mathbf{j}'<\mathbf{k}} \mathbb{1}(\mathbf{j} = \mathbf{j}')\mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) \\
&\overset{(a)}{=} \mathbb{E}_{X^n}(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})) - \sum_{\mathbf{j}<\mathbf{i}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) \\
&- \sum_{\mathbf{j}'\leq\mathbf{i}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}'}) + \sum_{\mathbf{j}\leq\mathbf{i}} \mathbb{E}_{X^n}(\tilde{e}^2_{\mathbf{j}}) \\
&= 0,
\end{aligned}$$

where in (a) we have used (a) proved above.

Case 3: When $\mathbf{k} \leq \mathbf{i}$ the proof is similar to case 2.

4) Clearly when $|\mathbf{i}| = 1$, the claim holds. Assume it is true for all $\mathbf{j}$ such that $|\mathbf{j}| < |\mathbf{i}|$. Take $\mathbf{i} \in \{0, 1\}^n$ and $t \in [1, n], i_t = 1$

arbitrarily. We first prove the claim for $\mathbf{k} = \mathbf{i} - \mathbf{i}_t$:

$$\begin{aligned}
&\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{i}}|X_{\mathbf{k}}) = \mathbb{E}_{X^n|X_{\mathbf{k}}}\left(\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)|X_{\mathbf{k}}\right)\\
&= \mathbb{E}_{X^n|X_{\mathbf{k}}}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})|X_{\mathbf{k}}\right) - \sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{j}}|X_{\mathbf{k}})\\
&\overset{(a)}{=} \mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}}) - \sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{j}}|X_{\mathbf{k}})\\
&\overset{(b)}{=} \sum_{\mathbf{j}\le\mathbf{i}-\mathbf{i}_t}\tilde{e}_{\mathbf{j}} - \sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{j}}|X_{\mathbf{k}})\\
&\overset{(c)}{=} \sum_{\mathbf{j}\le\mathbf{i}-\mathbf{i}_t}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{j}}|X_{\mathbf{k}}) - \sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{j}}|X_{\mathbf{k}})\\
&= \sum_{s\neq t}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{i}-\mathbf{i}_s}|X_{\mathbf{k}})\\
&\overset{(d)}{=} \sum_{s\neq t}\mathbb{E}_{X^n|X_{\mathbf{k}-\mathbf{i}_s}}(\tilde{e}_{\mathbf{i}-\mathbf{i}_s}|X_{\mathbf{k}-\mathbf{i}_s}) \overset{(e)}{=} 0,
\end{aligned}$$

where in (a) we have used $\mathbf{i} > \mathbf{k}$, (b) follows from equation (14), also (c) follows from $\mathbf{j} < \mathbf{k}$, (e) uses $\mathbf{k} \wedge (\mathbf{i} - \mathbf{i}_s) = \mathbf{k} - \mathbf{i}_s$, and finally, (d) uses the induction assumption. Now we extend the result to general $\mathbf{k} < \mathbf{i}$. Fix $\mathbf{k}$. Assume the claim is true for all $\mathbf{j}$ such that $\mathbf{k} < \mathbf{j} < \mathbf{i}$ (i.e $\forall \mathbf{k} < \mathbf{j} < \mathbf{i}$, $\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{X_{\mathbf{j}}|X_{\mathbf{k}}}) = 0$). We have:

$$\begin{aligned}
&\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{i}}|X_{\mathbf{k}})\\
&= \mathbb{E}_{X^n|X_{\mathbf{k}}}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}|X_{\mathbf{k}}\right)\\
&= \mathbb{E}_{X^n|X_{\mathbf{k}}}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})|X_{\mathbf{k}}\right) - \sum_{\mathbf{j}\le\mathbf{k}}\mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}_{\mathbf{j}}|X_{\mathbf{k}})\\
&= \mathbb{E}_{X^n|X_{\mathbf{k}}}(\tilde{e}|X_{\mathbf{k}}) - \sum_{\mathbf{j}\le\mathbf{k}}\tilde{e}_{\mathbf{j}} \overset{(14)}{=} 0.
\end{aligned}$$

□

C. Proof of Proposition 3

Proof.

$$\begin{aligned}
&\mathbf{P}_{\mathbf{i}} = Var_{X_{\mathbf{i}}}(\tilde{e}_{\mathbf{i}}(X^n)) = \mathbb{E}_{X_{\mathbf{i}}}(\tilde{e}^2_{\mathbf{i}}(X^n)) - \mathbb{E}^2_{X_{\mathbf{i}}}(\tilde{e}_{\mathbf{i}}(X^n))\\
&\overset{(a)}{=} \mathbb{E}_{X_{\mathbf{i}}}\left(\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)^2\right) - 0\\
&= \mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) - 2\sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\tilde{e}_{\mathbf{j}}\right)\\
&+ \mathbb{E}_{X_{\mathbf{i}}}\left(\left(\sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)^2\right)\\
&\overset{(b)}{=} \mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) - 2\sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}_{X^n|X_{\mathbf{i}}}(\sum_{\mathbf{l}\le\mathbf{i}}\tilde{e}_{\mathbf{l}}|X_{\mathbf{i}})\tilde{e}_{\mathbf{j}}\right)\\
&+ \mathbb{E}_{X_{\mathbf{i}}}\left(\left(\sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)^2\right)
\end{aligned}$$

$$\begin{aligned}
&\overset{(c)}{=} \mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) - 2\sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{i}}}\left(\sum_{\mathbf{l}\le\mathbf{i}}\mathbb{E}_{X^n|X_{\mathbf{i}}}(\tilde{e}_{\mathbf{l}}|X_{\mathbf{i}})\tilde{e}_{\mathbf{j}}\right)\\
&+ \mathbb{E}_{X_{\mathbf{i}}}\left(\left(\sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)^2\right)\\
&\overset{(d)}{=} \mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) - 2\sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{i}}}\left(\sum_{\mathbf{l}<\mathbf{i}}\tilde{e}_{\mathbf{l}}\tilde{e}_{\mathbf{j}}\right)\\
&+ \mathbb{E}_{X_{\mathbf{i}}}\left(\left(\sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)^2\right)\\
&\overset{(e)}{=} \mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) - 2\sum_{\mathbf{j}<\mathbf{i}}\sum_{\mathbf{l}<\mathbf{i}}\mathbb{1}(\mathbf{j}=\mathbf{l})\mathbb{E}_{X_{\mathbf{i}}}\left(\tilde{e}_{\mathbf{l}}\tilde{e}_{\mathbf{j}}\right)\\
&+ \mathbb{E}_{X_{\mathbf{i}}}\left(\left(\sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)^2\right)\\
&= \mathbb{E}_{X_{\mathbf{i}}}\left(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})\right) - 2\sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{j}}}(\tilde{e}^2_{\mathbf{j}}) + \mathbb{E}_{X_{\mathbf{i}}}\left(\left(\sum_{\mathbf{j}<\mathbf{i}}\tilde{e}_{\mathbf{j}}\right)^2\right)\\
&= \mathbb{E}_{X_{\mathbf{i}}}(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})) - 2\sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{j}}}(\tilde{e}^2_{\mathbf{j}}) + \sum_{\mathbf{j}<\mathbf{i}}\sum_{\mathbf{k}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{i}}}(\tilde{e}_{\mathbf{j}}\tilde{e}_{\mathbf{k}})\\
&\overset{(f)}{=} \mathbb{E}_{X_{\mathbf{i}}}(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})) - 2\sum_{\mathbf{j}<\mathbf{i}}\mathbb{E}_{X_{\mathbf{j}}}(\tilde{e}^2_{\mathbf{j}})\\
&+ \sum_{\mathbf{j}<\mathbf{i}}\sum_{\mathbf{k}<\mathbf{i}}\mathbb{1}(\mathbf{j}=\mathbf{k})\mathbb{E}_{X_{\mathbf{i}}}(\tilde{e}^2_{\mathbf{j}}) = \mathbb{E}_{X_{\mathbf{i}}}(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{e}|X_{\mathbf{i}})) - \sum_{\mathbf{j}<\mathbf{i}}\mathbf{P}_{\mathbf{j}},
\end{aligned}$$

□

where (a) follows from condition 1) in Lemma 3, b) follows from the decomposition in Equation (14) in the appendix, (c) uses linearity of expectation, (d) holds from condition 2) in Lemma 3, and in (e) and (f) we have used condition 1) in Lemma 3.

D. Proof of Theorem 1

Proof. This proof builds upon the results in [1]. The proof involves three main steps. In the first two steps we prove the lower bound. First, we bound the Pearson correlation [32] between the real-valued functions $\tilde{e}$, and $\tilde{f}$. In the second step, we relate the correlation to the probability that the two functions are equal and derive the necessary bounds. Finally, in the third step we use the lower bound proved in the first two steps to derive the upper bound.

Step 1: Let $s \triangleq P_X(e(X^n) = 1)$, $r \triangleq P_Y(f(Y^n) = 1)$. From Remark 1, the expectation of both functions is 0. So, the Pearson correlation is given by

$$\frac{\mathbb{E}_{X^n,Y^n}(\tilde{e}\,\tilde{f})}{(rs(1-s)(1-r))^{\frac{1}{2}}}.$$

Our goal is to bound this value. We have:

$$\mathbb{E}_{X^n,Y^n}(\tilde{e}\,\tilde{f}) \overset{(a)}{=} \mathbb{E}_{X^n,Y^n}\left((\sum_{\mathbf{i}\in\{0,1\}^n}\tilde{e}_{\mathbf{i}})(\sum_{\mathbf{k}\in\{0,1\}^n}\tilde{f}_{\mathbf{k}})\right)$$

$$\overset{(b)}{=} \sum_{\mathbf{i}\in\{0,1\}^n} \sum_{\mathbf{k}\in\{0,1\}^n} \mathbb{E}_{X^n,Y^n}(\tilde{e}_{\mathbf{i}}\tilde{f}_{\mathbf{k}}). \tag{16}$$

In (a) we have used Definition 5, and in (b) we use linearity of expectation. Using the fact that $\tilde{e}_{\mathbf{i}} \in \mathcal{G}_{i_1} \otimes \mathcal{G}_{i_2} \otimes \cdots \otimes \mathcal{G}_{i_n}$ and Definition 4, we have:

$$\tilde{e}_{\mathbf{i}} = c_{\mathbf{i}} \prod_{t:i_t=1} \tilde{h}(X_t),\ \tilde{f}_{\mathbf{k}} = d_{\mathbf{k}} \prod_{t:k_t=1} \tilde{g}(Y_t). \tag{17}$$

where,

$$\tilde{h}(X) = \begin{cases} 1-q, & \text{if } X=1, \\ -q. & \text{if } X=0, \end{cases}, \qquad \tilde{g}(Y) = \begin{cases} 1-r, & \text{if } Y=1, \\ -r. & \text{if } Y=0, \end{cases} \tag{18}$$

We replace $\tilde{e}_{\mathbf{i}}$ and $\tilde{f}_{\mathbf{k}}$ in (16):

$$\mathbb{E}_{X^n,Y^n}(\tilde{e}_{\mathbf{i}}\tilde{f}_{\mathbf{k}}) \overset{(17)}{=} \mathbb{E}_{X^n,Y^n}\left(\left(c_{\mathbf{i}} \prod_{t:i_t=1} \tilde{h}(X_t)\right)\left(d_{\mathbf{k}} \prod_{s:k_s=1} \tilde{g}(Y_s)\right)\right) \tag{19}$$

$$\begin{aligned}
&\overset{(a)}{=} c_{\mathbf{i}}d_{\mathbf{k}}\mathbb{E}_{X^n,Y^n}\left(\prod_{t:i_t=1} \tilde{h}(X_t) \prod_{s:k_s=1} \tilde{g}(Y_s)\right) \\
&\overset{(b)}{=} c_{\mathbf{i}}d_{\mathbf{k}}\mathbb{E}_{X^n,Y^n}\left(\prod_{t:i_t=1,k_t=1} \tilde{h}(X_t)\tilde{g}(Y_{k_t})\right)\mathbb{E}_{X^n}\left(\prod_{t:i_t=1,k_t=0} \tilde{h}(X_t)\right) \\
&\quad \times \mathbb{E}_{Y^n}\left(\prod_{t:i_t=0,k_t=1} \tilde{g}(Y_{k_t})\right) \\
&\overset{(c)}{=} \mathbb{1}(\mathbf{i}=\mathbf{k})c_{\mathbf{i}}d_{\mathbf{k}} \prod_{t:i_t=1} \mathbb{E}_{X^n,Y^n}\left(\tilde{h}(X_t)\tilde{g}(Y_t)\right) \\
&\overset{(d)}{\leq} \mathbb{1}(\mathbf{i}=\mathbf{k})c_{\mathbf{i}}d_{\mathbf{k}}(1-2\epsilon)^{N_{\mathbf{i}}} \prod_{t:i_t=1} \mathbb{E}^{\frac{1}{2}}_{X^n}\left(\tilde{e}^2(X_t)\right)\mathbb{E}^{\frac{1}{2}}_{Y^n}\left(\tilde{g}^2(Y)\right) \\
&\overset{(e)}{=} \mathbb{1}(\mathbf{i}=\mathbf{k})(1-2\epsilon)^{N_{\mathbf{i}}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} = \mathbb{1}(\mathbf{i}=\mathbf{k})C_{\mathbf{i}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}.
\end{aligned} \tag{20}$$

(a) follows from linearity of expectation. In (b) we have used the fact that in a pair of DMS's, X_i and Y_j are independent for $i \neq j$. (c) holds since from Lemma 3, $\mathbb{E}(\tilde{e}_i) = \mathbb{E}(\tilde{f}_i) = 0, \forall i \in [1,n]$. We prove (d) in Lemma 9 below. In (e) we have used proposition 1.

Lemma 9. *Let $g(X)$ and $h(Y)$ be two arbitrary zero-mean, real valued functions, then*:

$$\mathbb{E}_{X,Y}(g(X)h(Y)) \leq (1-2\epsilon)\mathbb{E}^{\frac{1}{2}}_X(g^2(X))\mathbb{E}^{\frac{1}{2}}_Y(h^2(Y)).$$

Proof. This is a well-known result [33]. A proof is provided here for completeness: Let the functions be given as follows:

$$g(X) = \begin{cases} \alpha & \text{if } X=0 \\ \beta & \text{if } X=1. \end{cases}, \qquad h(Y) = \begin{cases} \gamma & \text{if } Y=0 \\ \delta & \text{if } Y=1. \end{cases}$$

Also, let $P(X=1)=p$, and $P(Y=1)=q$. The zero-mean condition enforces the following equalities:

$$\alpha(1-p)+\beta p = 0 \Rightarrow \beta = \frac{-(1-p)\alpha}{p},$$
$$\gamma(1-q)+\delta q = 0 \Rightarrow \delta = \frac{-(1-q)\gamma}{q}.$$

Next, we calculate the joint distribution of P_{XY}. Let $P_{i,j} \triangleq P(X=i,Y=j), i,j \in \{0,1\}$. We have the following:

$$\begin{aligned}
P_{0,0}+P_{0,1} &= P(X=0) = 1-p, \\
P_{0,0}+P_{1,0} &= P(Y=0) = 1-q, \\
P_{0,0}+P_{1,1} &= P(X=Y) = 1-\epsilon, \\
P_{0,0}+P_{0,1}+P_{1,0}+P_{1,1} &= 1.
\end{aligned}$$

Solving the system of equations yields:

$$P_{0,0} = 1 - \frac{p+q+\epsilon}{2}, \qquad P_{0,1} = \frac{q+\epsilon-p}{2}, \tag{21}$$
$$P_{1,0} = \frac{p+\epsilon-q}{2}, \qquad P_{1,1} = \frac{p+q-\epsilon}{2}. \tag{22}$$

With the following constraint on the variables:

$$\begin{aligned}
p+\epsilon &\geq q, \qquad p+q \geq \epsilon, \\
q+\epsilon &\geq p, \qquad p+q+\epsilon \leq 2.
\end{aligned}$$

We have:

$$\frac{\mathbb{E}_{X,Y}(gh)}{\mathbb{E}^{\frac{1}{2}}_X(g^2)\mathbb{E}^{\frac{1}{2}}_Y(h^2)} \tag{23}$$

$$\begin{aligned}
&= \frac{\alpha\gamma\left(P_{0,0} - P_{0,1}\frac{(1-q)}{q} - P_{1,0}\frac{(1-p)}{p} + P_{1,1}\frac{(1-q)(1-p)}{pq}\right)}{\alpha\gamma\left(\left((1-p)+\frac{(1-p)^2}{p}\right)^{\frac{1}{2}}\left((1-q)+\frac{(1-q)^2}{q}\right)^{\frac{1}{2}}\right)} \\
&= \frac{P_{0,0} - P_{0,1}\frac{(1-q)}{q} - P_{1,0}\frac{(1-p)}{p} + P_{1,1}\frac{(1-q)(1-p)}{pq}}{(\frac{1-p}{p})^{\frac{1}{2}}(\frac{1-q}{q})^{\frac{1}{2}}} \\
&= \frac{P_{0,0}pq - P_{0,1}(1-q)p}{(pq(1-p)(1-q))^{\frac{1}{2}}} \\
&\quad - \frac{P_{1,0}(1-p)q - P_{1,1}(1-q)(1-p)}{(pq(1-p)(1-q))^{\frac{1}{2}}} \\
&\overset{(22)}{=} \frac{(1-\frac{p+q+\epsilon}{2})pq - (\frac{q+\epsilon-p}{2})(1-q)p}{(pq(1-p)(1-q))^{\frac{1}{2}}} \\
&\quad + \frac{-(\frac{p+\epsilon-q}{2})(1-p)q + (\frac{p+q-\epsilon}{2})(1-q)(1-p)}{(pq(1-p)(1-q))^{\frac{1}{2}}} \\
&= \frac{pq + (\frac{p+q}{2})\left((1-p)(1-p) - pq\right)}{(pq(1-p)(1-q))^{\frac{1}{2}}} + \\
&\quad + \frac{(\frac{q-p}{2})\left(q(1-p) - p(1-q)\right))}{(pq(1-p)(1-q))^{\frac{1}{2}}} + \\
&\quad \frac{\frac{\epsilon}{2}(pq + p(1-q) + q(1-p) + (1-p)(1-q))}{(pq(1-p)(1-q))^{\frac{1}{2}}} \\
&= \frac{pq + \frac{p+q}{2}(1-p-q) - \frac{p-q}{2}(q-p) - \frac{\epsilon}{2}}{(pq(1-p)(1-q))^{\frac{1}{2}}} \\
&= \frac{p+q-2pq-\epsilon}{2\left(pq(1-p)(1-q)\right)^{\frac{1}{2}}}.
\end{aligned} \tag{24}$$

We calculate the optimum point by taking partial derivatives:

$$\begin{aligned}
&\frac{\delta}{\delta p}\frac{\mathbb{E}_{X,Y}(gh)}{\mathbb{E}_X^{\frac{1}{2}}(g^2)\mathbb{E}_Y^{\frac{1}{2}}(h^2)} = 0 \Rightarrow \\
&2(1-2q)(pq(1-p)(1-q))^{\frac{1}{2}} \\
&-\frac{(1-2p)}{\sqrt{p(1-p)}}\sqrt{q(1-q)}(p+q-2pq-\epsilon) = 0 \\
&\overset{(a)}{\Rightarrow} 2(1-2q)p(1-p) - (1-2p)(p+q-2pq-\epsilon) = 0 \\
&\Rightarrow 2p(1-p)(1-2q) - p(1-2p)(1-2q) \\
&-(1-2p)q + (1-2p)\epsilon = 0 \\
&\Rightarrow p(1-2q) - (1-2p)q + (1-2p)\epsilon = 0 \\
&\Rightarrow p - q + (1-2p)\epsilon = 0. \qquad (25)
\end{aligned}$$

Where in (a) we have used $p, q \notin \{0,1\}$ to multiply by $\sqrt{pq(1-p)(1-q)}$. Taking the partial derivative with respect to q, by similar calculations we get:

$$\frac{\delta}{\delta q}\frac{\mathbb{E}_{X,Y}(gh)}{\mathbb{E}_X^{\frac{1}{2}}(g^2)\mathbb{E}_Y^{\frac{1}{2}}(h^2)} = 0 \rightarrow q - p + (1-2q)\epsilon. \qquad (26)$$

In order for (25) and (26) to be satisfied simultaneously, we must have $\epsilon = 0$, $p = q$, or $\epsilon = p+q = 1$, or $p = q = \frac{1}{2}$. For $\epsilon \notin \{0,1\}$, we must have $p = q = \frac{1}{2}$ in which case the value in (24) is:

$$\frac{\mathbb{E}_{X,Y}(gh)}{\mathbb{E}_X^{\frac{1}{2}}(g^2)\mathbb{E}_Y^{\frac{1}{2}}(h^2)} = 1 - 2\epsilon.$$

This completes the proof of the Lemma. □

Using equations (16) and (20) we get:

$$\mathbb{E}_X(\tilde{e}\tilde{f}) \leq \sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}.$$

Step 2: We use the results from step one to derive a bound on $P(e \neq f)$. Define $a \triangleq P(e(X^n) = 1, f(Y^n) = 1)$, $b \triangleq P(e(X^n) = 0, f(Y^n) = 1)$, $c \triangleq P(e(X^n) = 1, f(Y^n) = 0)$, and $d \triangleq P(e(X^n) = 0, f(Y^n) = 0)$, then

$$\begin{aligned}
&\mathbb{E}_{X^n,Y^N}(\tilde{e}(X^n)\tilde{f}(Y^n)) \\
&\quad = a(1-s)(1-r) - bs(1-r) - c(1-s)r + dsr, \qquad (27)
\end{aligned}$$

We write this equation in terms of $\sigma \triangleq P(f \neq g)$, s, and r using the following relations:

1) $a + c = s$, 2) $b + d = 1 - s$,
3) $a + b = r$, 4) $c + d = 1 - r$, 5) $b + c = \sigma$.

Solving the above we get:

$$a = \frac{s + r - \sigma}{2}, \qquad b = \frac{r + \sigma - s}{2}, \qquad (28)$$
$$c = \frac{s - r + \sigma}{2}, \qquad d = 1 - \frac{s + r + \sigma}{2}. \qquad (29)$$

We replace a, b, c, and d in (27) by their values in (29):

$$\begin{aligned}
&\frac{\sigma}{2} \geq (\frac{s+r}{2})(1-s)(1-r) + (\frac{s-r}{2})s(1-r) \\
&+ (\frac{r-s}{2})(1-s)r + sr(1-\frac{s+r}{2}) - \sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \\
&\Rightarrow \sigma \geq s + r - 2rs - 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \\
&\Rightarrow \sigma \geq (\sqrt{s(1-r)} - \sqrt{r(1-s)})^2 + 2\sqrt{s(1-s)r(1-r)} \\
&- 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \\
&\Rightarrow \sigma \geq 2\sqrt{s(1-s)r(1-r)} - 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}
\end{aligned}$$

On the other hand $\mathbb{E}_X(\tilde{e}^2) = s(1-s) = \sum_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}$, where the last equality follows from the fact that $\tilde{e}_{\mathbf{i}}$'s are uncorrelated. This proves the lower bound. Next we use the lower bound to derive the upper bound.

Step 3: The upper-bound can be derived by considering the function $h(Y^n)$ to be the complement of $f(Y^n)$ (i.e. $h(Y^n) \triangleq 1 \oplus_2 f(Y^n)$.) In this case $P(h(Y^n) = 1) = P(f(Y^n) = 0) = 1 - r$. The corresponding real function for $h(Y^n)$ is:

$$\begin{aligned}
\tilde{h}(Y^n) &= \begin{cases} r & \text{if } h(Y^n) = 1, \\ -(1-r) & \text{if } h(Y^n) = 0, \end{cases} \\
&= \begin{cases} r & \text{if } f(Y^n) = 0, \\ -(1-r) & \text{if } f(Y^n) = 1, \end{cases} \Rightarrow \tilde{h}(Y^n) = -\tilde{f}(Y^n).
\end{aligned}$$

So, $\tilde{h}(Y^n) = -\sum_{\mathbf{i}} \tilde{f}_{\mathbf{i}}$. Using the same method as in the previous step, we have:

$$\begin{aligned}
&\mathbb{E}_{X^n,Y^n}(\tilde{e}\tilde{h}) = -\mathbb{E}_{X^n,Y^n}(\tilde{e}\tilde{f}) \leq \sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \\
&\Rightarrow P(e(X^n) \neq h(Y^n)) \geq 2\sqrt{\sum_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}}\sqrt{\sum_{\mathbf{i}} \mathbf{Q}_{\mathbf{i}}} - 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}
\end{aligned}$$

On the other hand $P(e(X^n) \neq h(Y^n)) = P(e(X^n) \neq 1 \oplus f(Y^n)) = P(e(X^n) = f(Y^n)) = 1 - P(e(X^n) \neq f(Y^n))$. So,

$$\begin{aligned}
&1 - P(e(X^n) \neq f(Y^n)) \geq 2\sqrt{\sum_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}}\sqrt{\sum_{\mathbf{i}} \mathbf{Q}_{\mathbf{i}}} - 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \\
&\Rightarrow P(e(X^n) \neq f(Y^n)) \leq \\
&1 - 2\sqrt{\sum_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}}\sqrt{\sum_{\mathbf{i}} \mathbf{Q}_{\mathbf{i}}} + 2\sum_{\mathbf{i}} C_{\mathbf{i}} \mathbf{P}_{\mathbf{i}}^{\frac{1}{2}} \mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}}.
\end{aligned}$$

This completes the proof. □

E. Proof of Theorem 2

Proof. The proof of Theorem 2 follows similar steps as the proof of Theorem 1. The only difference is in the proof of step 1.

Step 1: Let $q \triangleq P_X(e(X^n)=1)$, $r \triangleq P_Y(f(Y^n)=1)$. We have:

$$\mathbb{E}_{X^n,Y^n}(\tilde{e}\tilde{f}) \overset{(a)}{=} \mathbb{E}_{X^n,Y^n}\left(\left(\sum_{\mathbf{i}\in\{0,1\}^n}\tilde{e}_{\mathbf{i}}\right)\left(\sum_{\mathbf{k}\in\{0,1\}^n}\tilde{f}_{\mathbf{k}}\right)\right) \overset{(b)}{=} \sum_{\mathbf{i}\in\{0,1\}^n}\sum_{\mathbf{k}\in\{0,1\}^n}\mathbb{E}_{X^n,Y^n}(\tilde{e}_{\mathbf{i}}\tilde{f}_{\mathbf{k}}). \tag{30}$$

In (a) we have used Definition 5, and in (b) we use linearity of expectation. Using the fact that $\tilde{e}_{\mathbf{i}} \in \mathcal{G}_{i_1}\otimes\mathcal{G}_{i_2}\otimes\cdots\otimes\mathcal{G}_{i_n}$ and Lemma 1, we have:

$$\tilde{e}_{\mathbf{i}}(X^n) = \sum_{\forall t\in\tau: l_t\in[1,|\mathcal{X}|-1]} c_{\mathbf{i},(l_t)_{t\in\tau}}\prod_{t\in\tau}\tilde{h}_{l_t}(X_t),$$
$$\tilde{f}_{\mathbf{i}}(Y^n) = \sum_{\forall t\in\tau: l_t\in[1,|\mathcal{Y}|-1]} d_{\mathbf{i},(l_t)_{t\in\tau}}\prod_{t\in\tau}\tilde{g}_{l_t}(Y_t), \tag{31}$$

where $c_{\mathbf{i},(\mathbf{l_t})_{\mathbf{t}\in\tau}} \in \mathbb{R}$, and $\tilde{h}_l(X), l \in \{1,2,\cdots,|\mathcal{X}|-1\}$, and $\tilde{g}_l(Y), l \in \{1,2,\cdots,|\mathcal{Y}|-1\}$ are a basis for $\mathcal{I}_{X,1}$ and $\mathcal{I}_{Y,1}$, respectively. We have:

$$\begin{aligned}\mathbb{E}_{X^n,Y^n}(\tilde{e}_{\mathbf{i}}\tilde{f}_{\mathbf{k}}) &\overset{(a)}{=} \mathbb{E}_{X^n,Y^n}(\tilde{e}_{\mathbf{i}}\tilde{f}_{\mathbf{i}})\mathbb{1}(\mathbf{i}=\mathbf{k})\\ &\overset{(b)}{=} \mathbb{1}(\mathbf{i}=\mathbf{k})\mathbb{E}_{X^n}(\tilde{e}_{\mathbf{i}}\mathbb{E}_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n))\\ &\overset{(c)}{\leq} \mathbb{1}(\mathbf{i}=\mathbf{k})\mathbb{E}^{\frac{1}{2}}_{X^n}(\tilde{e}^2_{\mathbf{i}})\mathbb{E}^{\frac{1}{2}}_{X^n}(\mathbb{E}^2_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n))\\ &= \mathbb{1}(\mathbf{i}=\mathbf{k})\mathbf{P}^{\frac{1}{2}}_{\mathbf{i}}\mathbb{E}^{\frac{1}{2}}_{X^n}(\mathbb{E}^2_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n)),\end{aligned} \tag{32}$$

(a) follows by the same arguments as the ones in step 1 of the proof of Theorem 1, (b) follows from the law of total expectation and the fact that $e_{\mathbf{i}}$ is a function of X^n. In (c) we have used the Cauchy-Schwarz inequality. It only remains to find bounds on $\mathbb{E}_{X^n}(\mathbb{E}^2_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n))$ which are functions of $\mathbf{Q_i}$, ψ, and $N_{\mathbf{i}}$. Let $(i_1,i_2,\cdots,i_{N_{\mathbf{i}}})$ be the indices for which the elements of $\mathbf{i}$ are equal to one. Note that:

$$\begin{aligned}&\mathbb{E}_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n) = \mathbb{E}_{Y_{\mathbf{i}}|X_{\mathbf{i}}}(\tilde{f}_{\mathbf{i}}|X_{\mathbf{i}})\\ &= \mathbb{E}_{Y_{i_{N_{\mathbf{i}}}}|X_{i_{N_{\mathbf{i}}}}}\left(\mathbb{E}_{Y_{\mathbf{i}-\mathbf{i}_{N_{\mathbf{i}}}}|X_{\mathbf{i}-\mathbf{i}_{N_{\mathbf{i}}}}}\left(\tilde{f}_{\mathbf{i}}|X_{\mathbf{i}-\mathbf{i}_{N_{\mathbf{i}}}}\right)|X_{i_{N_{\mathbf{i}}}}\right)\\ &= \mathbb{E}_{Y_{i_{N_{\mathbf{i}}}}|X_{i_{N_{\mathbf{i}}}}}\left(\mathbb{E}_{Y_{i_{N_{\mathbf{i}}-1}}|X_{i_{N_{\mathbf{i}}-1}}}\left(\cdots\left(\mathbb{E}_{Y_{i_1}|X_{i_1}}\left(\tilde{f}_{\mathbf{i}}|X_{i_1}\right)|X_{i_2}\right)\cdots\right)|X_{i_{N_{\mathbf{i}}}}\right),\end{aligned} \tag{33}$$

where the first equality follows from the fact that $f_{\mathbf{i}}$ is a function of $Y_{\mathbf{i}}$. The rest of the equalities follow from the discrete and memoryless properties of the input. For ease of notation define the following projection operators for $1 \leq i \leq n$:

$$\Pi_{X_i}: \mathcal{I}_{Y,i} \to \mathcal{I}_{X,i},\quad h(Y_i) \mapsto \mathbb{E}_{Y_i|X_i}(h(Y_i)).$$

Π_{X_i} can be interpreted as the projector of zero-mean functions of the random variable Y_i onto zero-mean functions of the random variable X_i. We can rewrite Equation (33) as follows:

$$\mathbb{E}_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n) = \Pi_{X_{i_{N_{\mathbf{i}}}}}\circ\Pi_{X_{i_{N_{\mathbf{i}}-1}}}\circ\cdots\circ\Pi_{X_{i_1}}(f_{\mathbf{i}}). \tag{34}$$

We find bounds on $\mathbb{E}_{X^n}(\mathbb{E}^2_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n))$ as follows:

$$\begin{aligned}&\mathbb{E}_{X^n}(\mathbb{E}^2_{Y^n|X^n}(\tilde{f}_{\mathbf{i}}|X^n))\\ &= \mathbb{E}_{X^n}\left(\left(\Pi_{X_{i_{N_{\mathbf{i}}}}}\circ\Pi_{X_{i_{N_{\mathbf{i}}-1}}}\circ\cdots\circ\Pi_{X_{i_1}}(f_{\mathbf{i}})\right)^2\right)\\ &\overset{(a)}{\leq} \mathbf{Q_i}||\Pi_{X_{i_{N_{\mathbf{i}}}}}\circ\Pi_{X_{i_{N_{\mathbf{i}}-1}}}\circ\cdots\circ\Pi_{X_{i_1}}||\\ &\overset{(b)}{=} \mathbf{Q_i}||\Pi_{X_{i_{N_{\mathbf{i}}}}}||\cdot||\Pi_{X_{i_{N_{\mathbf{i}}-1}}}||\cdots||\Pi_{X_{i_1}}||\\ &\overset{(c)}{=} \mathbf{Q_i}||\Pi_{X_1}||^n,\end{aligned} \tag{35}$$

where in (a) the operation norm is defined as $||\Pi|| = \sup_e \mathbb{E}(\Pi^2(e))$ where the supremum is taken over all zero-mean functions e with unit variance. (b) follows from the discrete memoryless property of the inputs. Finally, (c) holds since the source elements are identically distributed. On the other hand, we have:

$$\begin{aligned}\psi &= sup_{h,g\in\mathcal{L}}\mathbb{E}_{X_1,Y_1}(h(X_1)g(Y_1))\\ &= sup_{h,g\in\mathcal{L}}\mathbb{E}_{X_1}(h(X_1)\mathbb{E}_{Y_1|X_1}(g(Y_1)|X_1))\\ &\overset{(a)}{=} sup_{g\in\mathcal{L}}\mathbb{E}^{\frac{1}{2}}_{X_1}(h^2(X_1)\mathbb{E}^{\frac{1}{2}}_{X_1}(\mathbb{E}^2_{Y_1|X_1}(g(Y_1)|X_1))\\ &\overset{(b)}{=} sup_{g\in\mathcal{L}}\mathbb{E}^{\frac{1}{2}}_{X_1}(\mathbb{E}^2_{Y_1|X_1}(g(Y_1)|X_1))\\ &\overset{(c)}{=} ||\Pi_{X_1}||,\end{aligned} \tag{36}$$

where $\mathcal{L}$ is the set of all pairs of functions $g(X)$ and $h(Y)$ with zero mean which have unit variance. (a) follows from the Cauchy-Schwarz inequality and the fact that equality is satisfied by taking $g(X_1) = c\mathbb{E}_{Y_1|X_1}(h(Y_1)|X_1)$ where the constant c is chosen properly, so that $g(X_1)$ has unit variance. The quality (b) holds since $h(X_1)$ has unit variance, and (c) holds by the definition of operator norm. Combining equations (32), (35), (36) we have:

$$\mathbb{E}_{X^n,Y^n}(\tilde{e}_{\mathbf{i}}\tilde{f}_{\mathbf{k}}) \leq \mathbb{1}(\mathbf{i}=\mathbf{k})\psi^{N_{\mathbf{i}}}\mathbf{P}^{\frac{1}{2}}_{\mathbf{i}}\mathbf{Q}^{\frac{1}{2}}_{\mathbf{i}}.$$

The rest of the proof follows by the exact same arguments as in steps 2 and 3 in the proof of Theorem 1. □

F. Proof of Lemma 5

Proof. We provide an outline of the proof that the three properties in Definition 8 are satisfied:

1) As a reminder, the set $B_n(X^n)$ is the set of sequences $\tilde{x}^n$ which may be mapped to the same output sequence u^n as the output of x^n. In this coding scheme $B_n(x^n)$ is as follows:

$$B_n(x^n) = \{\tilde{x}^n | \exists u^n : (x^n,u^n), (\tilde{x}^n,u^n) \in A^n_\epsilon(X,U)\}.$$

Following the notation in [3], let $\mathcal{V}(x^n)$ be the set of all conditional types of sequences $\tilde{x}^n$ given x^n, and let $T_\upsilon(x^n)$ be the set of all sequences $\tilde{x}^n$ which have the conditional type $\upsilon \in \mathcal{V}(x^n)$ with respect to the sequence x^n. Then:

$$|B_n(x^n)| = \sum_{\upsilon\in\mathcal{V}(x^n)}|B(x^n)\bigcap T_\upsilon(x^n)|.$$

Note that $|B(x^n)\bigcap T_\upsilon(x^n)| \neq 0$ if and only if there exists a joint conditional type $\tilde{\upsilon}_{U,\tilde{X}|x^n}$ such that $|\tilde{P}_{U,X} - P_{U,X}| < \epsilon$ and $|\tilde{P}_{U,\tilde{X}} - P_{UX}| < \epsilon$ and $\tilde{P}_{U|X} = \upsilon$, where $\tilde{P}_{U,X,\tilde{X}}$ is the

joint type of the sequences in $\tilde{v}_{U,\tilde{X}|x^n}$ with x^n. As a result we have:

$$|B_n(x^n)| = \sum_{\substack{v\in\mathcal{V}(x^n)\\ \exists \tilde{v}_{U,\tilde{X}|x^n}:\\ |\tilde{P}_{U,X}-P_{U,X}|<\epsilon,|\tilde{P}_{U,\tilde{X}}-P_{UX}|<\epsilon}} |B(x^n)\bigcap T_v(x^n)|.$$

By standard type analysis arguments we conclude that:

$$|B_n(x^n)| \le 2^{\max n(H(\tilde{X}|X)+\delta_n)},$$

where the maximum is taken over all distributions $P_{U,X,\tilde{X}}$ such that $P_{U,X}=P_{U,\tilde{X}}$, and δ_n is a sequence of positive numbers which converges to 0 as $n\to\infty$. Since all of the sequences in $B_n(X^n)$ are typical we have:

$$P(\tilde{X}^n\in B_n(x^n)) \approx \frac{|B_n(x^n)|}{|A_\epsilon^n(x^n)|} \approx 2^{-n(I(\tilde{X};X)-\delta)} \triangleq 2^{-n\delta_X}.$$

Next we show that for $\tilde{x}^n\notin B_n(x^n)$:

$$\begin{aligned}&(1-2^{-n\delta_X})P(\underline{E}(x^n))P(\underline{E}(\tilde{x}^n))\\ &< P(\underline{E}(x^n),\underline{E}(\tilde{x}^n)) < (1+2^{-n\delta_X})P(\underline{E}(x^n))P(\underline{E}(\tilde{x}^n)).\end{aligned} \tag{37}$$

Note that by our construction x^n is mapped to a sequence in $\mathcal{C}\bigcap A_\epsilon^n(U|x^n)$ randomly and uniformly. So:

$$\begin{aligned}&P(\underline{E}(x^n)=c^n|\mathcal{C})\\ &=\frac{\mathbb{1}\left(c^n\in\mathcal{C}\bigcap A_\epsilon^n(U|x^n)\right)}{|\mathcal{C}\bigcap A_\epsilon^n(U|x^n)|}=\frac{\mathbb{1}\left(c^n\in\mathcal{C}\bigcap A_\epsilon^n(U|x^n)\right)}{|\mathcal{C}\bigcap A_\epsilon^n(U|x^n)-\{c^n\}|+1}\\ &\Rightarrow P(\underline{E}(x^n)=c^n)\\ &=P\left(c^n\in\mathcal{C}\cap A_\epsilon^n(U|x^n)\right)\mathbb{E}_{\mathcal{C}}\left(\frac{1}{|\mathcal{C}\bigcap A_\epsilon^n(U|x^n)-\{c^n\}|+1}\right).\end{aligned}$$

By a similar argument for $\tilde{x}^n\notin B_n(x^n)$ we have:

$$\begin{aligned}&P(\underline{E}(x^n)=c^n,\underline{E}(\tilde{x}^n)=\tilde{c}^n)=\\ &P\left(c^n\in\mathcal{C}\cap A_\epsilon^n(U|x^n),\tilde{c}^n\in\mathcal{C}\cap A_\epsilon^n(U|\tilde{x}^n)\right)\times\\ &\mathbb{E}_{\mathcal{C}}\left(\frac{1}{|\mathcal{C}\bigcap A_\epsilon^n(U|x^n)-\{c^n\}|+1}\frac{1}{|\mathcal{C}\bigcap A_{\epsilon^n(U|\tilde{x}^n)}-\{\tilde{c}^n\}|+1}\right).\end{aligned}$$

We show the following bound:

$$\begin{aligned}&P\left(c^n\in\mathcal{C}\cap A_\epsilon^n(U|x^n),\tilde{c}^n\in\mathcal{C}\cap A_\epsilon^n(U|\tilde{x}^n)\right)\\ &\le P\left(c^n\in\mathcal{C}\cap A_\epsilon^n(U|x^n)\right)P\left(\tilde{c}^n\in\mathcal{C}\cap A_\epsilon^n(U|\tilde{x}^n)\right)(1+2^{-n\delta_X}).\end{aligned} \tag{38}$$

Assume that $c^n\in A_\epsilon^n(U|x^n)$, and $\tilde{c}^n\in A_\epsilon^n(U|\tilde{x}^n)$, otherwise the two sides are equal to 0. The following equalities hold by the construction algorithm:

$$\begin{aligned}&P\left(c^n\in\mathcal{C}\cap A_\epsilon^n(U|x^n)\right)=P\left(c^n\in\mathcal{C}\right)=\frac{|\mathcal{C}|}{|A_\epsilon^n(U)|},\\ &P\left(\tilde{c}^n\in\mathcal{C}\cap A_\epsilon^n(U|\tilde{x}^n)\right)=P\left(\tilde{c}^n\in\mathcal{C}\right)=\frac{|\mathcal{C}|}{|A_\epsilon^n(U)|},\\ &P\left(c^n\in\mathcal{C}\cap A_\epsilon^n(U|x^n),\tilde{c}^n\in\mathcal{C}\cap A_\epsilon^n(U|\tilde{x}^n)\right)\\ &=P\left(c^n\in\mathcal{C},\tilde{c}^n\in\mathcal{C}\right)\\ &=\frac{\binom{|\mathcal{C}|}{2}}{\binom{A_\epsilon^n(U)}{2}}.\end{aligned}$$

Using the above it is straightforward to check that the bound in (38) holds. Similarly, it follows that

$$\begin{aligned}&\mathbb{E}_{\mathcal{C}}\left(\frac{1}{|\mathcal{C}\bigcap A_\epsilon^n(U|x^n)-\{c^n\}|+1}\frac{1}{|\mathcal{C}\bigcap A_{\epsilon^n(U|\tilde{x}^n)}-\{\tilde{c}^n\}|+1}\right)\le\\ &\mathbb{E}_{\mathcal{C}}\left(\frac{1}{|\mathcal{C}\bigcap A_\epsilon^n(U|x^n)-\{c^n\}|+1}\right)\times\\ &\mathbb{E}_{\mathcal{C}}\left(\frac{1}{|\mathcal{C}\bigcap A_{\epsilon^n(U|\tilde{x}^n)}-\{\tilde{c}^n\}|+1}\right)(1+2^{-n\delta_X}).\end{aligned}$$

Multiplying the two bound recovers the right-hand side of the inequality in (37). The left-hand side can be shown by similar arguments.

2) As n becomes large, the ith output element $E_i(X^n)$ is correlated with the input sequence X^n only through the ith input element X_i:

$$\begin{aligned}&\forall\delta>0,\exists n\in\mathbb{N}:m>n\Rightarrow\forall x^m\in\{0,1\}^m,v\in\{0,1\},\\ &|P_{\mathcal{S}}(E_i(X^m)=v|X^m=x^m)-P_{\mathcal{S}}(E_i(X^m)=v|X_i=x_i)|<\delta.\end{aligned}$$

The proof is as follows: For a fixed quantization function $\underline{e}:\{0,1\}^m\to\{0,1\}^m$, $\underline{e}(X^m)$ is a function of X^m. However, without the knowledge that which encoding function is used, $E_i(X^m)$ is related to X^m only through X_i. In other words, averaged over all encoding functions, the effects of the rest of the elements diminishes. We provide a proof of this statement below:

First, we are required to provide some definitions relating to the joint type of pairs of sequences. For binary strings u^m,x^m, define $N(a,b|u^m,x^m)\triangleq|\{j|u_j=a,x_j=b\}|$, that is the number of indices j for which the value of the pair (u_j,x_j) is (a,b). For $s,t\in\{0,1\}$, define $l_{s,t}\triangleq N(s,t|u^m,x^m)$, the vector $(l_{0,0},l_{0,1},l_{1,0},l_{1,1})$ is called the joint type of (u^m,x^m). For fixed x^m The set of sequences $T_{l_{0,0},l_{0,1},l_{1,0},l_{1,1}}=\{u^m|N(s,t|u^m,x^m)=l_{s,t},s,t\in\{0,1\}\}$, is the set of vectors which have joint type $(l_{0,0},l_{0,1},l_{1,0},l_{1,1})$ with the sequence x^m. Fix $m,\epsilon>0$, and define $\mathcal{L}_{\epsilon,n}\triangleq\{(l_{0,0},l_{0,1},l_{1,0},l_{1,1}):|\frac{l_{s,t}}{m}-P_{U,X}(s,t)|<\epsilon,\forall s,t\}$. Then for the conditional typical set $A_\epsilon^n(U|x^m)$ defined above we can write

$$A_\epsilon^n(U|x^m)=\bigcup_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}} T_{l_{0,0},l_{0,1},l_{1,0},l_{1,1}}.$$

The type of x^m, denoted by (l_0,l_1) is defined in a similar manner. Since $E_i(X^m)$ are chosen uniformly from the set $A_\epsilon^n(U|x^m)$, we have:

$$\begin{aligned}&P_{\mathcal{S}}(E_i(X^m)=v|X^m=x^m)=\frac{|\{u^m|u_1=v,u^m\in A_\epsilon^m(U|x^m)\}|}{|\{u^m|u^m\in A_\epsilon^m(U|x^m)\}|}\\ &=\frac{\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}}|\{u^m|u_1=v,u^m\in T_{l_{0,0},l_{0,1},l_{1,0},l_{1,1}}\}|}{\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}}|\{u^m|u^m\in T_{l_{0,0},l_{0,1},l_{1,0},l_{1,1}}\}|}\\ &=\frac{\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}}\binom{l_{x_1}-1}{l_{u_1,x_1}-1}\binom{l_{\tilde{x}_1}}{l_{u_1,\tilde{x}_1}}}{\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}}\binom{l_{x_1}}{l_{u_1,x_1}}\binom{l_{\tilde{x}_1}}{l_{u_1,\tilde{x}_1}}}\\ &=\frac{\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}}\frac{(l_{x_1}-1)!}{(l_{u_1,x_1}-1)!(l_{x_1}-l_{u_1,x_1})!}\frac{l_{\tilde{x}_1}!}{l_{u_1,\tilde{x}_1}!(l_{\tilde{x}_1}-l_{u_1,\tilde{x}_1})!}}{\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}}\frac{l_{x_1}!}{l_{u_1,x_1}!(l_{x_1}-l_{u_1,x_1})!}\frac{l_{\tilde{x}_1}!}{l_{u_1,\tilde{x}_1}!(l_{\tilde{x}_1}-l_{u_1,\tilde{x}_1})!}}\end{aligned}$$

$$\overset{(a)}{=} \frac{\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}} l_{u_1,x_1} \frac{1}{l_{u_1,x_1}!(l_{x_1}-l_{u_1,x_1})!} \frac{1}{l_{u_1,\bar{x}_1}!(l_{\bar{x}_1}-l_{u_1,\bar{x}_1})!}}{l_{x_1}\sum_{(l_{0,0},l_{0,1},l_{1,0},l_{1,1})\in\mathcal{L}_{\epsilon,n}} \frac{1}{l_{u_1,x_1}!(l_{x_1}-l_{u_1,x_1})!} \frac{1}{l_{u_1,\bar{x}_1}!(l_{\bar{x}_1}-l_{u_1,\bar{x}_1})!}}$$

$$\overset{(b)}{\Rightarrow} \frac{P_{U,X}(u_1,x_1)-\epsilon}{P_X(x_1)+\epsilon} \le P_{\mathbb{S}}(E_i(X^m)=v|X^m=x^m) \le \frac{P_{U,X}(u_1,x_1)+\epsilon}{P_X(x_1)-\epsilon}$$

$$\Rightarrow \exists m,\epsilon>0 : |P_{\mathbb{S}}(E_i(X^m)=v|X^m=x^m)-P_{U|X}(u_1|x_1)| \le \delta.$$

In (a), we use the fact that for fixed x^m, $(l_{x_1}, l_{\bar{x}_1})$ is fixed to simplify the numerators. In (b) we have used that for jointly typical ϵ-sequences (u^m, x^m), $l_{u_1,x_1} \in [n(P_{U,X}(u_1,x_1)-\epsilon), n(P_{U,X}(u_1,x_1)+\epsilon)]$, and $l_{x_1} \in [n(P_X(x_1)-\epsilon), n(P_X(x_1)+\epsilon)]$.

3) The encoder is insensitive to permutations. Due to typicality encoding the probability that a vector x^n is mapped to y^n depends only on their joint type and is equal to the probability that $\pi(x^n)$ is mapped to $\pi(y^n)$. □

G. Proof of Proposition 4

Proof.

Fix $k, k' \in \mathbb{N}$. Define the permutation $\pi_{k\to k'} \in S_n$ as the permutation which switches the kth and k'th elements and fixes all other elements. Also, let $\mathcal{E}$ be the set of all mappings $e : \{0,1\}^n \to \{0,1\}^n$.

$$P_{\mathbb{S}}\left(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_k} \mathbf{P}_{k,\mathbf{i}} > \gamma\right) = \sum_{\underline{e}\in\mathcal{E}} P_{\mathbb{S}}\left(\underline{e}\right) \mathbb{1}\left(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_k|\underline{e}} \mathbf{P}_{k,\mathbf{i}} > \gamma\right)$$

$$\overset{(a)}{=} \sum_{\underline{e}\in\mathcal{E}} P_{\mathbb{S}}\left(\underline{e}_{\pi_{k\to k'}}\right) \mathbb{1}\left(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_k} \mathbf{P}_{k,\mathbf{i}} > \gamma\,|\underline{e}\right)$$

$$\overset{(b)}{=} \sum_{\underline{g}\in\mathcal{E}} P_{\mathbb{S}}\left(\underline{g}\right) \mathbb{1}\left(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_k} \mathbf{P}_{\pi_{k\to k'}k,\pi_{k\to k'}\mathbf{i}} > \gamma\,|\underline{g}\right)$$

$$= \sum_{\underline{g}\in\mathcal{E}} P_{\mathbb{S}}\left(\underline{g}\right) \mathbb{1}\left(\sum_{\underline{l}:N_{\underline{l}}\le m,\underline{l}\neq\pi_{k\to k'}\mathbf{i}_k} \mathbf{P}_{k',\underline{l}} > \gamma\,|\underline{g}\right)$$

$$= P_{\mathbb{S}}\left(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_{k'}} \mathbf{P}_{k',\mathbf{i}} > \gamma\right),$$

where in (a) we have used property 3) in Definition 8, and in (b) we have defined $\underline{g} \triangleq \underline{e}_{\pi_{k\to k'}}$ and used $\pi^2_{k\to k'} = 1$. □

H. Proof of Theorem 3

Proof.

From Proposition 4, it is enough to show the theorem holds for $k = 1$. For ease of notation we drop the subscript k for the rest of the proof and denote $\mathbf{P}_{1,\mathbf{i}}$ by $\mathbf{P}_{\mathbf{i}}$. By the Markov inequality, we have the following:

$$P_{\mathbb{S}}(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_1} \mathbf{P}_{\mathbf{i}} \ge \gamma) \le \frac{\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_1} \mathbb{E}_{\mathbb{S}}(\mathbf{P}_{\mathbf{i}})}{\gamma}. \tag{39}$$

So, we need to show that $\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_1} \mathbb{E}_{\mathbb{S}}(\mathbf{P}_{\mathbf{i}})$ goes to 0 for all fixed m. We first prove the following claim.

Claim 1. *Fix* $\mathbf{i}$*, the following holds*:

$$\mathbb{E}_{\tilde{E},X_{\mathbf{i}}}(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{E}|X_{\mathbf{i}})) = \mathbb{E}_{X_{\mathbf{i}}}(\mathbb{E}^2_{\tilde{E},X^n|X_{\mathbf{i}}}(\tilde{E}|X_{\mathbf{i}})) + O(e^{-n\delta_X}).$$

Proof.

$$\mathbb{E}_{\tilde{E},X_{\mathbf{i}}}(\mathbb{E}^2_{X^n|X_{\mathbf{i}}}(\tilde{E}|X_{\mathbf{i}})) = \sum_{x_{\mathbf{i}},\tilde{e}} P(x_{\mathbf{i}})P(\tilde{e})(\sum_{x_{\sim\mathbf{i}}} P(x_{\sim\mathbf{i}})\tilde{e}(x^n))^2$$

$$= \sum_{x_{\mathbf{i}},\tilde{e}} P(x_{\mathbf{i}})P(\tilde{e}) \sum_{x_{\sim\mathbf{i}}} \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}}} P(x_{\sim\mathbf{i}})P(y_{\sim\mathbf{i}})\tilde{e}(x^n)\tilde{e}(y^n)$$

$$= \sum_{x^n} P(x^n) \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}}} P(y_{\sim\mathbf{i}})\mathbb{E}_{\tilde{E}}(\tilde{E}(x^n)\tilde{E}(y^n))$$

$$= \sum_{x^n} P(x^n) \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}},y^n\in B_n(x^n)} P(y_{\sim\mathbf{i}})\mathbb{E}_{\tilde{E}}(\tilde{E}(x^n)\tilde{E}(y^n))$$

$$+ \sum_{x^n} P(x^n) \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}},y^n\notin B_n(x^n)} P(y_{\sim\mathbf{i}})\mathbb{E}_{\tilde{E}}(\tilde{E}(x^n)\tilde{E}(y^n))$$

$$\overset{(a)}{\le} \sum_{x^n} P(x^n) \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}},y^n\in B_n(x^n)} P(y_{\sim\mathbf{i}})$$

$$+ \sum_{x^n} P(x^n) \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}},y^n\notin B_n(x^n)} P(y_{\sim\mathbf{i}})\mathbb{E}_{\tilde{E}}(\tilde{E}(x^n)\tilde{E}(y^n))$$

$$= P(Y^n \in B_n(X^n)|Y_{\mathbf{i}} = X_{\mathbf{i}})$$

$$+ \sum_{x^n} P(x^n) \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}},y^n\notin B_n(x^n)} P(y_{\sim\mathbf{i}})\mathbb{E}_{\tilde{E}}(\tilde{E}(x^n)\tilde{E}(y^n))$$

$$\overset{(b)}{=} O(e^{-n\delta_X}) +$$

$$\sum_{x^n} P(x^n) \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}},y^n\notin B_n(x^n)} P(y_{\sim\mathbf{i}})\mathbb{E}_{\tilde{E}}(\tilde{E}(x^n))\mathbb{E}_{\tilde{E}}(\tilde{E}(y^n))$$

$$\le O(e^{-n\delta_X}) + P(Y^n \in B_n(X^n)|Y_{\mathbf{i}} = X_{\mathbf{i}})$$

$$+ \sum_{x_{\mathbf{i}}} P(x_{\mathbf{i}}) \sum_{x_{\sim\mathbf{i}}} \sum_{y^n:y_{\mathbf{i}}=x_{\mathbf{i}}} P(x_{\sim\mathbf{i}})P(y_{\sim\mathbf{i}})\mathbb{E}_{\tilde{E}}(\tilde{E}(x^n))\mathbb{E}_{\tilde{E}}(\tilde{E}(y^n))$$

$$= O(e^{-n\delta_X}) + \mathbb{E}_{X_{\mathbf{i}}}(\mathbb{E}^2_{\tilde{E},X^n|X_{\mathbf{i}}}(\tilde{E}|X_{\mathbf{i}})).$$

In (a) we use the fact that $\tilde{E} \le 1$ by definition, in (b) follows from property 1) in Definition 8. □

Define $\bar{E}_{\mathbf{i}} = \mathbb{E}_{\tilde{E}}(\tilde{E}_{\mathbf{i}}) = \mathbb{E}_{\tilde{E}|X_{\mathbf{i}}}(\tilde{E}|X_{\mathbf{i}}) - \sum_{\mathbf{j}<\mathbf{i}} \bar{E}_{\mathbf{j}}$, and also define $\bar{P}_{\mathbf{i}} \triangleq Var(\bar{E}_{\mathbf{i}})$. Using the above claim we have:

$$P_{\mathbb{S}}(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_1} \mathbf{P}_{\mathbf{i}} \ge \gamma) \le \frac{\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_1} \mathbb{E}_{\mathbb{S}}(\mathbf{P}_{\mathbf{i}})}{\gamma}$$

$$\le \frac{2^m O(e^{-n\delta_X}) + \sum_{\mathbf{i}:N_{\mathbf{i}}\le m} \mathbb{E}_{\mathbb{S}}(\bar{P}_{\mathbf{i}}) - \mathbb{E}_{\mathbb{S}}(\bar{P}_{\mathbf{i}_1})}{\gamma}. \tag{40}$$

Using the arguments from the proof of Lemma 3, we can see that the properties stated in that Proposition hold for $\bar{E}_{\mathbf{i}}$ as well. By the same results as in Lemma 3 and Corollary 1, we have that $\sum_{\mathbf{i}\in\{0,1\}^n} \bar{P}_{\mathbf{i}} = \bar{P}_{\underline{1}}$. Following the calculations in (40):

$$P_{\mathbb{S}}(\sum_{\mathbf{i}:N_{\mathbf{i}}\le m,\mathbf{i}\neq\mathbf{i}_1} \mathbf{P}_{\mathbf{i}} \ge \gamma)$$

$$\le \frac{2^m O(e^{-n\delta_X}) + \sum_{\mathbf{i}:N_{\mathbf{i}}\le m} \mathbb{E}_{\mathbb{S}}(\bar{P}_{\mathbf{i}}) - \mathbb{E}_{\mathbb{S}}(\bar{P}_{\mathbf{i}_1})}{\gamma}$$

$$\le \frac{2^m O(e^{-n\delta_X}) + \sum_{\mathbf{i}\in\{0,1\}^n} \mathbb{E}_{\mathbb{S}}(\bar{P}_{\mathbf{i}}) - \mathbb{E}_{\mathbb{S}}(\bar{P}_{\mathbf{i}_1})}{\gamma}$$

$$
\begin{aligned}
&= \frac{2^m O(e^{-n\delta_X}) + \mathbb{E}_{\mathcal{S}}(\sum_{\mathbf{i}\in\{0,1\}^n} \bar{P}_{\mathbf{i}}) - \mathbb{E}_{\mathcal{S}}(\bar{P}_{\mathbf{i}_1})}{\gamma} \\
&= \frac{2^m O(e^{-n\delta_X}) + \mathbb{E}_{X^n}\left(\mathbb{E}^2_{\tilde{E}|X^n}(\tilde{E}(X^n)|X^n)\right) - \mathbb{E}_{\mathcal{S}}(\bar{P}_{\mathbf{i}_1})}{\gamma} \\
&\leq \frac{2^m O(e^{-n\delta_X}) + \mathbb{E}_{\mathcal{S}}(\bar{P}_{\mathbf{i}_1}) + O(\epsilon) - \mathbb{E}_{\mathcal{S}}(\bar{P}_{\mathbf{i}_1})}{\gamma} \\
&= \frac{2^m O(e^{-n\delta_X}) + O(\epsilon)}{\gamma},
\end{aligned}
$$

where in the last inequality we have used the second property in Definition 8. The last line goes to 0 as $n \to \infty$. This completes the proof. □

I. Proof of Theorem 4

Proof. From Theorem 1, we have:

$$\mathbf{P}^{\frac{1}{2}}\mathbf{Q}^{\frac{1}{2}} - 2\sum_{\mathbf{i}} C_{\mathbf{i}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} \leq P(E(X^n) \neq F(Y^n)).$$

From Theorem 3 we have:

$$
\begin{aligned}
&\forall m \in \mathbb{N}, \gamma > 0, P_{\mathcal{S}}\Big(\sum_{\mathbf{i}:N_{\mathbf{i}}\leq m, \mathbf{i}\neq\mathbf{i}_1} \mathbf{P}_{\mathbf{i}} < \gamma\Big) \to 1, \\
&P_{\mathcal{S}}\Big(\sum_{\mathbf{i}:N_{\mathbf{i}}\leq m, \mathbf{i}\neq\mathbf{i}_1} \mathbf{Q}_{\mathbf{i}} < \gamma\Big) \to 1. \qquad (41)
\end{aligned}
$$

Note that:

$$
\begin{aligned}
&\sum_{\mathbf{i}:N_{\mathbf{i}}\leq m, \mathbf{i}\neq\mathbf{i}_1} \mathbf{P}_{\mathbf{i}} < \gamma, \sum_{\mathbf{i}:N_{\mathbf{i}}\leq m, \mathbf{i}\neq\mathbf{i}_1} \mathbf{Q}_{\mathbf{i}} < \gamma \Rightarrow \\
&\sum_{\mathbf{i}} C_{\mathbf{i}}\mathbf{P}_{\mathbf{i}}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}}^{\frac{1}{2}} > (1-2\epsilon)(\mathbf{P}_{\mathbf{i}_1} + \gamma)^{\frac{1}{2}}(\mathbf{Q}_{\mathbf{i}_1} + \gamma)^{\frac{1}{2}} \\
&+ (1-2\epsilon)^m \mathbf{P}^{\frac{1}{2}}\mathbf{Q}^{\frac{1}{2}}, \qquad (42)
\end{aligned}
$$

which converges to $(1-2\epsilon)\mathbf{P}_{\mathbf{i}_1}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}_1}^{\frac{1}{2}} + (1-2\epsilon)^m\mathbf{P}^{\frac{1}{2}}\mathbf{Q}^{\frac{1}{2}}$ as $\gamma \to 0$. Also $C_{\mathbf{i}}$ is decreasing in $N_{\mathbf{i}}$ and goes to 0 as $N_{\mathbf{i}} \to \infty$. Choose γ small enough and m large enough such that $(1-2\epsilon)(\mathbf{P}_{\mathbf{i}_1} + \gamma)^{\frac{1}{2}}(\mathbf{Q}_{\mathbf{i}_1} + \gamma)^{\frac{1}{2}} + (1-2\epsilon)^m\mathbf{P}^{\frac{1}{2}}\mathbf{Q}^{\frac{1}{2}} - (1-2\epsilon)\mathbf{P}_{\mathbf{i}_1}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}_1}^{\frac{1}{2}} < \delta$. Then Equations (41) and (42) gives

$$P_{\mathcal{S}}\left(P_{X^n,Y^n}\left(E(X^n) \neq F(Y^n)\right) < \zeta\right) \to 0,$$

where $\zeta = 2\mathbf{P}^{\frac{1}{2}}\mathbf{Q}^{\frac{1}{2}} - 2(1-2\epsilon)\mathbf{P}_{\mathbf{i}_1}^{\frac{1}{2}}\mathbf{Q}_{\mathbf{i}_1}^{\frac{1}{2}} - \delta$. This is equivalent to the statement of the theorem. □

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the associate editor for their comments which led to significant improvements in the manuscript.

REFERENCES

[1] H. S. Witsenhausen, "On sequences of pairs of dependent random variables," *SIAM J. Appl. Math.*, vol. 28, no. 1, pp. 100–113, 1975.

[2] A. El Gamal and Y. H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[3] I. Csiszár and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York, NY, USA: Academic, 1981.

[4] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications* (Applications of Mathematics). New York, NY, USA: Springer, 1998.

[5] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 4, pp. 471–480, Jul. 1973.

[6] T. M. Cover, A. El Gamal, and M. Salehi, "Multiple access channels with arbitrarily correlated sources," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 6, pp. 648–657, Nov. 1980.

[7] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 3, pp. 306–311, May 1979.

[8] P. Gács and J. Körner, "Common information is far less than mutual information," *Problems Control Inf. Theory*, vol. 2, no. 2, pp. 119–162, 1972.

[9] H. O. Hirschfeld, "A connection between correlation and contingency," *Math. Proc. Cambridge Philos. Soc.*, vol. 31, no. 4, pp. 520–524, 1935.

[10] A. Rényi, "New version of the probabilistic generalization of the large sieve," *Acta Math. Acad. Sci. Hungarica*, vol. 10, nos. 1–2, pp. 217–226, 1959.

[11] A. B. Wagner, B. G. Kelly, and Y. G. Altug, "Distributed rate-distortion with common components," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4035–4057, Jul. 2011.

[12] F. S. Chaharsooghi, A. G. Sahebi, and S. S. Pradhan, "Distributed source coding in absence of common components," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 1362–1366.

[13] A. Bogdanov and E. Mossel, "On extracting common random bits from correlated sources," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6351–6355, Oct. 2011.

[14] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[15] A. Mahajan, A. Nayyar, and D. Teneketzis, "Identifying tractable decentralized control problems on the basis of information structure," in *Proc. 46th Annu. Allerton Conf. Commun. Control Comput.*, Sep. 2008, pp. 1440–1449.

[16] G. Pichler, P. Piantanida, and G. Matz, "Dictator functions maximize mutual information," 2016, *arXiv:1604.02109*. [Online]. Available: https://arxiv.org/abs/1604.02109

[17] Y. Geng, A. Gohari, C. Nair, and Y. Yu, "On Marton's inner bound and its optimality for classes of product broadcast channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 22–41, Jan. 2014.

[18] J. Chen and T. Berger, "Robust distributed source coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3385–3398, Aug. 2008.

[19] F. Shirani and S. S. Pradhan, "Finite block-length gains in distributed source coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2014, pp. 1702–1706.

[20] R. O'Donnell, *Analysis of Boolean Functions*. Cambridge, U.K.: Cambridge Univ. Press, 2014.

[21] B. Ghazi, P. Kamath, and M. Sudan, "Decidability of non-interactive simulation of joint distributions," in *Proc. IEEE 57th Annu. Symp. Found. Comput. Sci. (FOCS)*, Oct. 2016, pp. 545–554.

[22] M. Reed and B. Simon, *Methods of Modern Mathematical Physics I: Functional Analysis*. New York, NY, USA: Academic, 1972.

[23] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, vol. 9. New York, NY, USA: Dover, 1972.

[24] W. Kang and S. Ulukus, "A new data processing inequality and its applications in distributed source and channel coding," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 56–69, Jan. 2011.

[25] S. Y. Tung, "Multiterminal source coding," Ph.D. dissertation, School Elect. Eng., Cornell Univ., Ithaca, NY, USA, 1978.

[26] Z. Zhang and T. Berger, "New results in binary multiple descriptions," *IEEE Trans. Inf. Theory*, vol. IT-33, no. 4, pp. 502–521, Jul. 1987.

[27] M. Salehi and E. Kurtas, "Interference channels with correlated sources," in *Proc. IEEE Int. Symp. Inf. Theory*, Jan. 1993, p. 208.

[28] S. S. Pradhan, "Approximation of test channels in source coding," in *Proc. Conf. Inf. Syst. Sci. (CISS)*, 2004.

[29] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, Jul. 1948.

[30] V. Kostina and S. Verdú, "Lossy joint source-channel coding in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2545–2575, May 2013.

[31] T. F. N. Baader, *Term Rewriting and All That*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[32] Y. Huang, J. Benesty, J. Chen, and I. Cohen, *Noise Reduction in Speech Processing*. New York, NY, USA: Springer, 2009.

[33] S. Kamath and V. Anantharam, "On non-interactive simulation of joint distributions," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3419–3435, Jun. 2016.

A General Framework for Temporal Fair User Scheduling in NOMA Systems

Shahram Shahsavari, Farhad Shirani, and Elza Erkip

***Abstract*—Non-orthogonal multiple access (NOMA) is one of the promising radio access techniques for next generation wireless networks. Opportunistic multi-user scheduling is necessary to fully exploit multiplexing gains in NOMA systems, but compared with traditional scheduling, inter-relations between users' throughputs induced by multi-user interference poses new challenges in the design of NOMA schedulers. A successful NOMA scheduler has to carefully balance the following three objectives: Maximizing average system utility, satisfying desired fairness constraints among the users and enabling real time, and low computational cost implementations. In this paper, scheduling for NOMA systems under temporal fairness constraints is considered. Temporal fair scheduling leads to communication systems with predictable latency as opposed to utilitarian fair schedulers for which latency can be highly variable. It is shown that under temporal fairness constraints, optimal system utility is achieved using a class of opportunistic scheduling schemes called *threshold based strategies* (TBS). One of the challenges in heterogeneous NOMA scenarios—where only specific users may be activated simultaneously—is to determine the set of feasible temporal shares. A variable elimination algorithm is proposed to accomplish this task. Furthermore, an (online) iterative algorithm based on the Robbins–Monro method is proposed to construct a TBS by finding the optimal thresholds for a given system utility metric. The algorithm does not require knowledge of the users' channel statistics. Rather, at each time slot, it has access to the channel realizations in the previous time slots. Various numerical simulations of practical scenarios are provided to illustrate the effectiveness of the proposed NOMA scheduling in static and mobile scenarios.**

***Index Terms*—Non-orthogonal multiple access, multi-user scheduling, temporal fairness, threshold-based strategies, Robbins-Monro algorithm.**

I. Introduction

NON-orthogonal multiple access (NOMA) has emerged as one of the key enabling technologies for fifth generation wireless networks [1]–[4]. In order to satisfy the ever-growing demand for higher data rates in modern cellular systems, NOMA proposes serving multiple users in the same resource block. This is in contrast with conventional cellular systems which operate based on orthogonal multiple access (OMA) techniques such as orthogonal frequency-division multiple access (OFDMA) [5]. In OMA systems, each time-frequency resource block is assigned to only one user in each cell, whereas, in NOMA systems, multiple users can be scheduled either in uplink (UL) or in downlink (DL) simultaneously [6]. As a result, the scheduler in the NOMA system may choose among a larger collection of users at each resource block as compared to an OMA one, often leading to a higher system throughput [7]. The high system throughput is due to NOMA multiplexing gains, achieved through a combination of superposition encoding strategies at the transmitter(s) and successive interference cancellation (SIC) decoding at the receiver(s) [7]–[9]. However, the inter-relations between users' throughputs induced by multi-user interference complicate the design of high-performance schedulers, giving rise to new challenges both in terms of designing user power allocation schemes [10]–[12] as well as optimal schedulers [2], [13]. Ideally, the scheduler is designed in tandem with the encoding and decoding strategies and power optimization techniques. However, due to the complexity of the problem, scheduling is usually studied in isolation assuming that the system throughputs are given to the scheduler based on a predetermined communication strategy [2], [14].

The objective of a NOMA scheduler is to maximize the system utility (e.g. system throughput) subject to the users' individual demand constraints, e.g. temporal demands or minimum utility demands. More precisely, at each resource block, the scheduler estimates the set of resulting system utilities from activating any specific subset of UL or DL users. It then chooses the set of active users in that block based on this information and users' individual fairness demands. Quantifying fairness in user scheduling has been a topic of significant interest. Various criteria on the users' quality of service (QoS) have been proposed to model and evaluate fairness of scheduling strategies. For OMA systems, scheduling under utilitarian [15], [16], proportional [17], [18], and temporal [19], [20] fairness criteria have been studied.

In delay sensitive applications, a system with reasonable and predictable latency may be more desirable than a system with highly variable latency, but potentially higher throughput. In such scenarios, temporally fair schedulers are often favored over utilitarian fair schedulers. Temporally fair schedulers provide each user with a minimum temporal share in order to control the average delay [21]. Furthermore, most of the power consumption in cellular devices is due to the radio electronics which are activated during data transmission and reception. Consequently, the maximum power drain of users can be restricted by considering upper-bounds on the users' temporal shares [20]. From

Manuscript received September 14, 2018; revised January 11, 2019 and February 22, 2019; accepted February 24, 2019. Date of publication March 7, 2019; date of current version May 22, 2019. This work was supported in part by the NYU WIRELESS Industrial Affiliates and in part by the National Science Foundation Grants EARS-1547332 and NeTS-1527750. The guest editor coordinating the review of this paper and approving it for publication was Dr. Zhiguo Ding. *(Corresponding author: Farhad Shirani.)*

The authors are with the Department of Electrical and Computer Engineering, New York University Tandon School of Engineering, New York, NY 10012 USA (e-mail: shahram.shahsavari@nyu.edu; fsc265@nyu.edu; elza@nyu.edu).

Digital Object Identifier 10.1109/JSTSP.2019.2903745

1932-4553 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

the perspective of the network provider, an additional upside of temporally fair schedulers is that users with low channel quality do not hinder network throughput as severely as in utilitarian fair schedulers [22]. There has been a significant body of work dedicated to the study of temporally fair schedulers in wireless local area networks [23], [24] and OMA cellular systems [20], [25], [26]. However, temporal fairness of NOMA schedulers, which is the topic of this paper, has not been investigated before.

In OMA systems, optimal utility subject to temporal demand constraints is achieved using a class of opportunistic scheduling strategies called *threshold based strategies* (TBS) [19]. An opportunistic scheduler exploits the time-varying nature of the users' wireless channels. In TBSs, at each resource block, the active user u_i is chosen based on the sum of two components: i) Performance value R_i (typically transmission rate), and ii) a constant term called the *user threshold* λ_i. The user thresholds are chosen to optimize the tradeoff between system utility and users' temporal share demands. The thresholds can be interpreted as the Lagrangian multipliers corresponding to the fairness constraints in the optimization of the system utility. In [19], a method based on the Robbins-Monro algorithm is proposed to construct optimal temporally fair TBSs for OMA systems.

In this work, we consider the user scheduling problem for NOMA systems under temporal fairness constraints. We provide a mathematical formulation of the problem which is applicable under general utility models and assumptions on the subsets of users which can be activated simultaneously. Our model is applicable to both UL and DL scenarios.

We first address the question of feasibility of a set of temporal demands in a given NOMA system. A vector of temporal shares is said to be *feasible* if there exists a scheduling strategy for which the resulting user temporal shares are equal to the elements of the vector. In OMA systems, since exactly one user is active at each block, a vector of temporal shares is feasible as long as its elements sum to less than or equal to one. However, in NOMA systems the set of feasible temporal shares is not trivially known. Determining the feasible set is especially challenging in large heterogeneous NOMA systems, where only specific users may be activated simultaneously. In Section IV-A, we propose a variable elimination method to derive the set of feasible temporal shares in arbitrary heterogeneous NOMA scenarios. Furthermore, we prove that given a feasible set of temporal demands, TBSs are optimal for NOMA systems. We further prove that any optimal scheduling strategy can be written in the form of a TBS.

The question of existence and construction of optimal NOMA TBSs is more challenging than OMA TBSs. The reason is that a NOMA TBS assigns a threshold to each subset of users which can be activated simultaneously, rather than each user separately. Therefore, in an optimal TBS the thresholds assigned to the subsets of users are inter-related. In Section V, we propose a construction method based on the Robbins-Monro algorithm to find the optimal thresholds for a NOMA TBS. The algorithm does not require knowledge of the users' channel statistics. Rather, at each time-slot, it has access to the channel realizations in the previous time-slots and updates the scheduler thresholds iteratively to construct the optimal TBS. In Section VI, we consider practical NOMA systems where discrete modulation and coding strategies are used. In this case, the resulting system utilities are staircase functions of the users' signal to noise ratios. As a result, the utility from activating different subsets of users may lead to a tie in the TBS decision. This necessitates the design and optimization of a tie-breaking decision rule [19]. We propose a perturbation technique which circumvents the optimization and leads to TBSs whose average system utility is arbitrarily close to the optimal utility. In Section VII, we provide simulations and numerical examples in several practical scenarios involving static and mobile settings. We observe that the proposed scheduling algorithm adapts to the changes due to user mobility under typical velocity assumptions.

II. Notation

We represent random variables by capital letters such as X, U. Sets are denoted by calligraphic letters such as $\mathcal{X}, \mathcal{U}$. The set of natural numbers, and the real numbers are shown by $\mathbb{N}$, and $\mathbb{R}$ respectively. The set of numbers $\{1, 2, \ldots, n\}, n \in \mathbb{N}$ is represented by $[n]$. The closed interval $\{x : a \leq x \leq b\}$ is shown by $[a, b]$. The notation $[a, b]^n$ is used to denote the n-fold Cartesian product of the closed interval $[a, b]$ with itself. The vector $(x_1, x_2, \ldots, x_n)$ is written as x^n. The $m \times t$ matrix $[g_{i,j}]_{i\in[m],j\in[t]}$ is denoted by $g^{m\times t}$. For a random variable X, the corresponding probability space is $(\mathcal{X}, \mathbf{F}_X, P_X)$, where $\mathbf{F}_X$ is the underlying σ-field. The set of all subsets of $\mathcal{X}$ is written as $2^{\mathcal{X}}$. For an event $\mathcal{A} \in 2^{\mathcal{X}}$, the random variable $\mathbb{1}_{\mathcal{A}}$ is the indicator function of the event. We write $X \sim Unif[a, b]$ for a random variable X uniformly distributed on the interval $[a, b]$. Families of sets are shown using sans-serif letters (e.g. $\mathsf{X} = 2^{\mathcal{X}}$). Finally, $mod_k(i), i, k \in \mathbb{N}$ represents the value of i modulo k.

III. System Model

In this section, we describe the system model and formulate NOMA multi-user scheduling under temporal fairness constraints. We consider a single-cell time-slotted system with n users distributed within the cell. We define the user set as $\mathcal{U} = \{u_1, u_2, \ldots, u_n\}$ where $u_i, i \in [n]$ denotes the ith user. At each time-slot, a subset of UL or DL users are activated simultaneously by the base station using NOMA. The maximum number of active users at each time-slot is bounded from above due to practical considerations such as latency and computational complexity at the scheduler and decoder. For example, the decoding complexity, communication delay under SIC, and the scheduler's computational complexity are proportional to the number of multiplexed users [1]. Consequently, only subsets of users with at most $N_{\max} \leq n$ elements can be activated simultaneously, where $N_{\max}$ is determined based on the communication setup under consideration. Several works on NOMA scheduling consider $N_{\max} = 2$ and $N_{\max} = 3$ under various utilitarian and proportional fairness constraints [27], [28]. A subset of users which can be activated simultaneously is called a *virtual user*.

Definition 1 (Virtual User): For a NOMA system with n users and maximum number of active users $N_{\max} \leq n$, the set

of virtual users is defined as

$$\mathsf{V} = \left\{\mathcal{V}_j | j \in [m]\right\} = \left\{\mathcal{V}_j \subset \mathcal{U} | |\mathcal{V}_j| \leq N_{\max}\right\}.$$

The set $\mathcal{V}_j, j \in [m]$ is called the jth virtual user. The total number of virtual users in a NOMA system is equal to $m = \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{N_{\max}}$.

Our objective is to design a scheduler which maximizes the average network utility subject to temporal fairness constraints. At the beginning of each time-slot, the scheduler finds the utility due to activating each of the virtual users, and decides which virtual user to activate in that time-slot. The utility is usually defined as a function of the throughput of the elements of the virtual user.

Definition 2 (Performance Vector): The vector of jointly continuous variables $(R_{1,t}, R_{2,t}, \ldots, R_{m,t}), t \in \mathbb{N}$ is the performance vector of the virtual users at time t. The sequence $(R_{1,t}, R_{2,t}, \ldots, R_{m,t}), t \in \mathbb{N}$ is a sequence of independent[1] vectors distributed identically according to the joint density f_{R^m}.

Remark 1: It is assumed that the performance vector is bounded with probability one. Alternatively, we assume that $P(R^m \in [-M, M]^m) = 1$ for large enough $M \in \mathbb{R}_{\geq 0}$.

Remark 2: For the virtual user $\mathcal{V}_j = \{u_{i_1}, u_{i_2}, \ldots, u_{i_{k_j}}\}$, $j \in [m], k_j \in [n], i_1, i_2, \ldots, i_{k_j} \in [n]$, we sometimes write $\mathcal{V}_{i_1,i_2,\ldots,i_{k_j}}$ $(R_{i_1,i_2,\ldots,i_{k_j}})$ instead of $\mathcal{V}_j$ (R_j) to represent the virtual user (performance variable).

The following example clarifies the notion of performance vector and provides a characterization for $(R_{1,t}, R_{2,t}, \ldots, R_{m,t}), t \in \mathbb{N}$ in a large class of practical applications.

NOMA Downlink Scenario: In this example, we explicitly characterize the performance vector of a NOMA downlink system at any time-slot, where the system utility is defined to be the transmission sum-rate. The characterization can also be used for NOMA uplink scenarios with minor modifications (e.g. [29]). Let $h_{i,t}$ be the propagation channel coefficient between user u_i and the BS which captures small-scale and large-scale fading effects [30]. It is assumed that the channel coefficients $h_{i,t}, i \in [n]$ are independent over time. Let $R_{j,t}, j \in [m], t \in \mathbb{N}$ be the sum-rate of the elements of virtual user $\mathcal{V}_j$ given that it is activated at time t. In NOMA downlink, a combination of superposition coding at the BS and SIC decoding at the mobile user has been proposed [31]. As envisioned for practical NOMA downlink systems, the decoding occurs in the order of increasing channel gains [7]. For a fixed virtual user $\mathcal{V}_j, j \in [m]$ and user $u_i \in \mathcal{V}_j$, let $\mathcal{I}^i_{j,t}$ be the set of elements of $\mathcal{V}_j$ whose channels are stronger than that of u_i at time t. Alternatively, define $\mathcal{I}^i_{j,t} = \{u_l \in \mathcal{V}_j | |h_{l,t}| > |h_{i,t}|\}$. If $\mathcal{V}_j$ is activated at time t, user u_i applies SIC to cancel the interference from users in $\mathcal{V}_j$ whose channel gain is lower than that of u_i, hence only the signals from users in $\mathcal{I}^i_{j,t}$ are treated as noise and result in a lower transmission rate for u_i. It is well-known that in this scenario, the decoding strategy is optimal since the users' channels are degraded [32], [33]. The interested reader is referred to [9] for a detailed description of optimal decoding strategies in the downlink scenario. The resulting signal to interference plus noise ratio (SINR) of user u_i is

$$\text{SINR}^i_{j,t} = \frac{P^i_{j,t}|h_{i,t}|^2}{|h_{i,t}|^2 \sum_{l \in \mathcal{I}^i_{j,t}} P^l_{j,t} + \sigma^2}, i \in \mathcal{V}_j, j \in [m], t \in \mathbb{N}, \tag{1}$$

where, $P^i_{j,t}$ denotes the transmit power assigned to u_i if virtual user $\mathcal{V}_j$ is activated at time-slot t, and σ^2 is the noise power. Let $R^i_{j,t}$ denote the rate of user u_i if virtual user $\mathcal{V}_j$ is activated at time-slot t, and let $R_{j,t}$ be the resulting sum-rate. Then,

$$R^i_{j,t} = \log_2\left(1 + \text{SINR}_{i,j,t}\right), i \in \mathcal{V}_j, j \in [m], \tag{2}$$

$$R_{j,t} = \sum_{i=1}^{n} R^i_{j,t} \mathbb{1}_{\{u_i \in \mathcal{V}_j\}}, j \in [m]. \tag{3}$$

Temporal fair scheduling guarantees that each user is activated for at least a predefined fraction of the time-slots. More precisely, user $u_i, i \in [n]$ is activated for at least $\underline{w}_i$ of the time, where $\underline{w}_i \in [0, 1]$. Similarly, the scheduler guarantees that the users are not activated more than a predefined fraction of the time-slots which are given by the upper temporal share demands $\overline{w}^n$.

Definition 3 (Temporal Demand Vector): For an n user NOMA system, the vector $\underline{w}^n$ $(\overline{w}^n)$ is called the lower (upper) temporal demand vector.

The scheduler does not have access to the statistics of the performance vector f_{R^m}. Rather, at time-slot $t \in \mathbb{N}$, the scheduler takes $(R_{1,k}, R_{2,k}, \ldots, R_{m,k}), k \in [t]$, the realizations of the performance vector in all time-slots up to time t and outputs the virtual user which is to be activated in the next time-slot. The NOMA scheduling setup is parametrized by $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$.

Definition 4 (Scheduling Strategy): A scheduling strategy (scheduler) $Q = (Q_t)_{t \in \mathbb{N}}$ for the scheduling setup parametrized by the tuple $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$ is a family of (possibly stochastic) functions $Q_t : \mathbb{R}^{m \times t} \to \mathsf{V}, t \in \mathbb{N}$, for which:

- The input to $Q_t, t \in \mathbb{N}$ is the matrix of performance vectors $R^{m \times t}$ which consists of t independently and identically distributed column vectors with distribution f_{R^m}.
- The temporal demand constraints are satisfied:

$$P\left(\underline{w}_i - \epsilon \leq \underline{A}^Q_i \leq \overline{w}_i + \epsilon, i \in [n]\right) = 1, \forall \epsilon > 0, \tag{4}$$

where, the temporal share of user $u_i, i \in [n]$ up to time $t \in \mathbb{N}$ is defined as

$$A^Q_{i,t} = \frac{1}{t} \sum_{k=1}^{t} \mathbb{1}_{\left\{u_i \in Q_k(R^{m \times k})\right\}}, \forall i \in [n], t \in \mathbb{N}, \tag{5}$$

and the average temporal share of user $u_i, i \in [n]$ is

$$\underline{A}^Q_i = \liminf_{t \to \infty} A^Q_{i,t}, \forall i \in [n]. \tag{6}$$

Note that analogous to Equation (6), one could define $\overline{A}^Q_i = \limsup_{t \to \infty} \overline{A}^Q_{i,t}, \forall i \in [n]$ and modify Equation (4) accordingly. However, as we will show in the next sections, for scheduling strategies of interest, we have $\underline{A}^Q_i = \overline{A}^Q_i$.

[1]Note that the performance vector is assumed to be independent over time, meaning that at any two distinct time-slots, the performance vectors are independent of each other. However at a given time-slot the performance of the virtual users may be dependent with each other.

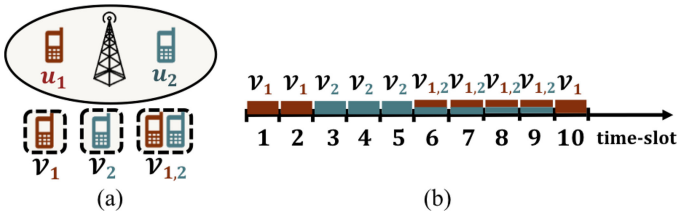

Fig. 1. (a) Two-user NOMA system with three virtual users. (b) Weighted Round Robin scheduling strategy when $\underline{w}_1 = \underline{w}_2 = 0.6$.

Remark 3: A scheduling setup where the temporal shares of users are required to take a specific value, i.e. $\underline{A}_i^Q = w_i, i \in [n]$, is called a scheduling setup with equality temporal constraints and is parametrized by $(n, N_{\max}, w^n, w^n, f_{R^m})$.

Definition 5 (System Utility): For a scheduling strategy Q:

- The average system utility up to time t, is defined as

$$U_t^Q = \frac{1}{t}\sum_{k=1}^{t}\sum_{j=1}^{m} R_{j,k}\mathbb{1}_{\left\{Q_k(R^{m\times k})=\mathcal{V}_j\right\}}. \tag{7}$$

- The average system utility is defined as

$$U^Q = \liminf_{t\to\infty} U_t^Q. \tag{8}$$

To further explain the notation, we provide an example of a weighted round robin scheduling strategy in a two-user NOMA scenario.

Example 1: Consider the downlink scenario shown in Figure 1. In this scenario $n = 2$, and $\mathcal{U} = \{u_1, u_2\}$. Furthermore, $m = 3$ and $\mathsf{V} = \{\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3\}$, where $\mathcal{V}_1 = \{u_1\}, \mathcal{V}_2 = \{u_2\}$, and $\mathcal{V}_3 = \mathcal{V}_{1,2} = \{u_1, u_2\}$. Let the fairness constraints be given by the temporal weight demands $\underline{w}_1 = \underline{w}_2 = 0.6$ and $\overline{w}_1 = \overline{w}_2 = 1$. This requires each user to be activated for at least 0.6 fraction of the time. One possible scheduling strategy in this scenario is the Weighted Round Robin (WRR) strategy shown in Figure 1(b). The strategy is described below:

$$Q_t = \begin{cases} \mathcal{V}_1, & \text{if } 0 \le mod_{10}(t) \le 2, \\ \mathcal{V}_2, & \text{if } 3 \le mod_{10}(t) \le 5, \\ \mathcal{V}_{1,2}, & \text{if } 6 \le mod_{10}(t) \le 9. \end{cases} \tag{9}$$

The WRR strategy is a non-opportunistic strategy where virtual users are chosen independently of the realization of the performance vector. As a result, the temporal share $A_{i,t}^Q, i \in [n], t \in \mathbb{N}$ is a deterministic function of t. Note that $\underline{A}_i^Q = 0.3 + 0.4 = 0.7, i = 1, 2$; hence the WRR strategy satisfies the temporal demand conditions (4). Also, it is straightforward to show that the average network utility is $U^Q = 0.3\mathbb{E}(R_1) + 0.3\mathbb{E}(R_2) + 0.4\mathbb{E}(R_3)$.

The scheduler $Q = (Q_t)_{t\in\mathbb{N}}$ takes the matrix $R^{m\times t}$ of performance values up to time t as input and outputs the virtual user $\mathcal{V}_j, j \in [m]$ which is to be activated at time t. Temporal share $A_{i,t}^Q, i \in [n], t \in \mathbb{N}$ in (5) represents the fraction of time-slots in which user u_i is activated until time t. The variable $\underline{A}_i^Q, i \in [n]$ is an asymptotic lower bound to the temporal share of user u_i and (4) represents the temporal fairness constraints. Furthermore, U_t^Q and U^Q are the instantaneous and average system utilities, respectively. The objective is to design a scheduling strategy which achieves the maximum average network utility while satisfying temporal fairness constraints.

Definition 6 (Optimal Strategy): For the scheduling setup parametrized by $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$, a strategy Q^* is optimal if and only if

$$Q^* \in \operatorname*{argmax}_{Q\in\mathcal{Q}} U^Q, \tag{10}$$

where $\mathcal{Q}$ is the set of all strategies for the scheduling setup.

The set $\mathcal{Q}$ includes strategies with memory as well as non-stationary and stochastic strategies. As a result, the cardinality of the set is large and the optimization problem described in Equation (10) is not computable through exhaustive search. However, in Section IV we show that this optimization problem can be expressed in a computable form by restricting the search to a specific subset of stationary and memoryless strategies called *threshold based strategies*. More precisely, we show that any optimal strategy is equivalent to a threshold based strategy where equivalence between strategies defined below

Definition 7 (Equivalence): For the scheduling setup $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$ two strategies Q and Q' are called equivalent ($Q \sim Q'$) if:

$$\lim_{t\to\infty}\frac{1}{t}\sum_{k=1}^{t} P\left(Q_k\left(R^{m\times k}\right) = Q'_k\left(R^{m\times k}\right)\right) = 1.$$

Definition 8 (Stationary and Memoryless): A strategy $Q = (Q_t)_{t\in\mathbb{N}}$ is called memoryless if $Q_t(R^{m\times t}), t \in \mathbb{N}$ is only a function of the performance vector $(R_{1,t}, R_{2,t}, \ldots, R_{m,t})$ corresponding to time t. For the memoryless strategy Q, we write $Q_t(R^m)$ instead of $Q_t(R^{m\times t})$ when there is no ambiguity. A memoryless strategy is called stationary if $Q_t(R^m) = Q_{t'}(R^m)$ for any $t, t' \in \mathbb{N}$.

Lemma 1: For a memoryless and stationary strategy Q, the following limits exist:

$$A_i^Q = \lim_{t\to\infty} A_{i,t}^Q, \qquad U^Q = \lim_{t\to\infty} U_t^Q. \tag{11}$$

The proof is provided in the Appendix.

Definition 9 (TBS): For the scheduling setup $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$ a threshold based strategy (TBS) is characterized by the vector $\lambda^n \in \mathbb{R}^n$. The strategy $Q_{TBS}(\lambda^n) = (Q_{TBS,t})_{t\in\mathbb{N}}$ is defined as:

$$Q_{TBS,t}\left(R^{m\times t}\right) = \operatorname*{argmax}_{\mathcal{V}_j\in\mathsf{V}} S\left(\mathcal{V}_j, R_{j,t}\right),\ t \in \mathbb{N}, \tag{12}$$

where $S\left(\mathcal{V}_j, R_{j,t}\right) = R_{j,t} + \sum_{i=1}^{n}\lambda_i\mathbb{1}_{\{u_i\in\mathcal{V}_j\}}$ is the 'scheduling measure' corresponding to the virtual user $\mathcal{V}_j$. The resulting temporal shares are represented as $w_i = A_i^{Q_{TBS}}, i \in [n]$. The utility of the TBS is written as $U_{w^n}(\lambda^n)$. The space of all threshold based strategies is denoted by $\mathcal{Q}_{TBS}$.

We note that threshold based strategies are stationary and memoryless. The reason is that the output of $Q_{TBS,t}, t \in \mathbb{N}$ in (12) depends only on the threshold vector λ^n and the realization of R^m at time t.

Example 2: Consider the NOMA system described in Example 1. A TBS with threshold vector $\lambda^2 = (\lambda_1, \lambda_2)$ has the following scheduling measures:

$$S(\mathcal{V}_1, R_{1,t}) = R_{1,t} + \lambda_1,$$
$$S(\mathcal{V}_2, R_{2,t}) = R_{2,t} + \lambda_2,$$
$$S(\mathcal{V}_{1,2}, R_{1,2,t}) = R_{1,2,t} + \lambda_1 + \lambda_2.$$

The virtual user with the highest scheduling measure is chosen at each time-slot. Note that the probability of a tie among the scheduling measures is 0 since the performance vector R^m is assumed to be jointly continuous.

IV. Existence of Optimal Threshold Based Strategies

In this section, we show that for any scheduling problem with temporal fairness constraints, optimal utility can be achieved using a threshold based scheduling strategy. Therefore, in considering the optimization problem described in Equation (10), the set of strategies $\mathcal{Q}$ can be restricted to the set of threshold based strategies. Furthermore, we show that any scheduling strategy which achieves optimal utility is equivalent to a threshold based strategy, where equivalence between strategies is defined in Definition 7.

A. Optimal Temporally Fair NOMA Scheduling

Theorem 1: For the NOMA scheduling setup $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$, assume that $\mathcal{Q} \neq \varnothing$. Then, there exists an optimal threshold based strategy Q_{TBS}. Furthermore, for any optimal strategy Q, there exists a threshold based strategy Q' such that $Q \sim Q'$.

The condition $\mathcal{Q} \neq \varnothing$ in Theorem 1 is called the feasibility condition and is investigated in Section IV-B. The proof of the theorem follows form the following steps:

- Under equality temporal demand constraints where $\underline{w}^n = \overline{w}^n = w^n$, existence of optimal TBSs follows from a generalization of the intermediate value theorem called the Poincaré-Miranda Theorem [34].
- The uniqueness of an optimal strategy up to equivalence follows from a variant of the dual (Lagrangian multiplier) optimization method.
- Under inequality temporal demand constraints, the proof of existence follows by discretizing the feasible space and solving the optimization for each point on the discretized space under equality constraints.

The complete proof of Theorem 1 is provided in the Appendix. The following corollaries follow from the proof.

Corollary 1: Consider the NOMA scheduling setup under equality temporal demand constraints $(n, N_{\max}, w^n, w^n, f_{R^m})$, where $\mathcal{Q} \neq \varnothing$. There exists a unique TBS Q_{TBS} satisfying the temporal demand constraints and this TBS is the optimal scheduling strategy for this setup.

The following corollary states that the search for the optimal strategy in Equation (10) may be restricted to the set of TBSs.

Corollary 2: For the scheduling setup $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$, the optimal achievable utility is given by:

$$U^*_{\underline{w}^n, \overline{w}^n} \triangleq \max_{\lambda^n : \underline{w}_i \leq A_i^{Q_{TBS}} \leq \overline{w}_i} U_{w^n}(\lambda^n), \tag{13}$$

where $U_{w^n}(\lambda^n)$ is defined in Definition 9.

As a consequence of Theorem 1, under equality temporal demand constraints, the optimal achievable utility is equal to the utility of the unique TBS satisfying the temporal demand constraints (i.e. $U^*_{w^n, w^n} = U_{w^n}(\lambda^n)$). The reason is that the threshold based strategy achieves optimal utility among all strategies with temporal shares equal to w^n.

The following Corollary is used in Section VII to provide a low complexity algorithm for constructing optimal TBSs.

Corollary 3: For the NOMA scheduling setup $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$, assume that there exist positive thresholds $\lambda_1, \lambda_2, \ldots, \lambda_n$ satisfying the complimentary slackness conditions:

$$\lambda_i \left(A_i^{Q_{TBS}} - \underline{w}_i \right) = 0, \forall i \in [n],$$
$$\underline{w}_i \leq A_i^{Q_{TBS}} \leq \overline{w}_i, \forall i \in [n],$$

where Q_{TBS} is the TBS corresponding to the threshold vector λ^n. Then, Q_{TBS} is an optimal scheduling strategy.

Note that the complementary slackness conditions in Corollary 3 are written only in terms of the lower temporal demands. Similar sufficient conditions can be derived in terms of the upper temporal share demands.

Remark 4: If $Q \sim Q'$, then the two scheduling strategies activate the same subsets of users in almost all time-slots. As a result, the two strategies have the same performance under any long-term fairness and utility criteria. Let $\mathcal{Q}^*$ be the set of all optimality achieving strategies under temporal demand constraints. A consequence of Theorem 1 is that all of the strategies in $\mathcal{Q}^*$ have the same performance with each other under any additional utility or fairness criteria.

B. Feasible Temporal Share Region

Section IV-A affirms the existence of a TBS that achieves the optimal average system utility given that the temporal demands are feasible. However, some values of $(\underline{w}^n, \overline{w}^n)$, are not achievable by any scheduling strategy. In other words, the set $\mathcal{Q}$ is empty for certain pairs of constraint vectors $(\underline{w}^n, \overline{w}^n)$. In this section, we provide a variable elimination method which allows us to characterize the feasible region for a given scheduling setup as a function of its temporal demand vectors.

Definition 10: A scheduling setup $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$ is called feasible if $\mathcal{Q} \neq \varnothing$. The set of temporal shares w^n for which the setup is feasible under equality constraints is called the feasible region and is denoted by $\mathcal{W}$.

The following theorem characterizes the set of all feasible scheduling setups.

Theorem 2: A scheduling setup with equality temporal constraints $(n, N_{\max}, w^n, w^n, f_{R^m})$ is feasible if and only if there exist a set of non-negative values $\{a_j : j \in [m]\}$ satisfying the

following bounds:

$$\sum_{j\in[m]} a_j = 1, \quad \sum_{j:u_i\in\mathcal{V}_j} a_j = w_i, \forall i \in [n], \quad 0 \le a_j, \forall j \in [m]. \tag{14}$$

Furthermore, the scheduling setup with inequality temporal constraints $(n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{R^m})$ is feasible if and only if there exist a set of non-negative numbers $\{w_i : i \in [n]\}$. Such that i) $(n, N_{\max}, w^n, w^n, f_{R^m})$ is feasible, and ii) the following bounds are satisfied:

$$\forall i \in [n] : \underline{w}_i \le w_i \le \overline{w}_i.$$

Proof Sketch: In order to prove that $\mathcal{Q} \neq \varnothing$ under equality constraints, we use a WRR scheduler in which the weight assigned to $\mathcal{V}_j$ is equal to a_j. Under inequality temporal constraints, in order to have $\mathcal{Q} \neq \varnothing$, it suffices that there is a vector of temporal shares in the feasible region which satisfies the inequality constraints. On the other hand, if the scheduling setup is feasible (i.e. $\mathcal{Q} \neq \varnothing$), then a WRR strategy exists which satisfies the temporal demand constraints. Taking a_j to be equal to the temporal weight assigned to $\mathcal{V}_j$, it is straightforward to verify that Equations in (14) hold. ■

The feasibility conditions in Theorem 2 are written in terms of auxiliary variables $a_j, j \in [m]$ which can be interpreted as the temporal shares of the virtual users. However, it is often desirable to write the feasibility conditions in terms of the temporal share vector w^n. The conditions can be re-written in the desired form using the Fourier-Motzkin elimination (FME) algorithm. The standard FME algorithm has worst case computational complexity of order $O(m^{2^{m-n-1}})$ [35]. In [36], a method for variable elimination was proposed which has a significantly lower computation complexity. The method leads to the following algorithm for determining the feasible region:

Step 1: Eliminate $a_i, i \le n+1$ using the equality constraints (14):

$$a_i = w_i - \sum_{j:u_i\in\mathcal{V}_j} a_j, i \in [n], \quad a_{n+1} = 1 - \sum_{j\in[m], j\neq n+1} a_j.$$

That is, replace $a_i, i \le n+1$ in all inequality constraints (14) by the right hand sides in the above equations.

Step 2: Define $c_{l,j}, l \in [m], 1 \le j \le n$ as the coefficient of w_j in the lth inequality after Step 1. Also, define $c_{l,j}, l \in [m], n+2 \le j \le m$ as the coefficient of a_j in the lth inequality. Construct the dual system of equations:

$$\sum_{l\in[m]} c_{l,j}x_l = 0, \quad x_l \in \mathbb{N} \cup \{0\}, \ j \in \{n+2, n+3, \ldots, m\}.$$

Step 3: Use the Normaliz algorithm [37] to find the Hilbert basis for the solution space of the dual system. Let $\mathcal{B} = \{b_1^m.b_2^m, \ldots, b_k^m\}$ be the Hilbert basis, where k is the number of Hilbert basis elements.

Step 4: Let $b_i^m = (b_{i,1}, b_{i,2}, \ldots, b_{i,m}), i \in [k]$. The following system of inequalities gives the feasible region:

$$0 \le \sum_{l\in[n+1]} \sum_{j\in[n]} b_{i,l}c_{j,l}w_j, \ i \in [k]. \tag{15}$$

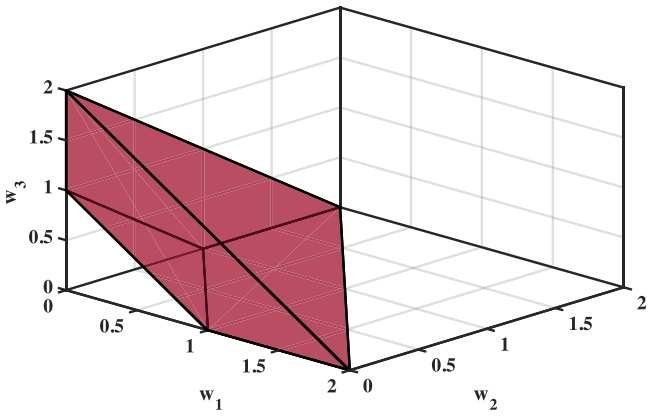

Fig. 2. The colored region shows the set of feasible weight vectors for the three user NOMA problem with $N_{\max} = 2$.

The elimination process is explained in the following example.

Example 3: Consider a three user downlink NOMA scenario with $N_{\max} = 2$. The scheduling setup is feasible if there exists a vector of virtual user temporal weights $(a_1, a_2, a_3, a_{1,2}, a_{1,3}, a_{2,3})$ such that:

$$0 \le a_1, \ 0 \le a_2, \ 0 \le a_3, \ 0 \le a_{1,2}, \ 0 \le a_{1,3}, \ 0 \le a_{2,3}$$

$$a_1 + a_2 + a_3 + a_{1,2} + a_{1,3} + a_{2,3} = 1,$$

$$a_1 + a_{1,2} + a_{1,3} = w_1, \quad a_2 + a_{1,2} + a_{2,3} = w_2,$$

$$a_3 + a_{1,3} + a_{2,3} = w_3.$$

Using the equality constraints, one could write a_1, a_2, a_3 and $a_{1,2}$ as functions of $w_1, w_2, w_3, a_{1,3}$ and $a_{2,3}$. We get:

$$0 \le 1 + a_{1,3} - w_1 - w_3, \quad 0 \le 1 + a_{2,3} - w_2 - w_3,$$

$$a_{1,3} + a_{2,3} \le \min(w_3, w_1 + w_2 + w_3 - 1),$$

$$0 \le a_{1,3}, \quad 0 \le a_{2,3}.$$

There are a total of five inequalities, i.e. $k = 5$. The dual system is given by:

$$x_1 - x_3 + x_4 = 0, \qquad x_2 - x_3 + x_5 = 0.$$

The Hilbert basis is $\mathcal{B} = \{(1,1,1,0,0), (0,0,1,1,1), (0,1,1,1,0), (1,0,1,0,1)\}$. From Equation (15), the feasible region is as follows:

$$0 \le w_i \le 1, \ i \in [3], \quad 1 \le w_1 + w_2 + w_3 \le 2.$$

The region is shown in Figure 2.The figure can be interpreted as follows: the sum of the temporal shares of all users cannot exceed two since no more than two users can be activated at each time-slot. Furthermore, the sum cannot be lower than one since at least one user is activated at each time-slot.

The problem of determining the feasible region is more complicated for large non-homogeneous NOMA systems where specific subsets of users cannot be activated simultaneously due to practical considerations. In such instances the elimination method proposed in this section can be a valuable tool in determining the feasible region.

V. Construction of Optimal Scheduling Strategies

In the previous section, it was shown that for any feasible scheduling problem, optimal utility is achieved using TBSs. In this section, we address the construction of optimal scheduling strategies and provide an iterative method which builds upon the Robbins-Monro algorithm [38] to find optimal thresholds for TBSs. Note that the scheduler does not have access to the statistics of the performance vector. The algorithm proposed in this section uses the empirical observations of the realizations of the performance vector to find the optimal thresholds iteratively.

A. The Robbins-Monro Algorithm

The Robbins-Monro algorithm [38] is a method for finding the roots of the univariate function $f:\mathbb{R}\rightarrow\mathbb{R}$ based on a limited number of noisy samples of $f(x), x\in\mathbb{R}$. More precisely, assume that we take l noisy samples $g_t=f(x_t)+\epsilon_t$ of the function $f(\cdot)$ at $x_t, t\in[l],$, where the random variable ϵ_t is the sampling noise at time t and l is a fixed natural number.

The objective is to approximate the solution of $f(x)=0$ by choosing $x_t, t\in[l]$ suitably such that the approximation converges to the root as $l\rightarrow\infty$. The algorithm was extended to find roots of multi-variate functions by Ruppert [39]. Let $f:\mathbb{R}^n\rightarrow\mathbb{R}^n$ be a mapping of the n-dimensional Euclidean space onto itself. Let $g_t=f(x_t^n)+\epsilon_t^n$ be the noisy sample of $f(x_t^n)$ at $x_t^n, t\in[l]$, and the step-size sequence $(s_t)_{t\in\mathbb{N}}$ be a sequence of positive real numbers. It can be shown that sequence $x_{t+1}^n=x_t^n-s_tg_t^n$ converges to the solution of the system $f(x^n)=0$ if the following conditions hold:

1) *Solvability:* The function $f(\cdot)$ has a root x^{*n}.
2) *Local Monotonicity:* $(x^n-x^{*n})^Tf(x^n)>0$ for $x^n\neq x^{*n}$.
3) *Zero-mean and i.i.d. noise:* $\epsilon_t^n, t\in\mathbb{N}$ is an i.i.d. sequence and $\mathbb{E}(\epsilon_t^n)=0$.
4) *Step-size constraints:* $s_t>0$, $\lim_{t\rightarrow\infty}s_t=0$, $\sum_{t=1}^{\infty}s_t=\infty$, $\sum_{t=1}^{\infty}s_t^2<\infty$.

B. Finding Thresholds under Equality Constraints

In Corollary 1, we showed that any threshold based strategy satisfying the equality temporal constraints is optimal. As a result, the objective of finding the optimal scheduling strategy is reduced to finding the thresholds which lead to a TBS satisfying the temporal demand constraints. More precisely, we are interested in finding the threshold vector λ^n such that

$$A_i^{Q_{TBS}(\lambda^n)}=w_i, i\in[n]. \tag{16}$$

Hence, finding the optimal TBS is equivalent to solving the non-linear system of equations in (16). Next, we show that the empirical observation of the realizations of R^m at the BS is sufficient to find the optimal thresholds using the multi-variate version of the Robbins-Monro stochastic approximation method [39].

In the scheduling problem, consider $f_i(\lambda^n)=A_i^Q(\lambda^n)-w_i, i\in[n]$. We are interested in finding the root of the function $f(\cdot)$ provided that the root exists (i.e. $\mathcal{Q}\neq\varnothing$). In Theorem 3, we show that conditions (1)-(4) provided above are satisfied for a suitable step-size sequence. Note that $A_i^Q(\lambda^n)$ depends on the statistics of the performance vector R^m and is not explicitly available in practice. Assume that at time t, the scheduler uses the threshold vector λ_t^n. Then, it observes $g_{t,i}\triangleq\mathbb{1}\{u_i\in Q_t(\lambda_t^n)\}-w_i$ which is a noisy sample of $f(\lambda_t^n)=A_i^Q(\lambda_t^n)-w_i$. The sampling noise is $\epsilon_{t,i}=g_{t,i}(\lambda_t^n)-f_i(\lambda_t^n)=\mathbb{1}\{u_i\in Q_t(\lambda_t^n)\}-A_i^Q(\lambda_t^n)$. The sequence of sampling noise vectors $\epsilon_t^n, t\in\mathbb{N}$ is an i.i.d. sequence since $Q_t(\lambda_t^n)$ depends only on the realization of R^m at time t which are assumed to be i.i.d. over time. Furthermore, it is straightforward to show that $\mathbb{E}(\epsilon_{t,i})=0$. Therefore, conditions (1) and (3) are satisfied. The following theorem shows that conditions (2) and (4) hold for $N_{\max}>1$.

Theorem 3: Let $f_i(\lambda^n)=A_i^Q(\lambda^n)-w_i, i\in[n]$. The convergence conditions (1)–(4) in the multi-variate Robbins-Monro algorithm are satisfied for step-size the sequence $s_t=\frac{1}{t}, t\in\mathbb{N}$.

The proof is provided in the Appendix.

C. Finding Thresholds Under General Temporal Constraints

In this section, we provide an algorithm for finding the optimal TBS thresholds under general temporal demand constraints (Algorithm 1). The optimization algorithm uses a combination of the gradient projection method [40] and the Robbins-Monro algorithm described in the previous section. The algorithm leverages the concavity of $U^*_{\underline{w}^n,\overline{w}^n}$ shown in Lemma 2 and applies gradient projection to ensure that the solution converges to an optimal threshold vector within the feasible space. Furthermore, we build upon Algorithm 1 to propose a low-complexity heuristic algorithm (Algorithm 2) which is used in Section VII for simulations.

Lemma 2: The optimal achievable utility $U^*_{\underline{w}^n,\overline{w}^n}$ is jointly concave as a function of $(\underline{w}^n,\overline{w}^n)$.

The proof is provided in the Appendix. As a consequence of Lemma 2, the optimization in (13) can be performed using standard gradient projection methods [40]. Note that the gradient projection method requires prior knowledge of the feasible set which is characterized using the method in Section IV-B.

Algorithm 1 performs an iterative two-step optimization. At each iteration, in the first step, given a fixed temporal demand vector w^n, the Robbins-Monro algorithm is used to find the thresholds under equality temporal constraints. Next, the gradient projection method is used to update the weight vector w^n based on $\nabla U_{w^n,w^n}$. The algorithm converges to the optimal utility due to the concavity of $U^*_{\underline{w}^n,\overline{w}^n}$. The iteration stops if $\Delta\geq\epsilon$, where Δ represents the variation in w^n at each step and ϵ is the stopping parameter. It can be noted that the choice of the initial demand vector w_0^n does not affect the convergence of the proposed method since $U^*_{w^n,w^n}$ is jointly concave as shown in Lemma 2.

Algorithm 1 requires estimating the gradient of $U^*_{w^n,w^n}$ which entails high computational complexity. To elaborate, in order to use the gradient projection method, the scheduler needs to know $\nabla U^*_{w^n,w^n}$. However, the scheduler does not know the statistics of the performance vector. As a result, it must estimate $\nabla U^*_{w^n,w^n}$ using a gradient estimation method based on the empirical observations of the performance vector. As an alternative, we propose

Algorithm 1: Two-stage Threshold Optimization in TBS.

1: Obtain feasibility region $\mathcal{W}$ (Section IV-B).
2: Set $\epsilon > 0$ and $\Delta = 2\epsilon$.
3: Choose initial demand vector $w^n = w_0^n$.
4: **while** $\Delta \geq \epsilon$ **do**
5: Find $U^*_{w^n,w^n}$ and corresponding λ^n (Robbins-Monro Algorithm in Section V-B).
6: Update w^n based on $\nabla U^*_{w^n,w^n}$ (gradient projection step).
7: $\Delta = ||w^n_{new} - w^n||$
8: **end while**

Algorithm 2: Heuristic Threshold Optimization in TBS.

Initialization: $\lambda_{1,i} = 0, i \in [n]$
1: **for** $t \in \mathbb{N}$ **do**
2: $\mathcal{V}_t = Q_t(\lambda^n_t)$
3: $A^Q_{t+1,i} = A^Q_{t,i} + \frac{1}{t+1}\Big(\mathbb{1}\{i \in \mathcal{V}_t\} - A^Q_{t,i}\Big)$
4: $\lambda_{\min} = \min_{i\in[n]} \lambda_{t,i}$
5: $\lambda_{t+1,i} = \lambda_{t,i} - s\Big(\lambda_{t,i} - \lambda_{\min}\Big)\Big(\mathbb{1}\{u_i \in \mathcal{V}_t\} - \underline{w}_i\Big), i \in [n]$
6: **for** $i = 1$ to n **do**
7: **if** $\lambda_{t,i} = \lambda_{\min}$ and $A^Q_{t+1,i} < \underline{w}_i$ **then**
8: $\lambda_{t+1,i} = \lambda_{t,i} + s\Big(\underline{w}_i - A^Q_{t+1,i}\Big)$
9: **end if**
10: **if** $\lambda_{t,i} = \lambda_{\min}$ and $\lambda_{\min} < 0$ **then**
11: $\lambda_{t+1,i} = \lambda_{t,i} + s$
12: **end if**
13: **end for**
14: **end for**

Algorithm 2 which is a low complexity heuristic variation of Algorithm 1. The algorithm is constructed using the complementary slackness conditions provided in Corollary 3. Algorithm 2 replaces gradient projection in Algorithm 1 by a simple perturbation step.

Algorithm 2 starts with a vector of initial thresholds. At time-slot t, it chooses virtual user $\mathcal{V}_t$ to be activated based on the threshold vector λ^n_t. It updates the temporal shares and thresholds based on the scheduling decision at the end of the time-slot (line 2–5). The update rule for the thresholds given in line 5 is a variation of the Robbins-Monro update described in Section V. The parameter s is the step-size. Lines (6–13) replace the gradient projection step in Algorithm 1 and verify that the temporal demand constraints and dual feasibility conditions are satisfied. The computational complexity of the algorithm grows polynomially in the number of users. For instance, when $N_{\max} = 2$, the computational complexity at each time-slot is proportional to the number of virtual users and is $O(n^2)$.

VI. Discrete and Mixed Performance Variables

So far, we have assumed that the performance vector R^m is jointly continuous. The proofs provided for Theorems 1 and 3 rely on the joint continuity assumption. However, in practical scenarios, the performance vector is a vector of discrete or mixed random variables. For instance, in cellular systems, the performance vector is discrete due to discrete modulation and coding schemes.

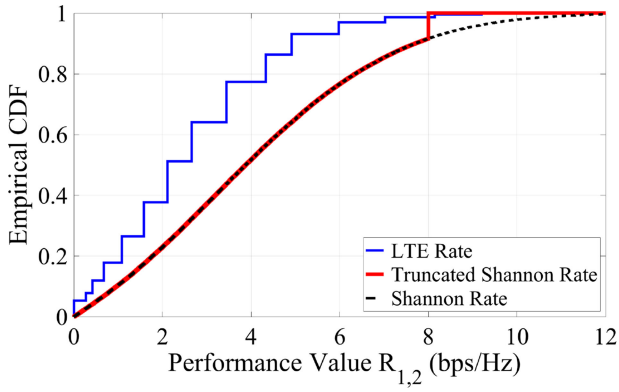

Fig. 3. Empirical CDF of performance value of virtual user $\mathcal{V}_{1,2}$ in two user NOMA.

The performance value of a virtual user is a function of the SINR of its elements. For instance, in Section III, sum-rate in the NOMA downlink scenario was considered as the performance metric which is a logarithmic function of the SINRs. Since the logarithm function is continuous, the performance vector is a jointly continuous vector of random variables. However, in practical scenarios, the function which relates the SINR to the performance value is neither injective nor continuous. The function is determined by the choice of the modulation and coding schemes at each time-slot. Moreover, in some applications, the performance value is approximated by a truncated Shannon rate function, i.e. $R = \min\{\log_2(1 + \text{SINR}), \gamma_{\max}\}$, where $\gamma_{\max}$ is the maximum data rate supported by the system. In this case, the performance value has a mixed distribution function. Figure 3 shows the empirical CDF of the performance value of virtual user $\mathcal{V}_{1,2}$ in the downlink of a two user NOMA system with SIC, where the performance value is taken as i) the Shannon sum-rate for NOMA downlink scenario as described in Section III, ii) truncated Shannon sum-rate, and iii) sum-rate with LTE modulation and coding schemes. In the truncated Shannon sum-rate model we use $\gamma_{\max} = 4$ bps/Hz and in the LTE rate model we use the parameters in [41, Table 7.2.3-1], where 15 combinations of modulation and coding schemes are used.

The analysis provided in the previous sections cannot be applied directly to mixed and discrete performance vectors. The reason is that when the performance values are jointly continuous, the probability of having a tie among the scheduling measures in a TBS is zero. However, there may be more than one virtual user with the highest scheduling measure in the case of a mixed or discrete performance vector. In such scenarios, there is a need for a tie-breaking rule which affects the optimality of the scheduler. One widely used solution in OMA scheduling is to use a stochastic tie-breaker where in the event of a tie, one of the users is activated randomly based on a given probability distribution called the tie-breaking probability [19]. This requires a joint optimization of the thresholds and the tie-breaking rule.

We propose a new class of scheduling strategies called ℓ-perturbed TBSs to handle mixed and discrete random variables. An ℓ-perturbed TBS is a variation of TBSs where the scheduling measure takes a perturbation of the performance vector as its input. To elaborate, fix $\ell \in \mathbb{N}$. Define $\widetilde{R}_{j,t}(\ell) = R_{j,t} + N_{j,t,1/\ell}$, $j \in [m]$ where $N_{j,t,1/\ell} \sim Unif[-1/\ell, 1/\ell]$ and the variables $N_{j,t,1/\ell}$ are jointly independent. It is straightforward to show that $(R_{j,t}(\ell))_{j\in[m]}$ is a jointly continuous vector of random variables. Let Q be a TBS characterized by the threshold vector λ^n. At time-slot t, the ℓ-perturbed TBS $Q_{1/\ell}$ activates $\mathcal{V}_{J,t} = Q_{1/\ell}(R^{m\times t}) = Q(\widetilde{R}^{m\times t})$, where J is the random variable corresponding to the index of the activated virtual user. The resulting utility is equal to $R_{J,t}$. The class of perturbed TBSs are formally defined below.

Definition 11 (Discrete Scheduling Setup): A discrete scheduling setup is characterized by $(n, N_{\max}, \underline{w}^n, \overline{w}^n, R^m)$, where R^m may be a discrete or mixed vector of random variables.

Definition 12 (ℓ-PTBS): For the scheduling setup $(n, N_{\max}, \underline{w}^n, \overline{w}^n, R^m)$ an ℓ-perturbed threshold based strategy (ℓ-PTBS) is characterized by the vector $\lambda^n \in \mathbb{R}^n$. The strategy $Q_{1/\ell}(\lambda^n) = (Q_{1/\ell,t})_{t\in\mathbb{N}}$ is defined as:

$$Q_{1/\ell,t}\big(R^{m\times t}\big) = \underset{\mathcal{V}_j\in\mathsf{V}}{\operatorname{argmax}}\ S_\ell\big(\mathcal{V}_j, \widetilde{R}_{j,t}\big),\ t \in \mathbb{N}, \tag{17}$$

where $\widetilde{R}_{j,t}(\ell) = R_{j,t} + N_{j,t,1/\ell}$ are the perturbed performance values and $N_{j,t,1/\ell} \sim Unif[-1/\ell, 1/\ell]$ are jointly independent.

The following theorem shows that the average system utility for the designed ℓ-PTBS approaches the optimal utility of the original system as $\ell \to \infty$. However, it should be noted that the precision supported by the scheduler's equipment sets an upper limit on ℓ.

Theorem 4: Let Q^* be the optimal scheduling strategy for the setup $\Omega_0 = (n, N_{\max}, \underline{w}^n, \overline{w}^n, R^m)$. Let $Q^*_{1/\ell}$ be the optimal TBS for the setup $\Omega_{1/\ell} = (n, N_{\max}, \underline{w}^n, \overline{w}^n, f_{\widetilde{R}^m})$, where $\widetilde{R}^m = R^m + N^m_{1/\ell}$ and $N^m_{1/\ell}$ is a vector of independent $Unif[-1/\ell, 1/\ell]$ variables. Let $\widehat{Q}_{1/\ell}$ be the ℓ-PTBS characterized by the same threshold vector as $Q^*_{1/\ell}$. Define U^* and $U_{1/\ell}$ as the average system utility due to Q^* and $\widehat{Q}_{1/\ell}$ when applied to system Ω_0, respectively. Then,

$$\lim_{\ell\to\infty}(U^* - U_{1/\ell}) = 0,$$

where convergence is in probability. Alternatively, the utility of $\widehat{Q}_{1/\ell}$ applied to Ω_0 converges to the optimal utility as $\ell \to \infty$.

The proof is provided in Appendix E.

VII. Numerical Results and Simulations

In this section, we provide various numerical examples and simulations to evaluate the performance of the approaches proposed in Sections V and VI. We simulate the DL of a small-cell NOMA system consisting of a BS and a number of users distributed uniformly at random in a ring around the BS with inner and outer radii of 20 m and 100 m, respectively. Two user mobility models are considered in the simulations. In the first model, the users are assumed to be static, whereas the second model uses a two-dimensional random walk. Table I lists the network parameters. We consider $N_{\max} = 2$, i.e. an individual user or a pair of users is scheduled at each time-slot. We assume that there are no upper temporal demand constraints. The user SINRs are modeled as described in Equation (1) and the network utility is assumed to be truncated Shannon sum-rate unless otherwise stated. At each time-slot prior to scheduling, a max-min power optimization is performed for each virtual user [11]. For a given virtual user, we find the transmit power which maximizes the minimum individual user rates in that virtual user. This max-min optimization allows for a balanced rate allocation within the virtual user. It can be shown that the max-min optimization is quasi-concave. Consequently, quasi-concave programming methods such as bisection search can be used to find the optimal transmit powers [11]. Maximum BS transmit power constraint is chosen such that the average SNR of 10 dB is achievable when a single user is active on the boundary of the cell. We use Algorithm 2 described in Section V for simulations. The step-size s is taken to be 0.001.

TABLE I
Simulation Parameters

Parameter	Value
Scenario	NOMA downlink with SIC
Number of users	2, 3, 4, 5, 6
Cell radius	100 m
System Bandwidth	10 MHz
Number of time-slots	5×10^6
Maximum spectral efficiency	6 bps/Hz
Noise spectral density	−174 dBm/Hz
Noise figure	9 dB
Shadowing standard deviation	8 dB
Path loss in dB	$128.1 + 37.6 \log_{10}(d \text{ in km})$
Rate in bps/Hz	$\min\{\log_2(1 + \text{SINR}), 6\}$
User mobility models	Static, 2D random walk

A. Performance Evaluation

We evaluate the performance of the NOMA scheduler in a scenario where the users are static. As a benchmark, we consider an OMA system where a single user is activated at each time-slot. To find a temporal fair scheduler in an OMA system, we consider the setup when $N_{\max} = 1$. We also consider Round Robin (RR) scheduling as another benchmark. Figure 4 shows the empirical cumulative distribution function (CDF) of the network throughput in a network with $n = 5$ users and $\underline{w}_i = 0.2, \forall i \in [5]$ for various scheduling strategies. We observe that there are significant improvements in terms of network throughput when the TBS (labeled opportunistic NOMA) is used compared to OMA (labeled opportunistic OMA) as expected. Furthermore, we note that RR scheduling in NOMA leads to a significant performance loss. The RR strategy chooses the virtual user regardless of the performance in that time-slot. As a result, the strategy is particularly inefficient in NOMA systems. The reason is that SIC which is used in NOMA may have a poor performance for a given virtual user in some time-slots.

Table II lists the percentage of the average throughput gain when using opportunistic NOMA scheduler compared to an opportunistic OMA scheduler. For a given number of users

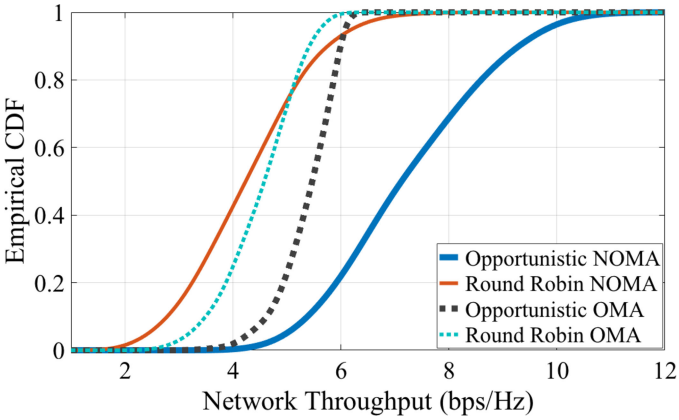

Fig. 4. Empirical CDF of network throughput for NOMA and OMA systems using different scheduling schemes when the users are static.

TABLE II
AVERAGE THROUGHPUT GAIN OF OPPORTUNISTIC NOMA SCHEDULING OVER OPPORTUNISTIC OMA SCHEDULING

Number of users	2	3	4	5	6
Throughput gain (%)	7.33	18.99	27.08	37.14	45.47

$n \in \{2, 3, \ldots, 6\}$, we simulated 100 independent realizations of the network. It can be observed that increasing the number of users boosts the NOMA performance gain. This is due to the fact that the number of virtual users increases as n becomes larger. As a result, the NOMA scheduler has more options in the choice of the active virtual user.

B. Convergence

In this section, we investigate the evolution of the scheduling thresholds when running Algorithm 2. We consider a scenario with $n = 5$ users and $\underline{w}^5 = [0.1, 0.1, 0.4, 0.3, 0.1]$. We assume that the users are static. Figure 5(a) shows the long-term user temporal shares $A_Q^i, t \in [5]$ and the user thresholds. It can be seen that the temporal demand constraints are satisfied. Also, the thresholds satisfy the optimality conditions discussed in Corollary 3. Figure 5(b) shows the evolution of the thresholds in different iterations of Algorithm 2.

In Figure 6, we consider the previous scenario with mobile users. We model the mobility of the users by a two-dimensional random walk where each user takes one step per time-slot in a direction θ uniformly distributed in $[0, 2\pi]$. Furthermore, we assume that the speed of the user at each step is randomly distributed between 1 m/s and 10 m/s. It is also assumed that the users do not exit the cell. In this scenario, the performance vector R^m is not stationary and $A_i^Q(\lambda^n)$ is time-varying. Therefore, the optimal thresholds change over time. Figure 6(a) shows the long-term temporal share of the users and the evolution of the thresholds in time. It can be seen that the thresholds track the variation of the system and the desired temporal demand constraints are satisfied. Figure 6(b) shows the evolution of the users' thresholds as the iterative algorithm proceeds. It can be observed that

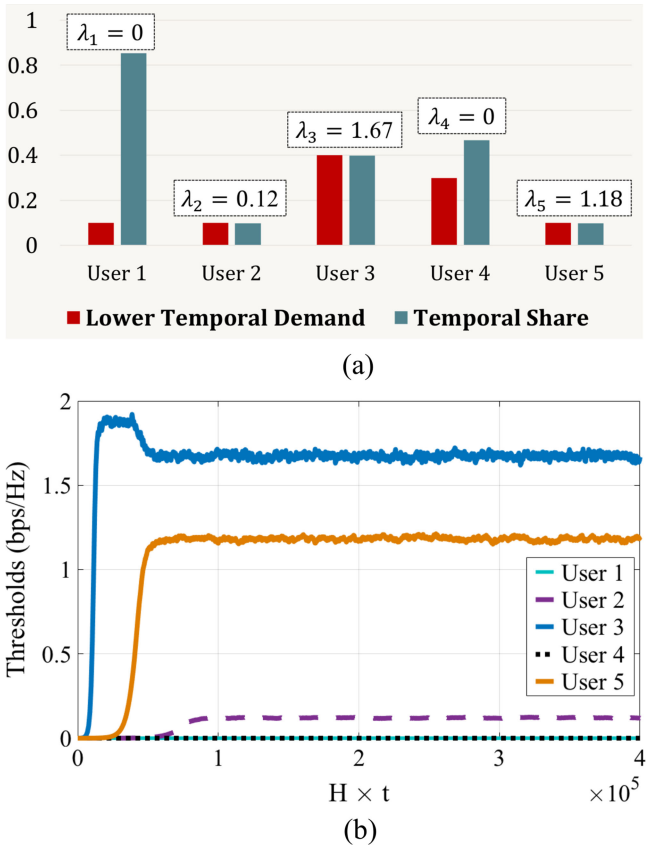

Fig. 5. (a) Long-term temporal share and the lower temporal demands of the static users. (b) The evolution of scheduling thresholds in Algorithm 2. The horizontal axis is the sampled time-slot index, where the sampling parameter H is set to 0.1.

the thresholds for users 1, 2, 4 and 5 are close to zero throughout the iterative process, whereas the threshold for user 3 increases to approximately 4 bps/Hz in a small fraction of the time-slots and fluctuates in the vicinity of 4 bps/Hz afterwards.

C. Discrete Performance Vectors

In this section, we consider a NOMA scenario with two users and discrete performance variables and discuss the effectiveness of the method described in Section VI. Due to the small number of virtual users in this scenario, we are able to find the optimal thresholds and tie-breaking decision analytically. We also use the perturbation method in Section VI to construct an ℓ-PTBS and compare the resulting performance with the optimal utility. It is shown that the utility from the method proposed in Section VI converges to the optimum utility as $\ell \to \infty$. Consider a two-user scenario where the performance values are independent discrete random variables distributed as follows:

$$R_1 = \begin{cases} 0.1 \text{ w.p. } 0.5 \\ 0.2 \text{ w.p. } 0.5 \end{cases}, \qquad R_2 = \begin{cases} 0.2 \text{ w.p. } 0.5 \\ 0.3 \text{ w.p. } 0.5 \end{cases},$$

$$R_{1,2} = \begin{cases} 0.1 \text{ w.p. } 0.75 \\ 0.4 \text{ w.p. } 0.25 \end{cases}.$$

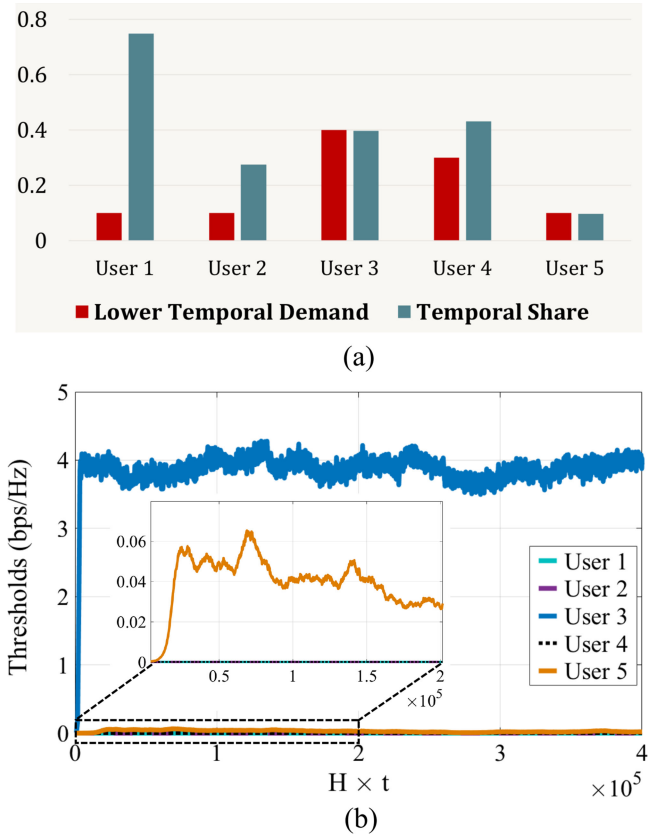

Fig. 6. (a) Long-term temporal share of the users in a mobile scenario. (b) The evolution of scheduling thresholds in time. The sampling parameter H is set to 0.1.

TABLE III
OPTIMAL TBS WITH DISCRETE PERFORMANCE VALUES

R^3	$(0.1, 0.2, 0.1)$	$(0.1, 0.2, 0.4)$	$(0.1, 0.3, 0.1)$	$(0.1, 0.3, 0.4)$
S^3	$(0.2, 0.2, 0.1)$	$(0.2, 0.2, 0.4)$	$(0.2, 0.3, 0.1)$	$(0.2, 0.3, 0.4)$
$Q(R^3)$	*tie*	$\mathcal{V}_{1,2}$	$\mathcal{V}_2$	$\mathcal{V}_{1,2}$
R^3	$(0.2, 0.2, 0.1)$	$(0.2, 0.2, 0.4)$	$(0.2, 0.3, 0.1)$	$(0.2, 0.3, 0.4)$
S^3	$(0.3, 0.2, 0.1)$	$(0.3, 0.2, 0.4)$	$(0.3, 0.3, 0.1)$	$(0.3, 0.3, 0.4)$
$Q(R^3)$	$\mathcal{V}_1$	$\mathcal{V}_{1,2}$	*tie*	$\mathcal{V}_{1,2}$

Let $\underline{w}_1 = 0.5, \underline{w}_2 = 0.25$. We first find the optimal thresholds and tie-breaking probability distributions analytically assuming that the channel statistics are known. For $\lambda_1 = \lambda_2 = 0$, we have $A_1^Q \leq \frac{7}{16}$. Therefore, λ_1 must be positive in order to satisfy the temporal demand of user u_1. Take λ_1 to 0.1, Table III lists all of the possible values for the scheduling measures vector S^3 and the choice of the active user. Note that a tie happens when $R^3 = (0.1, 0.2, 0.1)$ and $R^3 = (0.2, 0.3, 0.1)$. In the former, the tie happens among all three virtual users whereas in the latter, the tie is between $\mathcal{V}_1$ and $\mathcal{V}_2$. Let $p^3 = (p_1, p_2, p_{1,2})$ denote the tie-breaking distribution. It can be shown that an optimum tie-breaking distribution is $p^3 = (\frac{1}{3}, \frac{2}{3}, 0)$ when $R^3 = (0.1, 0.2, 0.1)$ and $p^3 = (0, 1, 0)$ when $R^3 = (0.2, 0.3, 0.1)$ by checking the sufficient conditions in Corollary 3. This gives

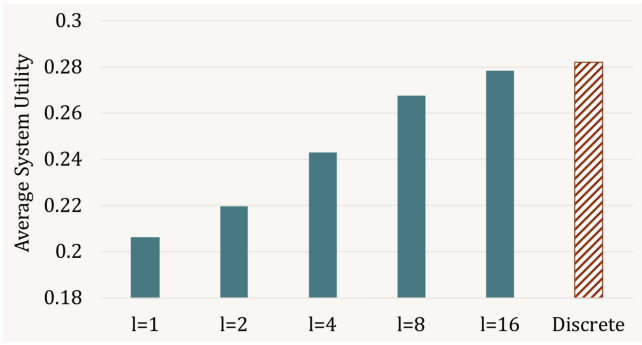

Fig. 7. Average system utility for the optimal strategy (tiled red) and the proposed method (filled green). The parameter ℓ determines the variance of the perturbation noise which affects the discrete utility vector in the proposed method.

$A_1^Q = 0.5$ and $A_2^Q = 0.75$ which satisfy the optimality constraints described in Corollary 3. As a result, the optimal average system utility is $\frac{45}{160} \approx 0.281$. To evaluate the method proposed in Section VI, we add a vector of independent random variables with distribution $Unif[-1/\ell, 1/\ell]$ to the performance vector and use the perturbed performance values as an input to the TBS. We consider $\ell \in \{1, 2, 4, 8, 16\}$ and use Algorithm 2 to obtain the optimal TBS for each value of ℓ. Figure 7 shows the average system utility for different values of ℓ as well as for the strategy with optimal thresholds and tie-breaking distributions mentioned above. It can be seen that the average system utility converges to the optimal value as ℓ goes to infinity.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have considered scheduling for NOMA systems under temporal demand constraints. We have shown that TBSs achieve optimal system utility and any optimal strategy is equivalent to a TBS. We have proposed a variable elimination method to find the feasible temporal share region for a given NOMA system. We have introduced an iterative algorithm based on the Robbins Monro method which finds the optimal thresholds for the TBS given the user utilities. The algorithm does not require knowledge of the users' channel statistics. Rather, it has access to the channel realizations at each time-slot. Lastly, we have provided numerical simulations to validate the proposed approach.

A natural extension to this work is multi-cell scheduling in NOMA systems. The methods proposed here may be extended and applied to centralized and distributed NOMA systems. Particularly, scheduling for multi-cell NOMA systems with limited cooperation is an interesting avenue for future work.

Another direction for future research is NOMA scheduling under short-term fairness constraints. The problem is of interest in delay sensitive applications. Short-term fairness may significantly affect the design of NOMA schedulers. It remains to be seen whether variations of TBSs can achieve near-optimal performance under short-term fairness constraints.

APPENDIX

A. Proof of Lemma 1

Let $\widetilde{Q}$ be a memoryless and stationary scheduling strategy. Since strategy $\widetilde{Q}$ is memoryless, $Q_t, t \in \mathbb{N}$ is only a function of the realization of performance vector R^m at time t. Due to stationarity, the random variables $\mathbb{1}_{\left\{u_i \in \widetilde{Q}_t(R^{m\times t})\right\}}$ are independent and identically distributed (i.i.d.). From the strong law of large numbers we have:

$$\lim_{t\to\infty} A_{i,t}^{\widetilde{Q}} \overset{a.s.}{=} \mathbb{E}\left(\mathbb{1}_{\left\{u_i \in \widetilde{Q}_t(R^{m\times t})\right\}}\right) \overset{(a)}{=} Pr\Big(u_i \in \widetilde{Q}_t(R^m)\Big), \tag{18}$$

where (a) follows from $\mathbb{E}(\mathbb{1}_{\mathcal{A}}) = Pr(\mathcal{A})$ for any event $\mathcal{A}$. Similarly, the random variables $X_t \triangleq \sum_{j=1}^{m} R_{j,t}\mathbb{1}_{\left\{\widetilde{Q}_t(R^{m\times t})=\mathcal{V}_j\right\}}$ are i.i.d.. Hence, from the strong law of large numbers we have:

$$\lim_{t\to\infty} U_t^{\widetilde{Q}} \overset{a.s.}{=} \sum_{j=1}^{m} \mathbb{E}\left(R_j \mathbb{1}_{\left\{\widetilde{Q}_t(R^m)=\mathcal{V}_j\right\}}\right). \tag{19}$$

B. Proof of Theorem 1

Case i) $w^n = \underline{w}^n = \overline{w}^n, N_{\max} = n$

As an intermediate step, we consider the special case of the scheduling problem when the temporal demand constraints must be satisfied with equality, and all subset of virtual users can be activated, i.e. $\mathsf{V} = 2^{\mathcal{U}}$. It turns out that the inclusion of the joint virtual user greatly simplifies the analysis of temporally fair schedulers.

First, we prove that if a threshold strategy exists which i) satisfies the temporal constraints, and ii) for which $\lambda_i \in [-2M, 2M], \forall i \in [n]$, then it is optimal, where M is defined in Remark 1. Fix $\epsilon > 0$. Let $\epsilon' = 2nM\epsilon$. Let $\widehat{Q} \in \mathcal{Q}_{TBS}$ be a TBS characterized by the threshold vector $\lambda^n \in [-2M, 2M]^n$ and let Q be an arbitrary scheduling strategy. From Equation (4) we know that $|A_i^Q - w_i| \le \epsilon, \forall i \in [n]$. Also, by assumption, $\lambda_i \le M, \forall i \in [n]$. As a result, $\lambda_i(A_i^Q - w_i) + \frac{\epsilon'}{n} \ge 0, \forall i \in [n]$. We have,

$$\begin{aligned}
U^Q &\le U^Q + \sum_{i=1}^{n}\Big(\lambda_i(A_i^Q - w_i)\Big) + \epsilon' \\
&\le \liminf_{t\to\infty}\left[\frac{1}{t}\sum_{k=1}^{t}\sum_{j=1}^{m}\left(R_{j,k}\mathbb{1}_{\left\{Q_k(R^{m\times k})=\mathcal{V}_j\right\}}\right)\right] \\
&\quad + \sum_{i=1}^{n}\lambda_i \cdot \liminf_{t\to\infty}\frac{1}{t}\left[\sum_{k=1}^{t}\left(\mathbb{1}_{\left\{u_i \in Q_k(R^{m\times k})\right\}}\right)\right] \\
&\quad - \sum_{i=1}^{n}\lambda_i w_i + \epsilon' \\
&\overset{(a)}{\le} \liminf_{t\to\infty}\frac{1}{t}\sum_{k=1}^{t}\left[\sum_{j=1}^{m}\left(R_{j,k}\mathbb{1}_{\left\{Q_k(R^{m\times k})=\mathcal{V}_j\right\}}\right)\right. \\
&\quad \left. + \sum_{i=1}^{n}\left(\lambda_i \mathbb{1}_{\{u_i \in Q_k(R^{m\times k})\}}\right)\right] - \sum_{i=1}^{n}\lambda_i w_i + \epsilon' \\
&= \liminf_{t\to\infty}\frac{1}{t}\left[\sum_{k=1}^{t}\sum_{j=1}^{m}\Big((R_{j,k}\right. \\
&\quad \left. + \sum_{i=1}^{n}\lambda_i \mathbb{1}_{\{u_i\in\mathcal{V}_j\}})\mathbb{1}_{\{Q_k(R^{m\times k})=\mathcal{V}_j\}}\Big)\right] \\
&\quad - \sum_{i=1}^{N}\lambda_i w_i + \epsilon' \\
&\overset{(b)}{\le} \liminf_{t\to\infty}\frac{1}{t} \\
&\quad \left[\sum_{k=1}^{t}\sum_{j=1}^{m}\left(\left(R_{j,k} + \sum_{i=1}^{n}\lambda_i\mathbb{1}_{\{u_i\in\mathcal{V}_j\}}\right)\mathbb{1}_{\left\{\widehat{Q}_k(R^{m\times k})=\mathcal{V}_j\right\}}\right)\right] \\
&\quad - \sum_{i=1}^{n}\lambda_i w_i + \epsilon' \\
&\overset{(c)}{=} \liminf_{t\to\infty}\left[\frac{1}{t}\sum_{k=1}^{t}\sum_{j=1}^{m}\left(R_{j,k}\mathbb{1}_{\left\{\widehat{Q}_k(R^{m\times k})=\mathcal{V}_j\right\}}\right)\right] \\
&\quad + \sum_{i=1}^{n}\liminf_{t\to\infty}\frac{1}{t}\left[\sum_{k=1}^{t}\left(\lambda_i\mathbb{1}_{\left\{u_i\in\widehat{Q}_k(R^{m\times k})\right\}}\right)\right] \\
&\quad - \sum_{i=1}^{n}\lambda_i w_i + \epsilon' \\
&\le U^{\widehat{Q}} + \overbrace{\sum_{i=1}^{n}\Big(\lambda_i(A_i^{\widehat{Q}} - w_i)\Big)}^{\le\epsilon'} + \epsilon' = U^{\widehat{Q}} + 2\epsilon',
\end{aligned}$$

where (a) holds since limit inferior satisfies supper-additivity, (b) holds due to the rearrangement inequality, and finally, (c) follows from the existence of the limit inferior. As a result:

$$U^Q \le U^{\widehat{Q}} + 2\epsilon', \forall\epsilon > 0, \Rightarrow U^Q \le U^{\widehat{Q}},$$

where equality holds if and only if all of the inequalities above are equalities. Particularly, equality in (b) requires that Q be equivalent with $\widehat{Q}$.

So far, we have shown that if there exists $\widehat{Q} \in \mathcal{Q}_{TBS}$ is a non-empty set, with $\lambda^n \in [-2M, 2M]^n$, then, any optimal strategy is equivalent to a threshold based strategy. In the next step, we show that at least one such $\widehat{Q}$ exists. To this end, we consider two sub-cases as follows:

Case i.1) $\sum_{i\in[n]} w_i = 1$

In this case, we show that a threshold based strategy with $\lambda_i \in [-2M, -M], \forall i \in [n]$ exists. Note that if $\lambda_i \le -M, \forall i \in [n]$, then only the individual users (i.e. $\mathcal{V}_i = \{u_i\}, i \in [n]$) will be chosen by the threshold strategy. The reason is that the scheduling measures for the individual users are larger than that of joint users with probability one due to Remark 1. Furthermore, from [19], it is known that when individual users are chosen, one can find a set of thresholds such that $A_i^Q = w_i$ with probability one for $\sum_{i\in[n]} w_i = 1$. This shows the existence of suitable thresholds in Case i.1.

Case i.2) $\sum_{i\in[n]} w_i > 1$

To prove existence in this case, we use the following n-dimensional extension of the intermediate value theorem.

Lemma 3 (Poincaré-Miranda [34]): Let $n \in \mathbb{N}$. Consider the set of continuous functions $f_i : \mathbb{R}^n \to \mathbb{R}, i \in [n]$. Assume that for each function $f_i, i \in [n]$, there exists positive reals M_i^+ and M_i^-, such that $f_i(x^n) > 0$ if $x_i = M_i^+$ and $f_i(x^n) < 0$ if $x_i = M_i^-$. Then, the function $f^n = (f_1, f_2, \ldots, f_n)$ has a root in the n-dimensional cube $\prod_{i=1}^n [-M_i^-, M_i^+]$. Alternatively:

$$\exists x_1^*, \ldots, x_n^* \in \prod_{i=1}^{n} [-M_i^-, M_i^+] : f_i(x_1^*, \ldots, x_n^*) = 0, \forall i \in [n].$$

We provide the proof when $0 < w_i < 1, i \in [n]$. Take $f_i(\lambda^n) \triangleq A_i^{Q_{TBS}} - w_i, \forall i \in [n]$. Then, f_i are continuous functions of λ^n. Next, we find a set of thresholds $(M_i^+, M_i^-), i \in [n]$ satisfying the conditions of Lemma 3. Note that if $\lambda_i = M$, $u_i \in Q_{TBS}(R^n)$ with probability one. To see this, let $\mathcal{V}_j$ be a virtual user such that $u_i \notin \mathcal{V}_j$ and let $\mathcal{V}_j' = \mathcal{V}_j \cup \{u_i\}$. Then,

$$\begin{aligned}
&P(S(\mathcal{V}_j, R_{j,t}) \le S(\mathcal{V}_j', R_{j,t})) \\
&= P\left(R_{j,t} + \sum_{i=1}^{n} \lambda_i \mathbb{1}_{\{u_i \in \mathcal{V}_j\}} \le R_{j',t} + \sum_{i=1}^{n} \lambda_i \mathbb{1}_{\{u_i \in \mathcal{V}_j\}} + M\right) \\
&= P(R_{j,t} - R_{j',t} \le M) = 1,
\end{aligned}$$

where the last equality follow from Remark 1. As a result, $A_i^{Q_{TBS}} - w_i = 1 - w_i > 0$. Hence, $M_i^+ = M$ satisfies the conditions of Lemma 3. Next, we construct $M_i^-, i \in [n]$. Note that by assumption $e \triangleq \frac{\sum_{i\in[n]} w_i - 1}{n} > 0$. Furthermore, it is straightforward to show that there exists $\alpha^n > 0$ such that $\sum_{i\in[n]} \alpha_i = 1$ and $w_i - \alpha_i e > 0, i \in [n]$. Define $w_i' = w_i - \alpha_i e, i \in [n]$. Then, by construction, $\sum_{i\in[n]} w_i' = 1$. By similar arguments as in the case i.1, for any fixed $i \in [n]$, there exists $\lambda_i \in [-2M, -M]$ such that $A_i^Q = w_i' < w_i$. So, $A_i^Q - w_i' < 0$. Consequently, $M_i^- = \lambda_i$ satisfies the condition that $f_i(\lambda^n) < 0, \lambda_i = M_i^-, \forall i \in [n]$. By Lemma 3, there exists λ^n such that $A_i^Q = w_i, i \in [n]$ simultaneously.

Case ii) $\underline{w}^n < \overline{w}^n$ or $N_{\max} < n$

The proof is broken into two subcases $w^n = \underline{w}^n = \overline{w}^n, N_{\max} < n$ and $\underline{w}^n \neq \overline{w}^n, N_{\max} \le n$, and follows by similar arguments as Case i). The complete proof is provided in [42].

C. Proof of Theorem 3

Condition (4) follows from the properties of the Harmonic series. We provide the proof for condition (2). We showed in Theorem 1 that the optimal threshold vector λ^{*n} exists. Let ϵ^n be an arbitrary vector of real numbers. Define b_i^* and $b_i, i \in [n]$ as the resulting temporal shares for the optimal TBS with threshold vector λ^{*n} and the temporal shares for $Q_{TBS}(\lambda^n)$, respectively, where $\lambda^n = \lambda^{*n} + \epsilon^n$. Let $\mathcal{A}_j^*$ and $\mathcal{A}_j, j \in [m]$ be the event that virtual user j is activated at a given time-slot by $Q_{TBS}(\lambda^{*n})$ and $Q_{TBS}(\lambda^n)$, respectively. We need to show that:

$$(\epsilon^n)^T (b^{*n} - b^n) > 0, \tag{20}$$

where $b_i^* = \sum_{j:u_i\in\mathcal{V}_j} P(\mathcal{A}_j^*)$, and $b_i = \sum_{j:u_i\in\mathcal{V}_j} P(\mathcal{A}_j)$. Equation (20) can be written as:

$$\sum_{i\in[n]} \epsilon_i (b_i^* - b_i) > 0. \tag{21}$$

Note that by the law of total probability

$$b_i^* = \sum_{k\in[m]} \sum_{j:u_i\in\mathcal{V}_j} P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right),$$

$$b_i = \sum_{k\in[m]} \sum_{j:u_i\in\mathcal{V}_j} P\left(\mathcal{A}_j \bigcap \mathcal{A}_k^*\right).$$

As a result, we need to show that

$$\begin{aligned}
&\sum_{i\in[n]} \epsilon_i \Bigg(\sum_{k\in[m]} \sum_{j:u_i\in\mathcal{V}_j} P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) \\
&\quad - \sum_{k\in[m]} \sum_{j:u_i\in\mathcal{V}_j} P\left(\mathcal{A}_j \bigcap \mathcal{A}_k^*\right) \Bigg) > 0 \\
&\Leftrightarrow \sum_{k\in[m]} \sum_{i\in[n]} \sum_{j:u_i\in\mathcal{V}_j} \epsilon_i \left(P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) - P\left(\mathcal{A}_j \bigcap \mathcal{A}_k^*\right)\right) > 0 \\
&\Leftrightarrow \sum_{k\in[m]} \sum_{j\in[m]} \sum_{i:u_i\in\mathcal{V}_j} \epsilon_i \left(P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) - P\left(\mathcal{A}_j \bigcap \mathcal{A}_k^*\right)\right) > 0 \\
&\Leftrightarrow \sum_{k\in[m]} \sum_{j\in[m]} P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) \left(\sum_{i:u_i\in\mathcal{V}_j} \epsilon_i\right) \\
&\quad - \sum_{k\in[m]} \sum_{j\in[m]} P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) \left(\sum_{i:u_i\in\mathcal{V}_k} \epsilon_i\right) > 0.
\end{aligned}$$

Let $e_j = \sum_{i:u_i\in\mathcal{V}_j} \epsilon_i, j \in [m]$. Note that e_j is the perturbation of the scheduling measure of the virtual user j defined in Definition 9 resulting from changing λ^{*n} to λ^n. In fact the scheduling measure can be written as $S(\mathcal{V}_j, R_j) = R_j + \sum_{i:u_i\in\mathcal{V}_j} \lambda_i^* + e_j$. We need to show that:

$$\begin{aligned}
&\sum_{k\in[m]} \sum_{j\in[m]} e_j P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) - \sum_{k\in[m]} \sum_{j\in[m]} e_k P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) > 0 \\
&\Leftrightarrow \sum_{k\in[m]} \sum_{j\in[m]} (e_j - e_k) \left(P\left(\mathcal{A}_j^* \bigcap \mathcal{A}_k\right) - P\left(\mathcal{A}_k^* \bigcap \mathcal{A}_j\right)\right) > 0
\end{aligned}$$

We claim that $e_j - e_k$ and $P(\mathcal{A}_j^* \bigcap \mathcal{A}_k) - P(\mathcal{A}_k^* \bigcap \mathcal{A}_j)$ have the same sign for all $j, k \in [m]$. To see this, note that if $e_j > e_k$ then the threshold for virtual user j is increased more than that of virtual user k after perturbing λ^{*n} by ϵ^n. As a result, it can be shown that $P(\mathcal{A}_j^* \bigcap \mathcal{A}_k) > P(\mathcal{A}_k^* \bigcap \mathcal{A}_j)$. Roughly speaking, this can be interpreted as follows: if the threshold for virtual user j is increased more than that of virtual user k, then its temporal share increases more than that of k as well. A similar argument can be provided for $e_j < e_k$.

D. Proof of Lemma 2

Fix the pair of vectors of temporal demands $(\underline{w}^n.\overline{w}^n)$ and $(\underline{w}'^n, \overline{w}'^n)$ and $\alpha \in [0, 1]$. We need to show the following

inequality $U^*_{\underline{w}''^n,\overline{w}''^n} \geq \alpha U^*_{\underline{w}^n,\overline{w}^n} + (1-\alpha)U^*_{\underline{w}'^n,\overline{w}'^n}$, where $\underline{w}''^n = \alpha\underline{w}^n + (1-\alpha)\underline{w}'^n$ and $\overline{w}''^n = \alpha\overline{w}^n + (1-\alpha)\overline{w}'^n$. Let Q_{TBS} be the optimal strategy for the temporal constraints $(\underline{w}^n.\overline{w}^n)$. Also, let ${Q'}_{TBS}$ be the optimal strategy for the temporal constraints $(\underline{w}'^n, \overline{w}'^n)$. Define the strategy Q'' as follows: for α fraction of the time-slots, the strategy chooses the active user based on Q_{TBS} and for $(1-\alpha)$ fraction of the time it uses ${Q'}_{TBS}$ to choose the active user. It is straightforward to verify that the resulting temporal shares are between $(\underline{w}''^n, \overline{w}''^n)$. Furthermore, the resulting utility from Q'' is $U'' = \alpha U^*_{\underline{w}^n,\overline{w}^n} + (1-\alpha)U^*_{\underline{w}'^n,\overline{w}'^n}$. By definition we have $U'' \leq U^*_{\underline{w}''^n,\overline{w}''^n}$. This completes the proof.

E. Proof of Theorem 4

We provide a sketch of the proof. Let U^* ($U^*_{1/\ell}$) be the optimal strategy for the setup Ω_0 ($\Omega_{1/\ell}$) achieved using the strategy Q^* ($Q^*_{1/\ell}$). Furthermore, let $U_{1/\ell}$ be the utility due to applying the ℓ-PTBS $\widehat{Q}_{1/\ell}$ to Ω_0. We need to show that the sequence $U_{1/\ell}$ converges to U^* in probability as $\ell \to \infty$. The sequence $U_{1/\ell}$ is upper-bounded by U^* by definition of U^*. Consequently, to prove Theorem 4, it is enough to show that $P(U^* \leq U_{1/\ell} + \frac{2}{\ell}) = 1$. In order to prove the last equality we consider an intermediate *genie-assisted* strategy $\widetilde{Q}_{1/\ell}$ for the setup $\Omega_{1/\ell}$. The strategy uses the output of Q^* as side-information assuming that the output is provided using a genie. More precisely, at time-slot t the strategy $\widetilde{Q}_{1/\ell}$ for $\Omega_{1/\ell}$ activates the same virtual user $\mathcal{V}_j$ which the strategy Q^* activates for Ω_0. Let $\widetilde{U}_{1/\ell}$ be the average utility of $\widetilde{Q}_{1/\ell}$. Then, $U^* \leq \widetilde{U}_{1/\ell} + \frac{1}{\ell}$ with probability one. The reason is that the two strategies activate the same virtual users and the utility in Ω_0 and $\Omega_{1/\ell}$ differ in a $Unif[-1/\ell, 1/\ell]$ variable for any given virtual user. On the other hand, using the rearrangement inequality as in the proof of Theorem 1, it can be shown that $P(\widetilde{U}_{1/\ell} \leq U^*_{1/\ell}) = 1$. Furthermore, $U^*_{1/\ell} \leq U_{1/\ell} + \frac{1}{\ell}$ by similar arguments. As a result,

$$P\left(U^* \leq U_{1/\ell} + \frac{2}{\ell}\right) \geq P\left(U^* \leq U^*_{1/\ell} + \frac{1}{\ell}\right)$$
$$\geq P\left(U^* \leq \widetilde{U}_{1/\ell} + \frac{1}{\ell}\right) = 1 \Rightarrow P\left(U^* \leq U_{1/\ell} + \frac{2}{\ell}\right) = 1.$$

The proof is completed by taking ℓ to infinity.

ACKNOWLEDGMENT

The authors would like to thank Dr. Mohammad A. Khojastepour from NEC Laboratories America for his constructive comments.

REFERENCES

[1] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surv. Tut.*, vol. 20, no. 3, pp. 2294–2323, Thirdquarter 2018.

[2] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *Proc. IEEE 24th Int. Symp. Pers. Indoor Mobile Radio Commun.*, 2013, pp. 611–615.

[3] Z. Ding *et al.*, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[4] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," 2017, arXiv:1706.05347.

[5] K. Seong, M. Mohseni, and J. M. Cioffi, "Optimal resource allocation for OFDMA downlink systems," in *Proc. IEEE Int. Symp. Inf. Theory*, 2006, pp. 1394–1398.

[6] Z. Ding, R. Schober, and H. V. Poor, "A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4438–4454, Jun. 2016.

[7] N. Otao, Y. Kishiyama, and K. Higuchi, "Performance of non-orthogonal access with SIC in cellular downlink using proportional fair-based resource allocation," in *Proc. Int. Symp. Wireless Commun. Syst.*, 2012, pp. 476–480.

[8] S. M. R. Islam, M. Zeng, O. A. Dobre, and K. S. Kwak, "Resource allocation for downlink NOMA systems: Key techniques and open issues," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 40–47, Apr. 2018.

[9] W. Yu and J. M. Cioffi, "Sum capacity of Gaussian vector broadcast channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1875–1892, Sep. 2004.

[10] L. Lei, D. Yuan, C. K. Ho, and S. Sun, "Power and channel allocation for non-orthogonal multiple access in 5G systems: Tractability and computation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8580–8594, Dec. 2016.

[11] Y. Liu, M. Elkashlan, Z. Ding, and G. K. Karagiannidis, "Fairness of user clustering in MIMO non-orthogonal multiple access systems," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1465–1468, Jul. 2016.

[12] Z. Yang, Z. Ding, P. Fan, and N. Al-Dhahir, "A general power allocation scheme to guarantee quality of service in downlink and uplink NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7244–7257, Nov. 2016.

[13] J. Cui, Y. Liu, Z. Ding, P. Fan, and A. Nallanathan, "Optimal user scheduling and power allocation for millimeter wave NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1502–1517, Mar. 2018.

[14] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE 77th Veh. Technol. Conf.*, 2013, pp. 1–5.

[15] X. Liu, E. K. Chong, and N. B. Shroff, "A framework for opportunistic scheduling in wireless networks," *Elsevier Comput. Netw.*, vol. 41, no. 4, pp. 451–474, 2003.

[16] Z. Zhang, Y. He, and E. K. Chong, "Opportunistic scheduling for OFDM systems with fairness constraints," *EURASIP J. Wireless Commun. Netw.*, vol. 2008, 2008, Art. no. 25.

[17] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: Shadow prices, proportional fairness and stability," *J. Oper. Res. Soc.*, vol. 49, no. 3, pp. 237–252, 1998.

[18] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1277–1294, Jun. 2002.

[19] X. Liu, E. K. P. Chong, and N. B. Shroff, "Opportunistic transmission scheduling with resource-sharing constraints in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 19, no. 10, pp. 2053–2064, Oct. 2001.

[20] S. S. Kulkarni and C. Rosenberg, "Opportunistic scheduling for wireless systems with multiple interfaces and multiple constraints," in *Proc. ACM Int. Workshop Model. Anal. Simul. Wireless Mobile Syst.*, 2003, pp. 11–19.

[21] T. Issariyakul and E. Hossain, "Throughput and temporal fairness optimization in a multi-rate TDMA wireless network," in *Proc. IEEE Int. Conf. Commun.*, vol. 7, 2004, pp. 4118–4122.

[22] A. Asadi and V. Mancuso, "A survey on opportunistic scheduling in wireless communications," *IEEE Commun. Surv. Tut.*, vol. 15, no. 4, pp. 1671–1688, Fourth Quarter 2013.

[23] G. Tan and J. V. Guttag, "Time-based fairness improves performance in multi-rate WLANs," in *Proc. USENIX Annu. Tech. Conf., General Track*, 2004, pp. 269–282.

[24] T. Joshi, A. Mukherjee, Y. Yoo, and D. P. Agrawal, "Airtime fairness for IEEE 802.11 multirate networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 4, pp. 513–527, Apr. 2008.

[25] S. Shahsavari and N. Akar, "A two-level temporal fair scheduler for multi-cell wireless networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 3, pp. 269–272, Jun. 2015.

[26] S. Shahsavari, N. Akar, and B. H. Khalaj, "Joint cell muting and user scheduling in multicell networks with temporal fairness," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art. no. 4846291.

[27] Z. Wei, D. W. K. Ng, and J. Yuan, "Power-efficient resource allocation for MC-NOMA with statistical channel state information," in *Proc. IEEE Global Commun. Conf.*, 2016, pp. 1–7.
[28] W. Liang, Z. Ding, Y. Li, and L. Song, "User pairing for downlink non-orthogonal multiple access networks using matching algorithm," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5319–5332, Dec. 2017.
[29] X. Chen, A. Benjebbour, A. Li, and A. Harada, "Multi-user proportional fair scheduling for uplink non-orthogonal multiple access (NOMA)," in *Proc. 79th IEEE Veh. Technol. Conf.*, 2014, pp. 1–5.
[30] T. S. Rappaport, *et al.*, *Wireless Commun.: Principles and Practice*, vol. 2. NJ, USA: Prentice Hall, 1996.
[31] S. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 721–742, Secondquarter 2017.
[32] P. Bergmans, "A simple converse for broadcast channels with additive white Gaussian noise (corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 2, pp. 279–280, Mar. 1974.
[33] B. Hassibi and M. Sharif, "Fundamental limits in MIMO broadcast channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 7, pp. 1333–1344, Sep. 2007.
[34] W. Kulpa, "The Poincaré-Miranda theorem," *Amer. Math. Monthly*, vol. 104, pp. 545–550, 1997.
[35] X. Allamigeon, U. Fahrenberg, S. Gaubert, R. D. Katz, and A. Legay, "Tropical Fourier-Motzkin elimination, with an application to real-time verification," *Int. J. Algebra Comput.*, vol. 24, no. 05, pp. 569–607, 2014.
[36] F. S. Chaharsooghi, M. J. Emadi, M. Zamanighomi, and M. R. Aref, "A new method for variable elimination in systems of inequations," in *Proc. IEEE Int. Symp. Inf. Theory*, 2011, pp. 1215–1219.
[37] R. Koch, "Affine monoids, Hilbert bases and Hilbert functions," Department of Mathematics / Computer Science, Ph.D. dissertation, Osnabrück University, Osnabrück, Germany, 2003.
[38] H. Robbins and S. Monro, "A stochastic approximation method," *Ann. Math. Statist.*, vol. 22, pp. 400–407, 1951.
[39] D. Ruppert, "A Newton-Raphson version of the multivariate robbins-monro procedure," *Ann. Statist.*, vol. 13, pp. 236–245, 1985.
[40] D. P. Bertsekas, *Nonlinear Programming*. Belmont, MA, USA: Athena scientific, 2016.
[41] 3GPP, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (TS 36.213 version 12.4.0 release 12)," European TeleCommunications Standards Institute, Sophia Antipolis, France, Rep. No. RTS/TSGR-0136213vc40, 2015.
[42] S. Shahsavari, F. Shirani, and E. Erkip, "A general framework for temporal fair user scheduling in NOMA systems," 2018, arXiv:1809.06431.

Shahram Shahsavari received the B.S. degree in electrical engineering from the Amirkabir University of Technology (Tehran Polytechnic), Iran, in 2013, and the M.S. degree in electrical engineering from the Sharif University of Technology, Iran, in 2015. He received the Ph.D. degree in electrical engineering from the New York University Tandon School of Engineering, NY, USA, in 2019. He is also with NYU WIRELESS Center at New York University conducting research on next generation wireless networks. His research interests include wireless communications, modern cellular systems, radio resource management, and network optimization. Dr. Shahsavari was the recipient of NYU Ernst Weber fellowship in 2015.

Farhad Shirani received the B.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2011, and the M.Sc. and Ph.D. degrees from the University of Michigan, Ann Arbor, MI, USA, in 2016. He also received the M.Sc. degree in mathematics from the University of Michigan in 2016. He served as a Lecturer and Postdoctoral Research Fellow with the University of Michigan in 2017. Currently, he is a Research Assistant Professor with the New York University at New York, NY, USA. His recent works include developing information theoretic methods for analysis of fundamental limits of web privacy, design of receiver architectures for energy efficient communication over MIMO systems, and design of algorithms for opportunistic multi-user scheduling under various fairness constraints. His research interests include privacy and security, wireless communications, and multi-terminal communication systems.

Elza Erkip received the B.S. degree in electrical and electronics engineering from Middle East Technical University, Ankara, Turkey, and the M.S. and the Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, USA. She is an Institute Professor with the Electrical and Computer Engineering Department at the New York University Tandon School of Engineering, NY, USA. Her research interests are in information theory, communication theory, and wireless communications.

Dr. Erkip is a member of the Science Academy of Turkey and is a Clarivate Highly Cited Researcher. She was the recipient of the NSF CAREER Award in 2001, the IEEE Communications Society WICE Outstanding Achievement Award in 2016, and the IEEE Communications Society Communication Theory Technical Committee (CTTC) Technical Achievement Award in 2018. Her paper awards include the IEEE Communications Society Stephen O. Rice Paper Prize in 2004, and the IEEE Communications Society Award for Advances in Communication in 2013. She has been a member of the Board of Governors of the IEEE Information Theory Society since 2012 where in 2018, she was the Society President. She was a Distinguished Lecturer of the IEEE Information Theory Society from 2013 to 2014.

She has had many editorial and conference organization responsibilities. Some recent ones include Asilomar Conference on Signals, Systems and Computers, MIMO Communications and Signal Processing Track Chair in 2017, IEEE Wireless Communications and Networking Conference Technical Co-Chair in 2017, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Guest Editor in 2015, and IEEE International Symposium of Information Theory General Co-Chair in 2013.

A Concentration of Measure Approach to Correlated Graph Matching

Farhad Shirani, Siddharth Garg, and Elza Erkip
Electrical and Computer Engineering Department
New York University, NY, USA

Abstract

The graph matching problem emerges naturally in various applications such as privacy, image processing and computational biology. In this paper graph matching is considered under a stochastic model, where a pair of randomly generated graphs with pairwise correlated edges are to be matched with each other. More precisely, given the labeling of the vertices in the first graph, the objective is to recover the labels in the second graph by leveraging the correlation among their edges. The problem is considered under various settings and graph models. In the first step, the Correlated Erdös-Rényi (CER) graph model is considered, where all edge pairs whose vertices have similar labels are generated based on identical distributions and independently of other edges. A matching scheme called the Typicality Matching Scheme is introduced. The scheme operates by investigating the joint typicality of the adjacency matrices of the two graphs. Necessary and sufficient conditions for successful matching are derived based on the parameters of the CER model. In the next step, the results are extended to graph matching in the presence of Community Structure (CS). The CS model is a generalization of the ER model where each vertex in the graph is associated with a community label, which affects its edge statistics. The results are further extended to matching of ensembles of more than two correlated graphs. Lastly, the problem of seeded graph matching is investigated where a subset of the labels in the second graph are known prior to matching. In this scenario, a polytime matching algorithm is proposed. It is shown that successful matching is guaranteed when the number of seeds grows logarithmically in the number of graph vertices. The logarithmic coefficient is shown to be inversely proportional to the mutual information between the edge variables in the two graphs.

This work was supported by NSF grant CCF-1815821. This work was presented in part at IEEE International Symposium on Information Theory (ISIT), July 2018.

I. Introduction

The graph matching problem models problems in a variety of applications including social network de-anonymization, pattern recognition, and computational biology [1], [2]. In this problem, an agent is given a correlated pair of randomly generated graphs: i) an 'anonymized' unlabeled graph, and ii) a 'de-anonymized' labeled graph as shown in Figure 1. The objective is to leverage the correlation among the edges of the graphs to recover the canonical labeling of the vertices in the anonymized graph.

There has been extensive research investigating the fundamental limits of graph matching, i.e. characterizing the necessary and sufficient conditions on graph parameters for successful matching. The problem has been considered under various probabilistic models capturing the correlation among the graph edges. In the *Correlated Erdös-Rényi* (CER) model the edges in the two graphs are pairwise correlated and are generated independently, based on identical distributions. More precisely, in this model, edges whose vertices are labeled identically are correlated through an arbitrary joint probability distribution and are generated independently of all other edges. In its simplest form — where the edges of the two graphs are exactly equal — graph matching is called *graph isomorphism*. Tight necessary and sufficient conditions for successful matching in the graph isomorphism scenario were derived in [3], [4] and polynomial time algorithms were proposed in [5]–[7]. The problem of matching non-identical pairs of correlated Erdös- Rényi graphs was studied in [8]–[14] and conditions for successful matching were derived. The CER model assumes the existence of statistical correlation among edge pairs connecting matching vertices in the two graphs, where the correlation model is based on an identical distribution among all matching edge pairs. Consequently, it does not model the community structure among the graph nodes which manifests in many applications [15], [16]. As an example, in social networks, users may be divided into communities based on various factors such as age-group, profession, and racial background. The users' community memberships affects the probability that they are connected with each other. A matching algorithm may potentially use the community membership information to enhance its performance. In order to take the users' community memberships into account, an extension to the CER model is considered which is called the *Community Structure* (CS) model. In this model, the edge probabilities depend on their corresponding vertices' community memberships. There have been several works studying both necessary and sufficient conditions for graph matching and the design of practical matching

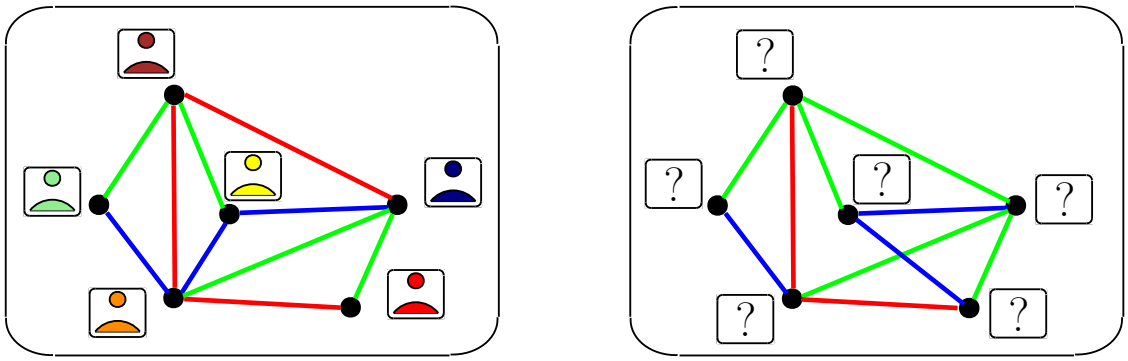

Fig. 1. An instance of the graph matching problem where the anonymized graph on the right is to be matched to the de-anonymized graph on the left.

schemes under the CS model [17], [18]. However, characterizing tight necessary and sufficient conditions for successful matching and designing polytime algorithms which are reliable under these conditions remains an open problem both in the CER and CS settings. A further extension of the problem, called *'seeded graph matching'* has also been investigated in the literature [19]–[28]. Seeded graph matching models applications where the matching agent has access to additional side-information in the form of pre-matched *seeds*. A seed vertex is one whose correct label in both graphs is known prior to the start of the matching process. One pertinent application of seeded graph matching is the de-anonymization of users over multiple social networks. Many web users are members of multiple online social networks such as Facebook, Twitter, Google+, LinkedIn, etc.. Each online network represents a subset of the users' "real" ego-networks. Graph matching provides algorithms to de-anonymize the users by reconciling these online network graphs, that is, to identify all the accounts belonging to the same individual. In this context, the availability of seeds is justified by the fact that a small fraction of individuals explicitly link their accounts across multiple networks. In this case, these linked accounts can be used as seeds in the matching algorithm. It turns out, that in many cases, these connections may be leveraged to identify a very large fraction of the users in the network [20]–[24]. In parallel to the study of fundamental limits of graph matching described above, there has been extensive research on the design of practical low complexity matching algorithms [29]–[31], where reliable matching of real-world networks with up to millions of nodes have been performed.

In this work, we use concentration of measure theorems in order to investigate the fundamental

limits of graph matching, and propose the *'typicality matching'* (TM) strategy which operates based on the concept of typicality of sequences of random variables [32], and is applicable under a wide range of graph models including CER,CS and seeded graph matching. In summary, the strategy considers the pair of adjacency matrices corresponding to the two graphs. Each $n \times n$ adjacency matrix may be viewed as an n^2-length sequence of random variables, where n is the number of vertices in the graph. Consequently, one may naturally extend the notion of typicality of sequences of random variables to that of random adjacency matrices. The TM strategy finds a labeling for the vertices in the anonymized graph which results in a pair of jointly typical adjacency matrices for the two graphs, where typicality is defined with respect to the underlying joint edge distribution. The success of the matching algorithm is investigated as the graph size grows asymptotically large. The matching algorithm is said to succeed if the fraction of correctly matched vertices approaches one as the number of vertices goes to infinity. Consequently, the TM algorithm is successful as long as any labeling which leads to a pair of jointly typical adjacency matrices assigns an incorrect label to a negligible fraction of size $o(n)$ vertices in the anonymized graph[1]. In order to study the conditions for the success of the TM strategy, we derive several new bounds on the probability of joint typicality of permutations of sequences of random variables. The bounds may be of independent interest in other research areas as well. The generality of the information theoretic approach allows us to investigate matching under a wide range of statistical models. In addition to deriving new conditions for successful matching under the CER and CS graph models which have been studied in prior works, we also consider weighted graphs, where the graph edges are allowed to have non-binary attributes. We further extend the results to the simultaneous matching of more than two graphs. Additionally, we derive converse results which provide necessary conditions for successful matching based on model parameters. Furthermore, we consider seeded graph matching and derive theoretical guarantees for successful matching as a function of the seed-set size and the parameters of the statistical model. In the case of seeded graph matching, we provide a matching algorithm whose complexity grows polynomially in the number of vertices. We further derive converse results by providing necessary conditions for successful matching as a function of the seed set size.

The rest of the paper is organized as follows: Section II describes the notation used in the paper. Section III provides the problem formulation. Section IV develops the necessary tools

[1]We write $f(x) = o(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

for analyzing the performance of the TM algorithm. Section V studies matching under the CER model.Section VI considers matching under the CS model. Section VII investigates matching collections of more than two graphs. In Section VIII, necessary conditions and converse results for matching of pairs of graphs are investigated. Section IX shows the equivalence of a well-known criterion successful matching, which has been considered in the literature, with the one considered in this work. Section X studies seeded graph matching. Section XI concludes the paper.

II. Notation

We represent random variables by capital letters such as X, U and their realizations by small letters such as x, u. Sets are denoted by calligraphic letters such as $\mathcal{X}, \mathcal{U}$. The set of natural numbers, and the real numbers are represented by $\mathbb{N}$, and $\mathbb{R}$ respectively. The random variable $\mathbb{1}_{\mathcal{E}}$ is the indicator function of the event $\mathcal{E}$. The set of numbers $\{n, n+1, \cdots, m\}, n, m \in \mathbb{N}$ is represented by $[n, m]$. Furthermore, for the interval $[1, m]$, we sometimes use the shorthand notation $[m]$ for brevity. For a given $n \in \mathbb{N}$, the n-length vector $(x_1, x_2, \ldots, x_n)$ is written as x^n.

III. Problem Formulation

A graph $g = (\mathcal{V}, \mathcal{E})$ is characterized by the vertex set $\mathcal{V} = \{v_1, v_2, \cdots, v_n\}$, and the edge set $\mathcal{E}$. We consider weighted graphs, where each edge is assigned an *attribute* $x \in [l]$ and $l \geq 2$. Consequently, the edge set $\mathcal{E}$ is a subset of the set $\{(x, v_i, v_j) | i \neq j, x \in [l]\}$, where for each pair (v_i, v_j) there is a unique attribute x for which $(x, v_i, v_j) \in \mathcal{E}$. The edge attribute models the nature of the connection between the corresponding vertices. For instance in social network graphs, where vertices represent the members of the network and edges capture their connections, an edge may take different attributes depending on whether the members are family members, close friends, or acquaintances. A labeled graph $\tilde{g} = (g, \sigma)$ is a graph equipped with a bijective *labeling function* $\sigma : \mathcal{V} \to [n]$. The labeling represents the identity of the members in the social network. For a labeled graph $\tilde{g}$, the adjacency matrix $G = [g_{i,j}]_{i,j \in [n]}$ captures the edge attributes, where $g_{i,j}$ is the unique value for which $(g_{i,j}, v_i, v_j) \in \mathcal{E}$.

In this work, we consider graphs whose edges are generated stochastically based on an underlying probability distribution. Under the CER and CS models, we consider special instances of the following stochastic graph model.

Definition 1 (**Random Graph).** *A random graph $\tilde{g}$ generated based on $\prod_{i\in[n],j<i} P_{X_{i,j}}$ is an undirected labeled graph, where the edge between $v_i, i \in [n]$ and $v_j, j < i$ is generated according to $P_{X_{\sigma(i),\sigma(j)}}$ independently of the other edges. Alternatively,*

$$P((x, v_i, v_j) \in \mathcal{E}) = P_{X_{\sigma(i),\sigma(j)}}(x), x \in [l], i, j \in [n].$$

In the graph matching problem, we are given a pair correlated graphs $(\tilde{g}^1, \tilde{g}^2)$, where only the labeling for the vertices of the first graph is available. The objective is to recover the labeling of the vertices in the second graph by leveraging the correlation among their edges. A pair of correlated random graphs is defined below.

Definition 2 (**Correlated Random Graph).** *A pair of correlated random graphs $(\tilde{g}^1, \tilde{g}^2)$ generated based on $\prod_{i\in[n],j<i} P_{X^1_{i,j},X^2_{i,j}}$ is a pair of undirected labeled graphs. Let v^1, w^1 and v^2, w^2 be two pairs of similarly labeled vertices in $\tilde{g}^1$ and $\tilde{g}^2$, respectively i.e. $\sigma^1(v^1) = \sigma^2(v^2) = s_1$ and $\sigma^1(w^1) = \sigma^2(w^2) = s_2$. Then, the pair of edges between (v^1, w^1) and (v^2, w^2) are generated according to $P_{X^1_{s_1,s_2},X^2_{s_1,s_2}}$. Alternatively,*

$$P((x^1, v^1_i, w^1_j) \in \mathcal{E}^1, (x^2, v^2_i, w^2_j) \in \mathcal{E}^2) = P_{X^1_{s_1,s_2},X^2_{s_1,s_2}}(x^1, x^2), x \in [l], i, j \in [n].$$

A graph matching strategy takes $(\tilde{g}^1, g^2)$ as its input and outputs $(\tilde{g}^1, \hat{g}^2)$, where g^2 is the graph $\tilde{g}^2$ with its labels removed, and $\hat{g}^2$ is the relabeled graph. The matching strategy is said to succeed if the fraction of correctly matched vertices approaches one as the number of vertices is increased asymptotically. This is formalized below.

Definition 3 (**Matching Strategy).** *Consider a family of pairs of correlated random graphs $\tilde{g}^1_n = (g^1_n, \sigma^1_n)$ and $\tilde{g}^2_n = (g^2_n, \sigma^2_n), n \in \mathbb{N}$, where n is the number of vertices. A matching strategy is a sequence of functions $f_n : (\tilde{g}^1_n, g^2_n) \to (\tilde{g}^1_n, \hat{g}^2_n), n \in \mathbb{N}$, where $\hat{g}^2_n = (g^2_n, \hat{\sigma}^2_n)$ and $\hat{\sigma}^2_n$ is the reconstruction of σ^2. Let I_n be distributed uniformly over $[n]$. The matching strategy is said to succeed if $P\left(\sigma^2(v^2_{I_n}) = \hat{\sigma}^2(v^2_{I_n})\right) \to 1$ as $n \to \infty$.*

The following defines an achievable region for the graph matching problem.

Definition 4 (**Achievable Region).** *For the graph matching problem, a family of sets of distributions $\widetilde{P} = (\mathcal{P}_n)_{n\in\mathbb{N}}$ is said to be in the achievable region if for every sequence of distributions $\prod_{s_1\in[n],s_2<s_1} P^{(n)}_{X^1_{s_1,s_2},X^2_{s_1,s_2}} \in \mathcal{P}_n$,, there exists a successful matching strategy. The maximal achievable*

family of sets of distributions is denoted by $\mathcal{P}^*$.

IV. Permutations of Typical Sequences

In the previous section, we described correlated pairs of random graphs, where the graph edges are generated randomly based on an underlying joint distribution. Alternatively, the adjacency matrices of the graphs are generated according to a joint distribution. Furthermore, as explained in Definition 2, we assume that each edge pair connecting two similarly labeled vertices in the two graphs is generated independently of all other edges based on the distribution $P_{X_{i,j}}$, where i, j are the vertex labels. Consequently, it is expected, given large enough graph sizes, that the adjacency matrices of the graphs look '*typical*' with respect to the joint edge distribution. Roughly speaking, this requires the frequency of joint occurrence of symbols (x^1, x^2) to be close to $\frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n} P_{X^1_{i,j},X^2_{i,j}}(x^1, x^2)$, where $x^1, x^2 \in [l]$. Based on this observation, in the next sections we propose the typicality matching strategy which operates by finding the labeling for the second graph which results in a jointly typical pair of adjacency matrices. This is analogous to typicality decoding in the channel coding problem in information theory, where the decoder finds the transmitted sequence by searching for a codeword which is jointly typical with the received sequence. In this analogy, the labeled graph $\tilde{g}^2$ is passed through a '*channel*' which outputs g^2, and the '*decode*r' wants to recover $\tilde{g}^2$ using g^2 and the side-information $\tilde{g}^1$. Changing the labeling of g^2 leads to a permutation of its adjacency matrix. Hence, we need to search over permutations of the adjacency matrix and find the one which leads to a typical pair of adjacency matrices. The error analysis of the typicality matching strategy requires investigating the probability of joint typicality of permutations of pairs of correlated sequences.

In this section, we analyze the joint typicality of permutations of collections of correlated sequences of random variables. While the analysis is used in the subsequent sections to derive the necessary and sufficient conditions for successful matching in various graph matching scenarios, it may also be of independent interest in other research areas as well.

We follow the notation used in [33] in our study of permutation groups which is summarized below.

Definition 5 (**Permutation).** *A permutation on the set of numbers* $[1, n]$ *is a bijection* $\pi : [1, n] \to [1, n]$. *The set of all permutations on the set of numbers* $[1, n]$ *is denoted by* S_n.

Definition 6 (**Cycle**). *A permutation $\pi \in S_n, n \in \mathbb{N}$ is called a cycle if there exists $m \in [1,n]$ and $\alpha_1, \alpha_2, \cdots, \alpha_m \in [1,n]$ such that i) $\pi(\alpha_i) = \alpha_{i+1}, i \in [1, m-1]$, ii) $\pi(\alpha_n) = \alpha_1$, and iii) $\pi(\beta) = \beta$ if $\beta \neq \alpha_i, \forall i \in [1,m]$. The variable m is called the length of the cycle. The element α is called a fixed point of the permutation if $\pi(\alpha) = \alpha$. We write $\pi = (\alpha_1, \alpha_2, \cdots, \alpha_m)$. The permutation π is called a non-trivial cycle if $m \geq 2$.*

Lemma 1 (**[33]**). *Every permutation $\pi \in S_n, n \in \mathbb{N}$ has a unique representation as a product of disjoint non-trivial cycles.*

Definition 7 (**Sequence Permutation**). *For a given sequence $y^n \in \mathbb{R}^n$ and permutation $\pi \in S_n$, the sequence $z^n = \pi(y^n)$ is defined as $z^n = (y_{\pi(i)})_{i \in [1,n]}$.*[2]

A. Typicality of Permutations of Pairs of Correlated Sequences

As a first step, we consider typicality of permutations pairs of correlated sequences.

Definition 8 (**Strong Typicality**). *Let the pair of random variables (X,Y) be defined on the probability space $(\mathcal{X}\times\mathcal{Y}, P_{X,Y})$, where $\mathcal{X}$ and $\mathcal{Y}$ are finite alphabets. The ϵ-typical set of sequences of length n with respect to $P_{X,Y}$ is defined as:*

$$A_\epsilon^n(X,Y) = \left\{(x^n, y^n) : \left|\frac{1}{n}N(\alpha,\beta|x^n,y^n) - P_{X,Y}(\alpha,\beta)\right| \leq \epsilon, \forall(\alpha,\beta) \in \mathcal{X}\times\mathcal{Y}\right\},$$

where $\epsilon > 0$, $n \in \mathbb{N}$, and $N(\alpha,\beta|x^n,y^n) = \sum_{i=1}^n \mathbb{1}\left((x_i,y_i) = (\alpha,\beta)\right)$.

For a correlated pair of independent and identically distributed (i.i.d) sequences (X^n, Y^n) and an arbitrary permutation $\pi \in S_n$, we are interested in bounding the probability $P((X^n, \pi(Y^n)) \in \mathcal{A}_\epsilon^n(X,Y))$. In our analysis, we make extensive use of the standard permutations defined below.

Definition 9 (**Standard Permutation**). *For a given $n, m, c \in \mathbb{N}$, and $1 \leq i_1 \leq i_2 \leq \cdots \leq i_c \leq n$ such that $n = \sum_{j=1}^c i_j + m$, an $(m, c, i_1, i_2, \cdots, i_c)$-permutation is a permutation in S_n which has m fixed points and c disjoint cycles with lengths $i_1, i_2, \cdots, i_c$, respectively.*

[2]Note that in Definitions 5 and 7 we have used π to denote both a scalar function which operates on the set $[1,n]$ as well as a function which operates on the vector space $\mathbb{R}^n$.

The $(m, c, i_1, i_2, \cdots, i_c)$-standard permutation is defined as the $(m, c, i_1, i_2, \cdots, i_c)$-permutation consisting of the cycles $(\sum_{j=1}^{k-1} i_j + 1, \sum_{j=1}^{k-1} i_j + 2, \cdots, \sum_{j=1}^{k} i_j), k \in [1, c]$. Alternatively, the $(m, c, i_1, i_2, \cdots, i_c)$-standard permutation is defined as:

$$\pi = (1, 2, \cdots, i_1)(i_1 + 1, i_1 + 2, \cdots, i_1 + i_2) \cdots \\ (\sum_{j=1}^{c-1} i_j + 1, \sum_{j=1}^{c-1} i_j + 2, \cdots, \sum_{j=1}^{c} i_j)(n - m + 1)(n - m + 2) \cdots (n).$$

Example 1. The $(2, 2, 3, 2)$-standard permutation is a permutation which has $m = 2$ fixed points and $c = 2$ cycles. The first cycle has length $i_1 = 3$ and the second cycle has length $i_2 = 2$. It is a permutation on sequences of length $n = \sum_{j=1}^{c} i_j + m = 3 + 2 + 2 = 7$. The permutation is given by $\pi = (123)(45)(6)(7)$. For an arbitrary sequence $\underline{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_7)$, we have:

$$\pi(\underline{\alpha}) = (\alpha_3, \alpha_1, \alpha_2, \alpha_5, \alpha_4, \alpha_6, \alpha_7).$$

The following proposition shows that in order to find bounds on the probability of joint typicality of permutations of correlated sequences, it suffices to study standard permutations.

Proposition 1. *Let (X^n, Y^n) be a pair of i.i.d sequences defined on finite alphabets. We have:*
i) For an arbitrary permutation $\pi \in S_n$,

$$P((\pi(X^n), \pi(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)) = P((X^n, Y^n) \in \mathcal{A}_\epsilon^n(X, Y)).$$

ii) let $n, m, c, i_1, i_2, \cdots, i_c \in \mathbb{N}$ be numbers as described in Definition 9. Let π_1 be an arbitrary $(m, c, i_1, i_2, \cdots, i_c)$-permutation and let π_2 be the $(m, c, i_1, i_2, \cdots, i_c)$-standard permutation. Then,

$$P((X^n, \pi_1(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)) = P((X^n, \pi_2(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)).$$

Proof. The proof of part i) follows from the fact that permuting both X^n and Y^n by the same permutation does not change their joint type. For part ii), it is known that there exists a permutation π such that $\pi(\pi_1) = \pi_2(\pi)$ [33]. Then the statement is proved using part i) as follows:

$$P\left((X^n, \pi_1(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)\right) = P\left((\pi(X^n), \pi(\pi_1(Y^n))) \in \mathcal{A}_\epsilon^n(X, Y)\right) \\ = P\left((\pi(X^n), \pi_2(\pi(Y^n))) \in \mathcal{A}_\epsilon^n(X, Y)\right) \overset{(a)}{=} P\left(\left(\widetilde{X}^n, \pi_2\left(\widetilde{Y}^n\right)\right) \in \mathcal{A}_\epsilon^n(X, Y)\right) \overset{(b)}{=} P\left((X^n, \pi_2(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)\right),$$

where in (a) we have defined $(\widetilde{X}^n, \widetilde{Y}^n) = (\pi(X^n), \pi(Y^n))$. and (b) holds since $(\widetilde{X}^n, \widetilde{Y}^n)$ has the same distribution as (X^n, Y^n). □

The following theorem provides upper-bound on the probability of joint typicality of permutations of correlated sequences for an arbitrary permutation with $m \in [n]$ fixed points.

Theorem 1. *Let (X^n, Y^n) be a pair of i.i.d sequences defined on finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively. For any permutation π with $m \in [n]$ fixed points, the following holds:*

$$P((X^n, \pi(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)) \leq 2^{-\frac{n}{4}(D(P_{X,Y}\|(1-\alpha)P_XP_Y+\alpha P_{X,Y})-|\mathcal{X}\|\mathcal{Y}|\epsilon+O(\frac{\log n}{n}))}, \tag{1}$$

where $\alpha = \frac{m}{n}$, and $D(\cdot\|\cdot)$ is the Kullback-Leibler divergence.

Proof. Appendix A. □

Remark 1. *The upper bound in Equation* (1) *goes to* 0 *as $n \to \infty$ for any non-trivial permutation (i.e. α bounded away from one) and small enough ϵ, as long as X and Y are not independent.*

The exponent $D(P_{X,Y}\|(1-\alpha)P_XP_Y + \alpha P_{X,Y})$ in Equation (1) can be interpreted as follows: for the fixed points of the permutation (α fraction of indices), we have $\pi(Y_i) = Y_i$. As a result, the joint distribution of the elements $(X_i, \pi(Y_i))$ is $P_{X,Y}$. For the rest of the elements, $\pi(Y_i)$ are permuted components of Y^n, as a result $(X_i, \pi(Y_i))$ are an independent pair of variables since (X^n, Y^n) is a correlated pair of i.i.d. sequences. Consequently, the distribution of $(X_i, \pi(Y_i))$ is P_XP_Y for $(1-\alpha)$ fraction of elements which are not fixed points of the permutation. The average distribution is $(1-\alpha)P_XP_Y+\alpha P_{X,Y}$ which appears as the second argument in the Kullback-Leibler Divergence in Equation (1).

Theorem 1 provides bounds on the probability of joint typicality of X^n and $\pi(Y^n)$ as a function of the number of fixed points m of the permutation $\pi(\cdot)$. A parameter of interest is the number of distinct permutations with a specific number of fixed points and its limiting behavior.

Definition 10 (**Derangement**). *Let $n \in \mathbb{N}$. A permutation on vectors of length n is called a derangement if it does not have any fixed points. The number of distinct derangements of n-length vectors is denoted by $!n$.*

Lemma 2. *Let $n \in \mathbb{N}$. Let N_m be the number of distinct permutations with exactly $m \in [0, n]$ fixed points. Then,*

$$\frac{n!}{m!(n-m)} \leq N_m = \binom{n}{m}!(n-m) \leq n^{n-m}. \tag{2}$$

Particularly, let $m = \alpha n, 0 < \alpha < 1$. Then, the following holds:

$$\lim_{n\to\infty} \frac{\log N_m}{n \log n} = 1 - \alpha. \tag{3}$$

Proof. Appendix B. □

In the following, we investigate whether the exponent in Equation (1) is tight (i.e. whether the exponent can be improved to arrive at a tighter upper-bound). Previously, we provided the justification for the appearance of the term $D(P_{X,Y}||(1-\alpha)P_X P_Y + \alpha P_{X,Y})$ in the exponent in Equation (1). However, a more careful analysis may yield improvements in the coefficient $\frac{n}{4}$ by focusing on specific classes of permutations as described in the following. As a first step, we only consider permutations consisting of a single non-trivial cycle and no fixed points.

Lemma 3. *Let (X^n, Y^n) be a pair of i.i.d sequences defined on finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively. For any permutation π with no fixed points, and a single cycle (i.e. $m = 0$ and $c = 1$), the following holds:*

$$P((X^n, \pi(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)) \leq 2^{-\frac{n}{2}(I(X;Y)-\delta)}, \tag{4}$$

where $\delta = 2\sum_{x,y} |\log_2 \frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}|\epsilon$ and $\epsilon > 0$.

Proof. Appendix C. □

Remark 2. *Note that Theorem 1 can also be applied to derive a bound on the probability of joint typicality given the permutation considered in Lemma 3. In this case $\alpha = \frac{m}{n} = 0$ and $D(P_{X,Y}||\alpha P_{X,Y} + (1-\alpha)P_X P_Y) = I(X;Y)$ and Theorem 1 yeilds the exponent $\frac{n}{4}I(X;Y)$ for the probability of joint typicality. Hence, Lemma 3 improves the exponent $\frac{n}{4}I(X;Y)$ in Theorem 1 to $\frac{n}{2}I(X;Y)$ for single-cycle permutations with no fixed points.*

The following lemma derives similar results for permutations with a large number of short cycles (e.g. cycles of length two or three) and no fixed points.

Lemma 4. *Let (X^n, Y^n) be a pair of correlated sequences of i.i.d variables defined on finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively. For any $(n, m, c, i_1, i_2, \cdots, i_c)$-permutation π with no fixed points (m=0), where $0 < i_1 < i_2 < \cdots < i_c < s < n$, the following holds:*

$$P((X^n, \pi(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)) \leq 2^{-\frac{n}{s}(I(X;Y)-\delta)}, \tag{5}$$

where $\delta = \sum_{x,y} |\log_2 \frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}| \epsilon$ and $\epsilon > 0$.

Proof. Appendix D. □

Remark 3. *Lemma 4 improves the exponent in Theorem 1 when the maximum cycle length is less than or equal to $s = 3$.*

B. Typicality of Permutations of Collections of Correlated Sequences

In the next step, we consider joint typicality of permutations of collections of correlated sequences.

Definition 11 (**Strong Typicality of Collections of Sequences).** *Let the random vector X^m be defined on the probability space $(\prod_{j\in[m]} \mathcal{X}_j, P_{X^m})$, where $\mathcal{X}_j, j \in [m]$ are finite alphabets, and $m > 2$. The ϵ-typical set of sequences of length n with respect to P_{X^m} is defined as:*

$$\mathcal{A}_\epsilon^n(X^m) = \left\{(x_{(j)}^n)_{j\in[m]} : \left|\frac{1}{n} N(\alpha^m | x_{(1)}^n, x_{(2)}^n, \cdots, x_{(m)}^n) - P_{X^m}(\alpha^m)\right| \leq \epsilon, \forall \alpha^m \in \prod_{j\in[m]} \mathcal{X}_j\right\},$$

where $\epsilon > 0$, $N(\alpha^m | x_{(1)}^n, x_{(2)}^n, \cdots, x_{(m)}^n) = \sum_{i=1}^n \mathbb{1}\left((x_{(j),i})_{j\in[m]} = \alpha^m\right)$, and $(x_{(j)}^n)_{j\in[m]} = (x_{(1)}^n, \cdots, x_{(m)}^n)$ is a vector of sequences.

In the previous section, in order to investigate the typicality of permutations of pairs of correlated sequences, we introduced standard permutations which are completely characterized by the number of fixed points, number of cycles, and cycle lengths of the permutation. The concept of standard permutations does not extend naturally when there are more than two sequences (i.e. more than one non-trivial permutation). Consequently, investigating typicality of permutations of collections of sequences requires developing additional analytical tools which are described in the following.

Definition 12 (Bell Number). *Consider the set* $\mathcal{N} = [1, n]$. *Let* $\mathsf{P} = \{\mathcal{P}_1, \mathcal{P}_2, \cdots, \mathcal{P}_{b_m}\}$ *be the set of all partitions of* $\mathcal{N}$, *where* $\mathcal{P}_k = \{\mathcal{A}_{k,1}, \mathcal{A}_{k,2} \cdots, \mathcal{A}_{k,|\mathcal{P}_k|}\}$. *The natural number* b_m *is the mth Bell number.*

In the following, we define Bell permutation vectors which are analogous to standard permutations for the case when the problem involves more than one non-trivial permutation.

Definition 13 (Partition Correspondence). *Let* $m, n \in \mathbb{N}$ *and* $(\pi_1, \pi_2, \cdots, \pi_m)$ *be arbitrary permutations operating on n-length vectors. The index* $i \in [n]$ *is said to correspond to the partition* $\mathcal{P}_k = \{\mathcal{A}_{k,1}, \mathcal{A}_{k,2}, \cdots, \mathcal{A}_{k,|\mathcal{P}_k|}\}$ *of the set* $[1, m]$ *if the following holds:*

$$\forall\, j, j' \in [m] : \pi_j^{-1}(i) = \pi_{j'}^{-1}(i) \iff \exists r : j, j' \in \mathcal{A}_{k,r}$$

To explain the above definition, let us consider a triple of permutations of n-length sequences, i.e. $m = 3$, and the partition $\mathcal{P}_k = \{\{1, 2\}, \{3\}\}$. Then an index $i \in [n]$ corresponds to the partition $\mathcal{P}_k$ if the first two permutation map the index to the same integer and the third permutation maps the index to a different integer.

Definition 14 (Bell Permutation Vector). *Let* $(i_1, i_2, \cdots, i_{b_m})$ *be an arbitrary sequence, where* $\sum_{k\in[b_m]} i_k = n, i_k \in [0, n]$, b_m *is the mth Bell number, and* $n, m \in \mathbb{N}$. *The vector of permutations* $(\pi_1, \pi_2, \cdots, \pi_m)$ *is called an* $(i_1, i_2, \cdots, i_{b_m})$*-Bell permutation vector if for every partition* $\mathcal{P}_k$ *exactly* i_k *indices correspond to that partition. Equivalently:*

$$\forall k \in [b_m] : i_k = |\{i \in [n] : \forall\, j, j' \in [m] : \pi_j^{-1}(i) = \pi_{j'}^{-1}(i) \iff \exists r : j, j' \in \mathcal{A}_{k,r}\}|.$$

The definition of Bell permutation vectors is further clarified through the following example.

Example 2. Consider 3 permutations (π_1, π_2, π_3) of vectors with length equal to 7, i.e. $m = 3$ and $n = 7$. Then, $b_m = 5$ and we have:

$$\mathcal{P}_1 = \{\{1\}, \{2\}, \{3\}\}, \quad \mathcal{P}_2 = \{\{1, 2\}, \{3\}\}, \quad \mathcal{P}_3 = \{\{1, 3\}, \{2\}\},$$

$$\mathcal{P}_4 = \{\{1\}, \{2, 3\}\}, \quad \mathcal{P}_5 = \{\{1, 2, 3\}\}.$$

Let π_1 be the trivial permutation fixing all indices and let $\pi_2 = (135)(24)$, $\pi_3 = (15)(24)(37)$. Then:

$$\pi_1((1, 2, \cdots, 7)) = (1, 2, 3, 4, 5, 6, 7),$$

$$\pi_2((1,2,\cdots,7)) = (5,4,1,2,3,6,7),$$

$$\pi_3((1,2,\cdots,7)) = (5,4,7,2,1,6,3),$$

Then, the vector (π_1,π_2,π_3) is a $(2,1,0,3,1)$-Bell permutation vector, where the indices $(3,5)$ correspond to the $\mathcal{P}_1$ partition (each of the three permutations map the index to a different integer), index 7 corresponds to the $\mathcal{P}_2$ partition (the first two permutations map the index to the same integer which is different from the one for the third permutation), indices $(1,2,4)$ correspond to the $\mathcal{P}_3$ permutation (the second and third permutations map the index to the same integer which is different from the output of the first permutation), and index 6 corresponds to $\mathcal{P}_5$ (all permutations map the index to the same integer).

Remark 4. *Bell permutation vectors are not unique. In other words, there can be several distinct $(i_1,i_2,\cdots,i_{b_m})$-Bell permutation vectors for given $n,m,i_1,i_2,\cdots,i_{b_m}$. This is in contrast with standard permutations defined in Definition 9, which are unique given the parameters $n,c,i_1,i_2,\cdots,i_c$.*

The following theorem provides bounds on the probability of joint typicality of permutations of collections of correlated sequences:

Theorem 2. *Let $(X^n_{(j)})_{j\in[m]}$ be a collection of correlated sequences of i.i.d random variables defined on finite alphabets $\mathcal{X}_{(j)}$, $j\in[m]$. For any $(i_1,i_2,\cdots,i_{b_m})$-Bell permutation vector $(\pi_1,\pi_2,\cdots,\pi_m)$, the following holds:*

$$P((\pi_i(X^n_{(i)})_{i\in[m]} \in \mathcal{A}^n_\epsilon(X^m)) \leq 2^{-\frac{n}{m(m-1)b_m}(D(P_{X^m}\|\sum_{k\in[b_m]}\frac{i_k}{n}P_{X_{\mathcal{P}_k}})-\epsilon\prod_{j\in[m]}|\mathcal{X}_j|+O(\frac{\log n}{n}))}, \tag{6}$$

where $P_{X_{\mathcal{P}_k}} = \prod_{l\in[1,|\mathcal{P}_k|]} P_{X_{k_1},X_{k_2},\cdots,X_{k_{|\mathcal{A}_{k,r}|}}}$, $\mathcal{A}_{k,r} = \{l_1,l_2,\cdots,l_{|\mathcal{A}_{k,r}|}\}, k\in[b_m], r\in[1,|\mathcal{P}_k|]$, and $D(\cdot\|\cdot)$ is the Kullback-Leibler divergence.

Proof. Appendix E. □

Note that for permutations of pairs of sequences of random variables, $m=2$ and the second Bell number is $b_2=2$. In this case $m(m-1)b_m=4$, and the bound on the probability of joint typicality given in Theorem 2 recovers the one in Theorem 1. In the following, we provide upper and lower bounds on the number of distinct Bell permutation vectors for a given vector $(i_1,i_2,\cdots,i_{b_m})$.

Definition 15 (**r-fold Derangement).** *A vector* $(\pi_1(\cdot), \pi_2(\cdot), \cdots, \pi_r(\cdot))$ *of permutations of n-length sequences is called an r-fold derangement if* $\pi_1(\cdot)$ *is the identity permutation, and* $\pi_l(i) \neq \pi_{l'}(i), l, l' \in [r], l \neq l', i \in [n]$. *The number of distinct r-fold derangements of* $[n]$ *is denoted by* $d_r(n)$. *Particularly* $d_2(n) = !n$ *is the number of derangements of* $[n]$.

Lemma 5. *Let* $n \in \mathbb{N}$ *and* $r \in [n]$. *Then,*

$$((n - r + 1)!)^{r-1} \leq d_r(n) \leq (!n)^{r-1}.$$

Proof. Appendix F. □

Lemma 6. *Let* $(i_1, i_2, \cdots, i_{b_m})$ *be a vector of non-negative integers such that* $\sum_{k\in[b_m]} i_k = n$. *Define* $N_{i_1,i_2,\cdots,i_{b_m}}$ *as the number of distinct* $(i_1, i_2, \cdots, i_{b_m})$*-Bell permutation vectors. Then,*

$$\binom{n}{i_1, i_2, \cdots, i_{b_m}} \prod_{k\in[b_m]} d_{|\mathcal{P}_k|}(i_k) \leq N_{i_1,i_2,\cdots,i_{b_m}} \leq \binom{n}{i_1, i_2, \cdots, i_{b_m}} n^{\sum_{k\in[b_m]} |\mathcal{P}_k| i_k - n}. \tag{7}$$

Particularly, let $i_k = \alpha_k \cdot n, n \in \mathbb{N}$. *The following holds:*

$$\lim_{n\to\infty} \frac{\log N_{i_1,i_2,\cdots,i_{b_m}}}{n \log n} = \sum_{k\in[b_m]} |\mathcal{P}_k|\alpha_k - 1. \tag{8}$$

Proof. Appendix G. □

V. Matching Erdös-Rènyi Graphs

In this section, we consider matching of correlated pairs of Erdös-Rènyi (CPER) graphs. In section III, we described correlated random graphs. A CPER is a special instance of the correlated random graphs defined in Definition 2. We propose the typicality matching strategy and provide sufficient conditions on the joint edge statistics under which the strategy succeeds.

A. Problem Setup

In order to describe the notation used in this section, we formally define labeled graphs below.

Definition 16 (**Labeled Graphs).** *A labeling is a bijective function* $\sigma : \mathcal{V} \to [1, n]$. *The pair* $\tilde{g} = (g, \sigma)$ *is called an* (n, l)*-labeled graph. For the labeled graph* $\tilde{g}$ *the adjacency matrix is defined as* $G_\sigma = [g_{\sigma,i,j}]_{i,j\in[1,n]}$ *where* $g_{\sigma,i,j}$ *is the unique value such that* $(g_{\sigma,i,j}, v_i, v_j) \in \mathcal{E}_n$, *where* $(v_i, v_j) = (\sigma^{-1}(i), \sigma^{-1}(j))$. *The upper triangle (UT) corresponding to* $\tilde{g}$ *is the structure* $U_\sigma = [G_{\sigma,i,j}]_{i<j}$. *The subscript '*$\sigma$*' is dropped when there is no ambiguity.*

Remark 5. *In the context of Definition 16, an unlabeled graph with binary valued edges is a graph for which* $l = 2$*. In this case, if the pair* $v_{n,i}$ *and* $v_{n,i}$ *are not connected, we write* $(0, v_{n,i}, v_{n,j}) \in \mathcal{E}$*, otherwise* $(1, v_{n,i}, v_{n,j}) \in \mathcal{E}$*.*

Remark 6. *Without loss of generality, we assume that for any arbitrary pair of vertices* $(v_{n,i}, v_{n,j})$*, there exists a unique* $x \in [0, l-1]$ *such that* $(x, v_{n,i}, v_{n,j}) \in \mathcal{E}$*.*

Remark 7. *In this work, we often consider sequences of graphs* $g^{(n)}, n \in \mathbb{N}$*, where* $g^{(n)}$ *has* n *vertices. In such instances, we write* $g^{(n)} = (\mathcal{V}^{(n)}, \mathcal{C}^{(n)}, \mathcal{E}^{(n)})$ *to characterize the nth graph in the sequence. The superscript '*(n)*' is omitted where there is no ambiguity.*

Remark 8. *In this work, we only consider undirected graphs where* $(x, v_i, v_j) \in \mathcal{E}$ *if and only if* $(x, v_j, v_i) \in \mathcal{E}$*. The results can be extended to directed graphs in a straightforward manner.*

Any pair of labeling functions are related through a permutation as described below.

Definition 17. *For two labelings* σ *and* σ'*, the* (σ, σ')*-permutation is defined as the bijection* $\pi_{(\sigma,\sigma')}$*, where:*

$$\pi_{(\sigma,\sigma')}(i) = j, \quad \text{if} \quad \sigma'^{-1}(j) = \sigma^{-1}(i), \forall i, j \in [1, n].$$

Definition 18 (Correlated Pair of ER Graphs). *Let* $P_{X,X'}$ *be a conditional distribution defined on* $\mathcal{X} \times \mathcal{X}'$*, where* $\mathcal{X} = \mathcal{X}' = [0, l-1]$*. A correlated pair of ER graphs* $\underline{\tilde{g}} = (\tilde{g}, \tilde{g}')$ *generated according to* $P_{X,X'}$ *is characterized by: i) the pair of ER graphs* (g, g') *generated according to* P_X *and* $P_{X'}$*, respectively, ii) the pair of labelings* (σ, σ') *for the unlabeled graphs* (g, g')*, and iii) the probability distribution* $P_{X,X'}$*, such that:*
1)The graphs have the same set of vertices $\mathcal{V} = \mathcal{V}'$*.*
2) For any two edges $e = (x, v_{j_1}, v_{j_2}), e' = (x', v'_{j'_1}, v'_{j'_2}), x, x' \in [0, l-1]$*, we have*

$$Pr\left(e \in \mathcal{E}, e' \in \mathcal{E}'\right) = \begin{cases} P_{X,X'}(x, x'), & \text{if } \sigma(v_{j_l}) = \sigma'(v'_{j'_l}) \\ P_X(x)P_{X'}(x'), & \text{Otherwise} \end{cases},$$

where $l \in \{1, 2\}$*,* $v_{j_1}, v_{j_2} \in \mathcal{V}_1 \times \mathcal{V}_2$*, and* $v'_{j'_1}, v'_{j'_2} \in \mathcal{V}_1 \times \mathcal{V}_2$*.*

B. The Typicality Matching Strategy for CERs

Given a correlated pair of graphs $\underline{g} = (\tilde{g}^1, g^2)$, where only the labeling for $\tilde{g}^1$ is given, the typicality matching strategy operates as follows. The scheme finds a labeling $\hat{\sigma}^2$, for which the pair of UT's $U^1_{\sigma^1}$ and $U^2_{\hat{\sigma}^2}$ are jointly typical with respect to P_{n,X_1,X_2} when viewed as vectors of length $\frac{n(n-1)}{2}$. The strategy succeeds if at least one such labeling exists and fails otherwise. Alternatively, it finds an element $\hat{\sigma}^2$ in the set:

$$\widehat{\Sigma} = \{\hat{\sigma}^2 | (U^1_{\sigma^1}, U^2_{\hat{\sigma}^2}) \in \mathcal{A}_\epsilon^{\frac{n(n-1)}{2}}(X_1, X_2)\},$$

where $\epsilon = \omega(\frac{1}{n})$. The algorithm declares $\hat{\sigma}^2$ as the correct labeling. Note that the set $\widehat{\Sigma}$ may have more than one element. We will show that under certain conditions on the joint graph statistics, all of the elements of $\widehat{\Sigma}$ satisfy the criteria for successful matching given in Definition 23. In other words, for all of the elements of $\widehat{\Sigma}$ the probability of incorrect labeling for any given vertex is arbitrarily small for large n.

Theorem 3. *For the typicality matching strategy, a given family of sets of distributions $\widetilde{P} = (\mathcal{P}_n)_{n\in\mathbb{N}}$ is achievable, if for every sequence of distributions $P_{n,X_1,X_2} \in \mathcal{P}_n, n \in \mathbb{N}$*

$$8(1-\alpha)\frac{\log n}{n-1} \leq D(P^{(n)}_{X_1,X_2} \| (1-\alpha^2)P^{(n)}_{X_1}P^{(n)}_{X_2} + \alpha^2 P^{(n)}_{X_1,X_2}), 0 \leq \alpha \leq \alpha_n, \tag{9}$$

where α_n is a sequence such that $\alpha_n \to 1$ as $n \to \infty$.

Proof. Appendix H. □

Remark 9. *As described in Section IV, the bound in Equation* (9) *can be potentially tightened with the coefficient 8 in the left hand side replaced by 6.*

The Kullback Leibler divergence term $D(P^{(n)}_{X_1,X_2} \| (1-\alpha^2)P^{(n)}_{X_1}P^{(n)}_{X_2} + \alpha^2 P^{(n)}_{X_1,X_2})$ in the right hand side of Equation (9) can be interpreted as follows. Let α be the fraction of the vertices which are matched correctly by the typicality matching scheme. Then almost α^2 elements in the two adjacency matrices of the graphs are in the correct position, and the rest are permuted. The elements which are in the correct position are distributed according to the joint distribution $P^{(n)}_{X_1,X_2}$, whereas the permuted elements are distributed according to $P^{(n)}_{X_1}P^{(n)}_{X_1}$, i.e. independently of each other. Consequently, the empirical joint distribution of the elements of the two matrices is close to $(1-\alpha^2)P^{(n)}_{X_1}P^{(n)}_{X_2} + \alpha^2 P^{(n)}_{X_1,X_2}$ with high probability. The typicality matching scheme outputs such a labeling if the resulting adjacency matrix — generated according to $(1-\alpha^2)P^{(n)}_{X_1}P^{(n)}_{X_2} + \alpha^2 P^{(n)}_{X_1,X_2}$

based on the above argument — is typical with respect to $P^{(n)}_{X_1,X_2}$. It is well-known that the error exponent for such a binary hypothesis test is equal to $D(P^{(n)}_{X_1,X_2}\|(1-\alpha^2)P^{(n)}_{X_1}P^{(n)}_{X_2}+\alpha^2 P^{(n)}_{X_1,X_2})$. Furthermore, the $(1-\alpha)\frac{\log n}{n-1}$ term on the left hand side is the exponent of the total number of permutations with α fraction of fixed points.

VI. Matching Graphs with Community Structure

In this section, we describe the typicality matching scheme for matching graphs with community structure and provide achievable regions for these matching scenarios.

A. Problem Setup

To describe the notation used in the section, consider a graph with $n \in \mathbb{N}$ vertices belonging to $c \in \mathbb{N}$ communities whose edges take $l \geq 2$ possible attributes. It is assumed that the set of communities $C = \{C_1, C_2, \cdots, C_c\}$ partitions the vertex set $\mathcal{V}$. The i^{th} community is written as $C_i = \{v_{j_1}, v_{j_2}, \cdots, v_{j_{n_i}}\}$. The following formally defines a graph with community structure.

Definition 19 (Graph with Community Structure). *An $(n, c, (n_i)_{i\in[c]}, l)$-unlabeled graph with community structure (UCS) g is characterized by the triple $(\mathcal{V}, C, \mathcal{E})$, where $n, l, c, n_1, n_2, \cdots, n_c \in \mathbb{N}$ and $l \geq 2$. The set $\mathcal{V} = \{v_1, v_2, \cdots, v_n\}$ is called the vertex set. The family of sets $C = \{C_1, C_2, \cdots, C_c\}$ provides a partition for $\mathcal{V}$ and is called the family of communities. The i^{th} community is written as $C_i = \{v_{j_1}, v_{j_2}, \cdots, v_{j_{n_i}}\}$. The set $\mathcal{E} \subset \{(x, v_{j_1}, v_{j_2}) | x \in [0, l-1], j_1 \in [1, n], j_2 \in [1, n]\}$ is called the edge set of the graph. For the edge (x, v_{j_1}, v_{j_2}), the variable 'x' represents the value assigned to the edge between vertices v_{j_1} and v_{j_2}. The set $\mathcal{E}_{i_1,i_2} = \{(x, v_{j_1}, v_{j_2}) \in \mathcal{E} | v_{j_1} \in C_{i_1}, v_{j_2} \in C_{i_2}\}$ is the set of edges connecting the vertices in communities C_{i_1} and C_{i_2}.*

Remark 10. *Single-community graphs, where $c = 1$, have been studied extensively in the graph matching literature. For instance Erdös-Rényi (ER) graphs studied in Section V are single-community graphs.*

We consider graphs generated stochastically based on the community structure model. In this model, the probability of an edge between a pair of vertices is determined by their community memberships. More precisely, for a given vertex set $\mathcal{V}$ and set of communities C, it is assumed

that the edge set $\mathcal{E}$ is generated randomly, where the attribute X of the edge between vertices $v_{i_1} \in C_{j_1}$ and $v_{i_2} \in C_{j_2}$ is generated based on the conditional distribution $P_{X|C_{i_1},C_{i_2}}$.

Definition 20 (**Random Graph with Community Structure).** *Let $P_{X|C_i,C_o}$ be a set of conditional distributions defined on $\mathcal{X} \times C \times C$, where $\mathcal{X} = [0, l-1]$ and C is defined in Definition 19. A random graph with community structure (RCS) g generated according to $P_{X|C_i,C_o}$ is a randomly generated $(n, c, (n_i)_{i\in[c]}, l)$-UCS with vertex set $\mathcal{V}$, community set C, and edge set $\mathcal{E}$, such that*

$$P((x, v_{j_1}, v_{j_2}) \in \mathcal{E}) = P_{X|C_i,C_o}(x|C_{j_1}, C_{j_2}), \forall x \in [0, l-1],$$

where $v_{j_1}, v_{j_2} \in C_{j_1} \times C_{j_2}$, and edges between different vertices are mutually independent.

Remark 11. *Note that for undirected graphs considered in this work, we must have $P_{X|C_i,C_o}(x|C_{j_1}, C_{j_2}) = P_{X|C_i,C_o}(x|C_{j_2}, C_{j_1})$.*

The following provides the notation used to represent the adjacency matrix of labeled graphs with community structure.

Definition 21 (**Adjacency Matrix).** *For an $(n, c, (n_i)_{i\in[c]}, l)$-UCS $g = (\mathcal{V}, C, \mathcal{E})$, a labeling is defined as a bijective function $\sigma : \mathcal{V} \to [1, n]$. The pair $\tilde{g} = (g, \sigma)$ is called an $(n, c, (n_i)_{i\in[c]}, l)$-labeled graph with community structure (LCS). For the labeled graph $\tilde{g}$ the adjacency matrix is defined as $G_\sigma = [G_{\sigma,i,j}]_{i,j\in[1,n]}$ where $G_{\sigma,i,j}$ is the unique value such that $(G_{\sigma,i,j}, v_i, v_j) \in \mathcal{E}_n$, where $(v_i, v_j) = (\sigma^{-1}(i), \sigma^{-1}(j))$. The submatrix $G_{\sigma,C_i,C_j} = [G_{\sigma,i,j}]_{i,j:v_i,v_j\in C_i\times C_j}$ is the adjacency matrix corresponding to the community pair C_i and C_j. The upper triangle (UT) corresponding to $\tilde{g}$ is the structure $U_\sigma = [G_{\sigma,i,j}]_{i<j}$. The upper triangle corresponding to communities C_i and C_j in $\tilde{g}$ is denoted by $U_{\sigma,C_i,C_j} = [G_{\sigma,i,j}]_{i<j:v_i,v_j\in C_i\times C_j}$. The subscript '$\sigma$' is dropped when there is no ambiguity.*

We consider pairs of correlated RCSs. It is assumed that edges between pairs of vertices in the two graphs with the same labeling are correlated and are generated based on a joint probability distribution, whereas edges between pairs of vertices with different labeling are generated independently. A pair of correlated RCSs is formally defined below.

Definition 22 (**Correlated Pair of RCSs).** *Let $P_{X,X'|C_{j_1},C_{j_2},C'_{j'_1},C'_{j'_2}}$, $j_1, j_2, j'_1, j'_2 \in [1, c]$ be a set of conditional distributions defined on $\mathcal{X}\times\mathcal{X}'\times C\times C\times C'\times C'$, where $\mathcal{X} = \mathcal{X}' = [0, l-1]$ and (C, C') are a pair of community sets of size $c \in \mathbb{N}$. A correlated pair of random graphs with community*

structure (CPCS) generated according to $P_{X,X'|C_{j_1},C_{j_2},C'_{j'_1},C'_{j'_2}}$ *is a pair* $\underline{\tilde{g}} = (\tilde{g}, \tilde{g}')$ *characterized by: i) the pair of RCSs* (g, g') *generated according to* $P_{X|C_{j_1},C_{j_2}}$ *and* $P_{X'|C'_{j'_1},C'_{j'_2}}$*, respectively, ii) the pair of labelings* (σ, σ') *for the graphs* (g, g')*, and iii) the probability distribution* $P_{X,X'|C_{j_1},C_{j_2},C'_{j'_1},C'_{j'_2}}$*, such that:*

1)The graphs have the same set of vertices $\mathcal{V} = \mathcal{V}'$*.*

2) For any two edges $e = (x, v_{j_1}, v_{j_2}), e' = (x', v'_{j'_1}, v'_{j'_2}), x, x' \in [0, l-1]$*, we have*

$$Pr\left(e \in \mathcal{E}, e' \in \mathcal{E}'\right) = \begin{cases} P_{X,X'}(x, x'), & \text{if } \sigma(v_{j_l}) = \sigma'(v'_{j'_l}) \\ Q_{X,X'}(x, x'), & \text{Otherwise} \end{cases},$$

where $l \in \{1, 2\}$*,* $v_{j_1}, v_{j_2} \in C_{j_1} \times C_{j_2}$*,* $v'_{j'_1}, v'_{j'_2} \in C'_{j'_1} \times C'_{j'_2}$*, the distribution* $P_{X,X'}$ *is the joint edge distribution when the edges connect vertices with similar labels and is given by* $P_{X,X'|C_{j_1},C_{j_2},C'_{j'_1},C'_{j'_2}}$*, the distribution* $Q_{X,X'}$ *is the conditional edge distribution when the edges connect labels with different labels and is given by* $P_{X|C_{j_1},C_{j_2}} \times P_{X'|C'_{j'_1},C'_{j'_2}}$*.*

Remark 12. *In Definition 22, we have assumed that both graphs have the same number of vertices. In other words, the vertex set for both graphs is* $\mathcal{V} = \mathcal{V}' = \{v_1, v_2, \cdots, v_n\}$*. We further assume that the community memberships in both graphs are the same. In other words, we assume that* $v_j \in C_i \Rightarrow v'_{j'} \in C'_i$ *given that* $\sigma(v_j) = \sigma'(v'_{j'})$ *for any* $j, j' \in [n]$ *and* $i \in [c]$*. However, the results presented in this work can be extended to graphs with unequal but overlapping vertex sets and unequal community memberships in a straightforward manner.*

Remark 13. *We assume that the size of the communities in the graph sequence grows linearly in the number of vertices. More precisely, let* $\Lambda^{(n)}(i) \triangleq |C_i^{(n)}|$ *be the size of the* i^{th} *community, we assume that*[3] $\Lambda^{(n)}(i) = \Theta(n)$ *for all* $i \in [c]$*. Furthermore, we assume that the number of communities* c *is constant in* n*.*

We consider the matching strategies under two assumptions: i) with side-information, where the strategy uses prior knowledge of vertices' community memberships, ii) without side-information, where the strategy does not use prior knowledge of the vertices' community memberships, rather, it uses the statistics $P_{X,X'|C_i,C_o,C_{i'},C_{o'}}$ and the community sizes $(n_i)_{i\in[c]}$. The matching strategy is said to succeed if the fraction of vertices in the second graph which are labeled correctly approaches one as the number of vertices increases asymptotically.

[3]We write $f(x) = \Theta(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)}$ is a non-zero constant.

Definition 23 (Matching Strategy). *A matching strategy is defined under the following two scenarios:*

- ***With Side-information:*** *A matching strategy operating with complete side-information is a sequence of functions* $f_n^{CSI} : (\underline{g}^{(n)}, C^{(n)}, C'^{(n)}) \mapsto \hat{\sigma}'^{(n)}, n \in \mathbb{N}$*, where* $\underline{g}^{(n)} = (\tilde{g}_1^{(n)}, g_2^{(n)})$ *consists of a pair of graphs with CS with n vertices.*
- ***Without Side-information:*** *A matching strategy operating without side-information is a sequence of functions* $f_n^{WSI} : \underline{g}^{(n)} \mapsto \hat{\sigma}'^{(n)}, n \in \mathbb{N}$.

The output of a successful matching strategy satisfies $P\left(\sigma'^{(n)}(v'_{J^{(n)}}) = \hat{\sigma}'^{(n)}(v'_{J^{(n)}})\right) \to 1$ *as* $n \to \infty$*, where the random variable* $J^{(n)}$ *is uniformly distributed over* $[1, n]$ *and* $\sigma'^{(n)}$ *is the labeling for the graph* $g'^{(n)}$ *for which* $(\tilde{g}^{(n)}, \tilde{g}'^{(n)})$ *is a CPCS, where* $\tilde{g}'^{(n)} \triangleq (g'^{(n)}, \sigma'^{(n)})$.

Note that the output of a successful matching strategy $\hat{\sigma}'$ does not necessarily match every vertex correctly, i.e. does not satisfy $\hat{\sigma}' = \sigma'$. In other words, the pair $(\tilde{g}, \hat{g}')$ is not precisely a CPCS, where $\hat{g}' \triangleq (g', \hat{\sigma}')$. Rather, the fraction of mismatched vertices approaches zero as the size of the graph grows asymptotically large. This is in contrast with prior works [20], [26], [29] where a matching scheme is defined to be successful if it matches every vertex correctly, simultaneously, with probability approaching one as the graph grows asymptotically large. This relaxation of the success criteria is essential in application of concentration of measure theorems used in the next sections, and leads to significant simplification of our derivations. However, in Section IX, we show that the necessary and sufficient conditions on graph statistics which guarantee successful matching are equivalent for asymptotically large graphs under both success criteria. Consequently, the conditions derived in this work are applicable under the success criterion considered in prior works as well.

B. Matching in Presence of Side-information

First, we describe the matching strategy under the complete side-information scenario. In this scenario, the community membership of the nodes at both graphs are known prior to matching. Given a CPCS $\underline{\tilde{g}}$ generated according to $P_{X,X'|C_{j_1},C_{j_2},C'_{j'_1},C'_{j'_2}}$, $j_1, j_2, j'_1, j'_2 \in [1, c]$, the scheme operates as follows. It finds a labeling $\hat{\sigma}'$, for which i) the set of pairs $(G_{\sigma,C_{j_1},C_{j_2}}, G'_{\hat{\sigma}',C'_{j_1},C'_{j_2}})$, $j_1, j_2 \in [c]$ are jointly typical each with respect to $P_{X,X'|C_{j_1},C_{j_2},C'_{j_1},C'_{j_2}}(\cdot,\cdot|C_{j_1}, C_{j_2}, C'_{j_1}, C'_{j_2})$ when viewed as vectors of length $n_i n_j, i \neq j$, and ii) the set of pairs $(U_{\sigma,C_j,C_j}, U'_{\hat{\sigma}',C'_j,C'_j})$, $j \in [c]$ are jointly typical with

respect to $P_{X,X'|C_{j_1},C_{j_2},C'_{j_1},C'_{j_2}}(\cdot,\cdot|C_j,C_j,C'_j,C'_j)$ when viewed as vectors of length $\frac{n_i(n_i-1)}{2}, j \in [c]$. Specifically, it returns a randomly picked element $\hat{\sigma}'$ from the set:

$$\widehat{\Sigma}_{C.C'} = \{\hat{\sigma}'|(U_{\sigma,C_j,C_j}, U'_{\hat{\sigma}',C'_j,C'_j}) \in \mathcal{A}_\epsilon^{\frac{n_j(n_j-1)}{2}}(P_{X,X'|C_j,C_j,C'_j,C'_j}), \forall j \in [c],$$

$$(G_{\sigma,C_i,C_j}, G'_{\hat{\sigma}',C'_i,C'_j}) \in \mathcal{A}_\epsilon^{n_i n_j}(P_{X,X'|C_i,C_j,C'_i,C'_j}), \forall i,j \in [c], i \neq j\},$$

where $\epsilon = \omega(\frac{1}{n})$, and declares $\hat{\sigma}'$ as the correct labeling. We show that under this scheme, the probability of incorrect labeling for any given vertex is arbitrarily small for large n.

Theorem 4. *For the typicality matching scheme, a given family of sets of distributions $\widetilde{P} = (\mathcal{P}^{(n)})_{n\in\mathbb{N}}$ is achievable, if for any constants $\delta > 0$, $\alpha \in [0, 1-\delta]$ and every sequence of distributions $P^{(n)}_{X,X'|C_{j_1},C_{j_2},C'_{j'_1},C'_{j'_2}} \in \mathcal{P}_n, j_1, j_2, j'_1, j'_2 \in [1, c]$, and community sizes $(n_1^{(n)}, n_2^{(n)}, \cdots, n_c^{(n)}), n \in \mathbb{N}$:*

$$4(1-\alpha)\frac{\log n}{n} \leq \min_{[\alpha_i]_{i\in[c]}\in\mathcal{A}_\alpha} \sum_{i,j\in[c],i<j} \frac{n_i^{(n)} n_j^{(n)}}{n^2} \cdot D(P^{(n)}_{X,X'|C_i,C_j} \| (1-\beta_{i,j}) P^{(n)}_{X|C_i,C_j} P^{(n)}_{X'|C_i,C_j} + \beta_{i,j} P^{(n)}_{X,X'|C_i,C_j})$$

$$+ \sum_{i\in[c]} \frac{n_i^{(n)}(n_i^{(n)}-1)}{2n^2} \cdot D(P^{(n)}_{X,X'|C_i,C_i} \| (1-\beta_i) P^{(n)}_{X|C_i,C_i} P^{(n)}_{X'|C_i,C_i} + \beta_i P^{(n)}_{X,X'|C_i,C_i}), \tag{10}$$

as $n \to \infty$, where $\mathcal{A}_\alpha = \{([\alpha_i]_{i\in[c]}) : \alpha_i \leq \frac{n_i^{(n)}}{n}, \sum_{i\in[c]} \alpha_i = \alpha\}$, and $\beta_{i,j} = \frac{n^2}{n_i^{(n)} n_j^{(n)}} \alpha_i \alpha_j, i, j \in [c]$ and $\beta_i = \frac{n\alpha_i(n\alpha_i-1)}{n_i^{(n)}(n_i^{(n)}-1)}, i \in [c]$. The maximal family of sets of distributions which are achievable using the typicality matching scheme with complete side-information is denoted by $\mathcal{P}_{full}$.

Proof. Appendix I. □

Remark 14. *Note that the community sizes $(n_1^{(n)}, n_2^{(n)}, \cdots, n_c^{(n)}), n \in \mathbb{N}$ are assumed to grow in n such that $\lim_{n\to\infty} \frac{n_i^n}{n} > 0$.*

Theorem 3 recovers to the following achievable region for matching of pairs of Erdős-Rènyi graphs derived in Theorem 4.

C. Matching in Absence of Side-information

The scheme described in the previous section can be extended to matching graphs without community memberships side-information. In this scenario, it is assumed that the distribution $P_{X,X'|C_{j_1},C_{j_2},C'_{j'_1},C'_{j'_2}}, j_1, j_2, j'_1, j'_2 \in [1, c]$ is known, but the community memberships of the vertices in the graphs are not known. In this case, the scheme sweeps over all possible possible community

membership assignments of the vertices in the two graphs. For each community membership assignment, the scheme attempts to match the two graphs using the method proposed in the complete side-information scenario. If it finds a labeling which satisfies the joint typicality conditions, it declares the labeling as the correct labeling. Otherwise, the scheme proceeds to the next community membership assignment. More precisely, for a given community assignment $(\hat{C}, \hat{C}')$, the scheme forms the following ambiguity set

$$\widehat{\Sigma}_{\hat{C},\hat{C}'} = \{\hat{\sigma}' | (U_{\sigma,\hat{C}_i,\hat{C}_i}, U'_{\hat{\sigma}',\hat{C}'_i,\hat{C}'_i}) \in \mathcal{A}_\epsilon^{\frac{n_i(n_i-1)}{2}}(P_{X,X'|\hat{C}_i,\hat{C}_i,\hat{C}'_i,\hat{C}'_i}), \forall i \in [c],$$
$$(G_{\sigma,\hat{C}_i,\hat{C}_j}, \widetilde{G}'_{\hat{\sigma}',\hat{C}'_i,\hat{C}'_j}) \in \mathcal{A}_\epsilon^{n_i n_j}(P_{X,X'|\hat{C}_i,\hat{C}_j,\hat{C}'_i,\hat{C}'_j}), \forall i, j \in [c], i \neq j\}.$$

Define $\widehat{\Sigma}_0$ as follows:

$$\widehat{\Sigma}_0 = \cup_{(\hat{C},\hat{C}') \in \mathsf{C}} \widehat{\Sigma}_{\hat{C},\hat{C}'}.$$

where C is the set of all possible community membership assignments. The scheme outputs a randomly and uniformly chosen element of $\widehat{\Sigma}_0$ as the correct labeling. The following theorem shows that the achievable region for this scheme is the same as the one described in Theorem 4.

Theorem 5. *Let $\mathcal{P}_0$ be the maximal family of sets of achievable distributions for the typicality matching scheme without side-information. Then, $\mathcal{P}_0 = \mathcal{P}_{full}$.*

The proof follows similar arguments as that of Theorem 4. We provide an outline. It is enough to show that $|\widehat{\Sigma}_0|$ has the same exponent as that of $|\widehat{\Sigma}_{C,C'}|$. To see this note that the size of the set of all community membership assignments C has an exponent which is $\Theta(n)$:

$$|\mathsf{C}| \leq 2^{cn}.$$

On the other hand,

$$|\widehat{\Sigma}_0| \leq |\mathsf{C}| \cdot |\widehat{\Sigma}_{C,C'}| \leq 2^{nc} \cdot 2^{\Theta(n \log n)} = 2^{\Theta(n \log n)}.$$

The rest of the proof follows by the same arguments as in Theorem 4.

VII. Matching Collections of Graphs

In the previous sections, we considered matching of pairs of correlated graphs. The results can be further extended to problems involving matching of collections of more than two graphs.

In this section, we consider matching collections of more than two correlated graphs, where the first graph is deanonymized and the other graphs are anonymized. For brevity we consider collections of correlated Erdös-Rényi graphs, i.e. single-community random graphs. The results can be further exteneded to correlated graphs with community structure in a straightforward manner. The following formally describes a collection of correlated Erdös-Rényi graphs.

Definition 24 (**Correlated Collection of ER Graphs).** *Let P_{X^m} be a conditional distribution defined on $\prod_{k\in[m]}\mathcal{X}_i$, where $\mathcal{X}_i = [0, l-1], i \in [m]$ and $m > 2$. A correlated collection of ER graphs $\underline{\tilde{g}} = (\tilde{g}^i)_{i\in[m]}$ generated according to P_{X^m} is characterized by: i) the collection of ER graphs $(g^i)_{i\in[m]}$ each generated according to P_{X_i}, ii) the collection of labelings $(\sigma_i)_{i\in[m]}$ for the unlabeled graphs $(g^i)_{i\in[m]}$, and iii) the joint probability distribution P_{X^m}, such that:*
1)The graphs have the same set of vertices $\mathcal{V} = \mathcal{V}_i, i \in [m]$.
2) For any collection of edges $e^i = (x^i, v_{j_1^i}, v_{j_2^i}), x^i \in [0, l-1], i \in [m]$, we have

$$Pr\left(e^i \in \mathcal{E}^i, i \in [m]\right) = \begin{cases} P_{X^m}(x^m), & \text{if } \sigma^i(v_{j_l^i}) = \sigma^k(v_{j_l^k}), \forall i,k \in [m] \\ \prod_{i\in[m]} P_{X_i}(x_i), & \text{Otherwise} \end{cases},$$

where $l \in \{1, 2\}$, and $v_{j_1^i}, v_{j_2^i} \in \mathcal{V}_1 \times \mathcal{V}_2, i \in [m]$.

Similar to the Typicality Matching Strategy for pairs of correlated graphs described in Section V, we propose a matching strategy based on typicality for collections of correlated graphs. Given a correlated collection of graphs $(g^i)_{i\in[m]}$, where the labeling for $\tilde{g}^1$ is given and the rest of the graphs are ananymized, the typicality matching strategy operates as follows. The scheme finds a collection $\widehat{\Sigma}$ of labelings $\hat{\sigma}^j, j \in [2, m]$, for which the UT's $U^j_{\sigma^j}, j \in [m]$ are jointly typical with respect to P_{n,X^m} when viewed as vectors of length $\frac{n(n-1)}{2}$. The strategy succeeds if at least one such labeling exists and fails otherwise.

Theorem 6. *For the typicality matching strategy, a given family of sets of distributions $\widetilde{P} = (\mathcal{P}_n)_{n\in\mathbb{N}}$ is achievable, if for every sequence of distributions $P_{n,X^m} \in \mathcal{P}_n, n \in \mathbb{N}$ we have*

$$\frac{\log n}{n}\Big(\sum_{k\in[b_m]} |\mathcal{P}_k|\alpha_k - 1\Big) \leq \frac{1}{2b_m m(m-1)} D(P_{X^m} \| \sum_{k\in[b_m]} \alpha'_k P_{X_{\mathcal{P}_k}}) + O(\frac{\log n}{n}), \tag{11}$$

for all $\alpha_1, \alpha_2, \cdots, \alpha_{b_m} : \sum_{k\in[b_m]} \alpha_k = n, \alpha_{b_m} \in [1, 1-\alpha_n]$, where $\alpha'_k = \frac{\alpha_k^2}{2} + \sum_{k',k'':\mathcal{P}_{k',k''}=\mathcal{P}_l} \alpha_{k'}\alpha_{k''}$, $\mathcal{P}_{k',k''} = \{\mathcal{A}' \cap \mathcal{A}'' : \mathcal{A}' \in \mathcal{P}_{k'}, \mathcal{A}'' \in \mathcal{P}_{k''}\}, k', k'' \in [b_m]$, and $\mathcal{P}_{b_m} = [1, n]$ is the single-element partition.

Proof. Appendix J. □

Remark 15. *Note that Equation* (11) *recovers the result given in Equation* (9) *for matching of pairs of correlated ER graphs, i.e.* $m = 2$.

VIII. Converse Results

In this section, we provide conditions on the graph parameters under which graph matching is not possible. Without loss of generality, we assume that (σ, σ') are a pair of random labelings chosen uniformly among the set of all possible labeling for the two graphs. Roughly speaking, the information revealed by identifying the realization of σ' is equal to $H(\sigma') \approx n \log n$. Consequently, using Fano's inequality, we show that the information contained in (σ, G, G') regarding σ', which is quantified as the mutual information $I(\sigma'; \sigma, G, G')$, must be at least $n \log n$ bits for successful matching. The mutual information $I(\sigma'; \sigma, G, G')$ is a function of multi-letter probability distributions. We use standard information theoretic techniques to bound $I(\sigma'; \sigma, G, G')$ using information quantities which are functionals of single-letter distributions. The following states the resulting necessary conditions for successful matching.

Theorem 7. *For the graph matching problem under the community structure model with complete side-information, the following provides necessary conditions for successful matching:*

$$\frac{\log n}{n} \leq \sum_{i,j \in [c], i<j} \frac{n_i n_j}{n^2} I(X, X' | C_i, C_j, C'_i C'_j) + \sum_{i \in [c]} \frac{n_i(n_i - 1)}{2n^2} I(X, X' | C_i, C_i, C'_i, C'_i) + O(\frac{\log n}{n}),$$

where $I(X, X' | C_i, C_j, C'_i C'_j)$ *is defined with respect to* $P_{X,X'|C_i,C_j,C'_i C'_j}$.

Proof. Appendix K. □

For Erdős-Rènyi graphs, the following corollary is a direct consequence of Theorem 7.

Corollary 1. *For the graph matching problem under the Erdős-Rènyi model, the following provides necessary conditions for successful matching:*

$$\frac{2 \log n}{n} \leq I(X, X') + O(\frac{\log n}{n}).$$

IX. Criteria for Successful Matching

In Section III, it was pointed out that the criterion for successful matching defined in Definition 23 requires the fraction of correctly matched vertices to approach one as the size of the graph

grows asymptotically large. This is a relaxation of the criterion considered in prior works [20], [26], [29] where a matching scheme is said to be successful if it matches every vertex correctly simultaneously with probability approaching one as the size of the graph grows asymptotically large. In this section, we show that for pairs of Erdös-Rènyi graphs with binary-valued edges, the necessary and sufficient conditions on the edge statistics which guarantee successful matching are equivalent under the two success criteria. The results can be potentially extended to graphs with community structure, non binary-valued edges, and collections of graphs considered in the previous sections. Consequently, the conditions derived in this work are applicable under the scenarios considered in the prior works as well. We use the following proposition to prove the equivalency of the success criteria.

Proposition 2. *Let $\underline{\tilde{g}}$ be a CPER distributed according to $P_{X,X'}$ and let G and G' be the corresponding adjacency matrices. Let (S^n, S'^n) be the first row in G and G', respectively. Let S''^n be the second row in G. Assume that the triple of vectors (T^n, T'^n, T''^n) are such that they are jointly equal to (S^n, S'^n, S''^n) in $(1-\alpha)$ fraction of their elements, where $\alpha \in [0,1]$. Alternatively,*

$$1 - \alpha = \frac{1}{n} \sum_{i \in [1,n]} \mathbb{1}((S_i, S'_i, S''_i) = (T_i, T'_i, T''_i)).$$

Then, there exist a binary hypothesis test $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and function $\zeta : [0,1] \to [0,\infty)$, such that:

$$P(f(T^n, T'^n) = 1) \geq \beta_n,$$
$$P(f(T''^n, T'^n) = 1) \leq 2^{-n\zeta(\alpha)I(X;X')},$$

where $\zeta(\alpha) \to 1$ as $\alpha \to 0$, and $\beta_n \to 1$ as $n \to \infty$.

X. Seeded Graph Matching

So far, we have investigated the fundamental limits of graph matching assuming the availability of unlimited computational resources. In this section, we consider seeded graph matching, and propose a matching algorithm whose complexity grows polynomially in the number of vertices of the graph and leads to successful matching in a wide range of graph matching scenarios. The algorithm leverages ideas from prior work a related problem called *online fingerprinting* which involves matching of correlated bipartite graphs [34].

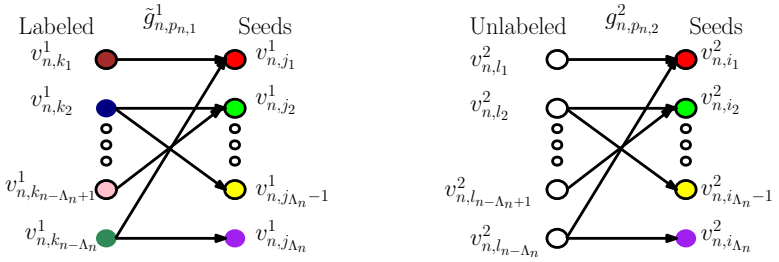

Fig. 2. The matching algorithm constructs the bipartite graph which captures the connections between the unmatched vertices with the seed vertices.

In seeded graph matching, it is assumed that we are given the correct labeling for a subset of the vertices in the anonymized graph prior to the start of the matching process. The subset of pre-matched vertices are called '*seeds*'. The motivation behind the problem formulation is that in many applications of graph matching, the correct labeling of a subset of vertices is known through side-inforamtion. For instance, in social network deanonymization, many users link their social media accounts across social networks publicly. As shown in this section, the seed side-information can be used to significantly reduce the complexity of the matching algorithm.

The proposed graph matching algorithm operates as follows. First, the algorithm constructs the bipartite graph shown in Figure 2 whose edges consist of the connections between the unmatched vertices with the seeded vertices in each graph. The algorithm proceeds in two steps. First, it constructs the '*fingerprint*' vectors for each of the unmatched vertices in the two bipartite graphs based on their connections to the seed vertices. The fingerprint vector of a vertex is the row in the adjacency matrix of the bipartite graph corresponding to the edges between that vertex and the seed vertices. In the second step, the algorithm finds a jointly typical pair of fingerprint vectors in the deanonymized and deanonymized graph adjacency matrices and matches the corresponding vertices, where typicality is defined based on the joint distribution between the edges of the two graphs. Note that the bipartite graphs encompass only a subset of the edges in the original graphs. Hence by restricting the matching process to the bipartite graphs, some of the information which could potentially help in matching is ignored. This leads to more restrictive conditions on successful matching compared to the ones derived in the previous sections. However, the computational complexity of the resulting matching algorithm is considerably improved. In the following, we focus on matching of seeded CPERs. The results can be easily extended to seeded CPCSs similar to the unseeded graph matching in prior sections. A seeded CPER (SCPER) is

formally defined below.

Definition 25 (**Correlated Pair of Seeded ER Graphs).** *An SPCER is a triple* $(\tilde{g}, \tilde{g}', \mathcal{S})$*, where* $\underline{\tilde{g}} = (\tilde{g}, \tilde{g}')$ *is a CPER generated according to* $P_{X,X'}$*, and* $\mathcal{S} \subseteq \mathcal{V}$ *is the seed set.*

Let $\mathcal{S} = \{v_{i_1}, v_{i_2}, \cdots, v_{i_\Lambda}\}$ and define the reverse seed set $\mathcal{S}^{-1} = \{v_{j_1}, v_{j_2}, \cdots, v_{j_\Lambda}\}$, where $\sigma(v_{j_k}) = \sigma'(v_{i_k}), k \in [1, \Lambda]$. The algorithm is given the correct labeling of all the vertices in the first graph $\sigma : \mathcal{V} \to [1, n]$ and the seed vertices in the second graph $\sigma'|_{\mathcal{S}} : \mathcal{S} \to [1, n]$. The objective is to find the correct labeling of the rest of the vertices in the second graph $\hat{\sigma}_n : \mathcal{V}; \to [1, n]$ so that the fraction of mislabeled vertices is negligible as the number of vertices grows asymptotically large, i.e. $P(\hat{\sigma}' = \sigma') \to 1$ as $n \to \infty$. To this end, the algorithm first constructs a fingerprint for each vertex in each of the graphs. For an arbitrary vertex v_i in g_{P_X}, its fingerprint is defined as the vector $\underline{F}_i = (F_i(1), F_i(2), \cdots, F_i(\Lambda))$. which indicates its connections to the reverse seed elements:

$$F_i(l) = \begin{cases} 1 & \text{if} \quad (v_i, v_{j_l}) \in \mathcal{E} \\ 0 & \text{Otherwise} \end{cases}, \qquad l \in [1, \Lambda].$$

The fingerprint of a vertex v_i in the second graph is defined in a similar fashion based on connections to the elements of the seed set $\mathcal{S}$. Take an unmatched vertex $v_i \notin \mathcal{S}$. The algorithm matches v_i in g to a vertex v_j in g' if it is the unique vertex such that the fingerprint pair $(\underline{F}_i, \underline{F}'_j)$ are jointly ϵ-typical with respect to the distribution $P_{X,X'}$, where[4] $\epsilon = \omega(\frac{1}{\sqrt{\Lambda}})$:

$$\exists! i : (\underline{F}_i, \underline{F}'_j) \in \mathcal{A}^n_\epsilon(X, X') \Rightarrow \hat{\sigma}(v_i) = \sigma'(v_j),$$

where $\mathcal{A}^n_\epsilon(X, X')$ is the set of jointly ϵ-typical set sequences of length n with respect to $P_{X,X'}$. If a unique match is not found, then vertex v_i is added to the ambiguity set $\mathcal{L}$. Hence, $\mathcal{V} \backslash \mathcal{L}$ is the set of all matched vertices. In the next step, these vertices are added to the seed set and the expanded seed set is used to match the vertices in the ambiguity set. The algorithm succeeds if all vertices are matched at this step and fails otherwise. We call this strategy the Seeded Typicality Matching Strategy (STMS).

Theorem 8. *Define the family of sets of pairs of distribution and seed sizes* $\widetilde{\mathcal{P}}$ *as follows:*

$$\widetilde{\mathcal{P}} = \left\{ (\mathcal{P}_n, \Lambda_n)_{n \in \mathbb{N}} \middle| \forall P_{n,X,X'} \in \mathcal{P}_n : \frac{2 \log n}{I(X, X')} \leq \Lambda_n, I(X; X') = \omega\left(\sqrt{\frac{1}{\Lambda_n}} \right) \right\}.$$

[4] Alternatively, $\lim_{n \to \infty} \frac{\epsilon}{\sqrt{|\mathcal{S}|}} = \infty$.

Any family of SCPERs with parameters chosen from $\widetilde{\mathcal{P}}$ is matchable using the STMS.

The proof of Theorem 8 which is provided in Appendix M uses the following lemma on the cardinality of $\mathcal{L}$.

Lemma 7. *The following holds:*

$$P(|\mathcal{L}| > \frac{2n}{\Lambda\epsilon^2}) \to 0, \ as \ n \to \infty,$$

Proof. Appendix L. □

XI. Conclusion

We have considered matching of collections of correlated graphs. We have studied the problem under the Erdös-Rènyi model as well as the more general community structure model. The derivations apply to graphs whose edges may take non-binary attributes. We have introduced a graph matching scheme called the Typicality Matching scheme which relies on tools such as concentration of measure and typicality of sequences of random variables to perform graph matching. We further provide converse results which lead to necessary conditions on graph parameters for successful matching. We have investigated seeded graph matching, where the correct labeling of a subset of graph vertices is known prior to the matching process. We have introduced a matching algorithm for seeded graph matching which successfully matches the graphs in wide range of matching problems with large enough seeds and has a computational complexity which grows polynomially in the number of graph vertices.

Appendix A
Proof of Theorem 1

Define the following partition for the set of indices $[1, n]$:

$$\mathcal{A}_0 = \{1, i_1 + 1, i_1 + i_2 + 1, \cdots, \sum_{j=1}^{r-1} i_j + 1\}, \quad \mathcal{A}_1 = \{k|\text{k is even}, \ \& \ k \notin \mathcal{A}_0, \ \& \ k \leq \sum_{i=1}^{r} i_j\},$$

$$\mathcal{A}_2 = \{k|\text{k is odd}, \ \& \ k \notin \mathcal{A}_0, \ \& \ k \leq \sum_{i=1}^{r} i_j\}, \quad \mathcal{A}_3 = \{k|k > \sum_{i=1}^{r} i_j\}.$$

The set $\mathcal{A}_1$ is the set of indices at the start of each cycle in π, the sets $\mathcal{A}_2$ and $\mathcal{A}_3$ are the sets of odd and even indices which are not start of any cycles and $\mathcal{A}_4$ is the set of fixed points of π. Let $Z^n = \pi(Y^n)$. It is straightforward to verify that $(X_i, Z_i), i \in \mathcal{A}_j, j \in [3]$ are three sequences of independent and identically distributed variables which are distributed according to $P_X P_Y$. The reason is that the standard permutation shifts elements of a sequence by at most one position, whereas the elements in the sequences $(X_i, Z_i), i \in \mathcal{A}_j, j \in [3]$ are at least two indices apart and are hence independent of each other (i.e. $Z_i \neq Y_i$). Furthermore, $(X_i, Z_i), i \in \mathcal{A}_4$ is a sequence of independent and identically distributed variables which are distributed according to $P_{X,Y}$ since $Z_i = Y_i$. Let $\underline{T}_j, j \in [4]$ be the type of the sequence $(X_i, Z_i), i \in \mathcal{A}_j, j \in [4]$, so that $T_{j,x,y} = \frac{\sum_{i \in \mathcal{A}_j} \mathbb{1}(X_i = x, Z_i = y)}{|\mathcal{A}_j|}, j, x, y \in [4] \times \mathcal{X} \times \mathcal{Y}$. We are interested in the probability of the event $(X^n, Z^n) \in \mathcal{A}_\epsilon^n(X, Y)$. From Definition 8 this event can be rewritten as follows:

$$P\left((X^n, Z^n) \in \mathcal{A}_\epsilon^n(X, Y)\right) = P\left(\underline{T}(X^n, Y^n) \doteq P_{X,Y}(\cdot, \cdot) \pm \epsilon\right)$$

$$= P(\alpha_1 \underline{T}_1 + \alpha_2 \underline{T}_2 + \alpha_3 \underline{T}_3 + \alpha_4 \underline{T}_4 \doteq P_{X,Y}(\cdot, \cdot) \pm \epsilon),$$

where $\alpha_i = \frac{|\mathcal{A}_i|}{n}, i \in [4]$, we write $a \doteq x \pm \epsilon$ to denote $x - \epsilon \leq a \leq x_\epsilon$, and addition is defined element-wise. We have:

$$P((X^n, Z^n) \in \mathcal{A}_\epsilon^n(X, Y)) = \sum_{(\underline{t}_1, \underline{t}_2, \underline{t}_3, \underline{t}_4) \in \mathcal{T}} P(\underline{T}_i = \underline{t}_i, i \in [4]),$$

where $\mathcal{T} = \{(\underline{t}_1, \underline{t}_2, \underline{t}_3, \underline{t}_4) : \alpha_1 \underline{t}_1 + \alpha_2 \underline{t}_2 + \alpha_3 \underline{t}_3 + \alpha_4 \underline{t}_4 \doteq n(P_{X,Y}(\cdot, \cdot) \pm \epsilon)\}$. Using the property that for any set of events, the probability of the intersection is less than or equal to the geometric average of the individual probabilities, we have:

$$P((X^n, Z^n) \in \mathcal{A}_\epsilon^n(X, Y)) \leq \sum_{(\underline{t}_1, \underline{t}_2, \underline{t}_3, \underline{t}_4) \in \mathcal{T}} \sqrt[4]{\Pi_{i \in [4]} P(\underline{T}_i = \underline{t}_i)}.$$

Since the elements $(X_i, Z_i), i \in \mathcal{A}_j, j \in [4]$ are i.i.d, it follows from standard information theoretic arguments [32] that:

$$P(\underline{T}_i = \underline{t}_i) \leq 2^{-|\mathcal{A}_i|(D(\underline{t}_i \| P_X P_Y) - |\mathcal{X}\|\mathcal{Y}|\epsilon)}, i \in [3], \quad P(\underline{T}_4 = \underline{t}_4) \leq 2^{-|\mathcal{A}_4|(D(\underline{t}_4 \| P_{X,Y}) - |\mathcal{X}\|\mathcal{Y}|\epsilon)}.$$

We have,

$$P((X^n, Z^n) \in \mathcal{A}_\epsilon^n(X, Y))$$

$$\leq \sum_{(\underline{t}_1, \underline{t}_2, \underline{t}_3, \underline{t}_4) \in \mathcal{T}} \sqrt[4]{2^{-n(\alpha_1 D(\underline{t}_1 \| P_X P_Y) + \alpha_2 D(\underline{t}_2 \| P_X P_Y) + \alpha_3 D(\underline{t}_3 \| P_X P_Y) + \alpha_4 D(\underline{t}_4 \| P_{X,Y}) - |\mathcal{X}\|\mathcal{Y}|\epsilon)}}$$

$$\overset{(a)}{\leq} \sum_{(\underline{t}_1,\underline{t}_2,\underline{t}_3,\underline{t}_4)\in\mathcal{T}} \sqrt[4]{2^{-n(D(\alpha_1\underline{t}_1+\alpha_2\underline{t}_2+\alpha_3\underline{t}_3+\alpha_4\underline{t}_4\|(\alpha_1+\alpha_2+\alpha_3)P_XP_Y+\alpha_4P_{X,Y})-|\mathcal{X}\|\mathcal{Y}|\epsilon)}}$$

$$= |\mathcal{T}|\sqrt[4]{2^{-n(D(P_{X,Y}\|(1-\alpha)P_XP_Y+\alpha P_{X,Y})-|\mathcal{X}\|\mathcal{Y}|\epsilon)}}$$

$$\overset{(b)}{\leq} 2^{-\frac{n}{4}(D(P_{X,Y}\|(1-\alpha)P_XP_Y+\alpha P_{X,Y})-|\mathcal{X}\|\mathcal{Y}|\epsilon+O(\frac{\log n}{n}))},$$

where the (a) follows from the convexity of the divergence function and (b) follows by the fact that the number of joint types grows polynomially in n. □

Appendix B
Proof of Lemma 2

First, we prove Equation (2). Note that

$$N_m = \binom{n}{m}!(n-m) \leq \binom{n}{m}(n-m)! = \frac{n!}{m!} \leq n^{n-m}.$$

This proves the right hand side of the equation. To prove the left hand side, we first argue that the iterative inequality $!n \geq !(n-1)(n-1)$ holds. In other words, the number of derangements of numbers in the interval $[n]$ is at least $n-1$ times the number of derangements of the numbers in the interval $[n-1]$. We prove the statement by constructing $!(n-1)(n-1)$ distinct derangements of the numbers $[n]$. Note that a derangement $\pi(\cdot)$ of $[n]$ is characterized by the vector $(\pi(1), \pi(2), \cdots (n))$. There are a total of $n-1$ choices for $\pi(1)$ (every integer in $[n]$ except for 1). Once $\pi(1)$ is fixed, the rest of the vector $(\pi(2), \pi(3), \cdots, \pi(n))$ can be constructed using any derangement of the set of numbers $[n]-\{\pi(1)\}$. There are a total of $!(n-1)$ such derangements. So, we have constructed $(n-1)!(n-1)$ distinct derangements of $[n]$. Consequently. $!n \geq !(n-1)(n-1)$. By induction, we have $!n \geq (n-1)!$. So,

$$N_m = \binom{n}{m}!(n-m) \geq \binom{n}{m}(n-m-1)! = \frac{n!}{m!(n-m)}.$$

Next, we prove that Equation (3) holds. Note that from the right hand side of Equaation (2) we have:

$$\lim_{n\to\infty} \frac{\log N_m}{n\log n} \leq \lim_{n\to\infty} \frac{\log n^{n-m}}{n\log n} = \lim_{n\to\infty} \frac{n-m}{n} = 1-\alpha.$$

Also, from the left hand side of Equation (3), we have:

$$\lim_{n\to\infty} \frac{\log N_m}{n\log n} \geq \lim_{n\to\infty} \frac{\log \frac{n!}{m!(n-m)}}{n\log n} = \lim_{n\to\infty} \frac{\log \frac{n!}{m!}}{n\log n} - \frac{\log (n-m)}{n\log n}.$$

The second term in the last inequality converges to 0 as $n \to \infty$. Hence,

$$\begin{aligned}
&\lim_{n\to\infty} \frac{\log N_m}{n \log n} \geq \lim_{n\to\infty} \frac{\log \frac{n!}{m!}}{n \log n} \\
&\overset{(a)}{\geq} \lim_{n\to\infty} \frac{\log \frac{n!}{m^m}}{n \log n} \geq \lim_{n\to\infty} \frac{\log n!}{n \log n} - \frac{\log m^m}{n \log n} \overset{(b)}{\geq} \lim_{n\to\infty} \frac{n \log n - n + O(\log n)}{n \log n} - \frac{\log m^m}{n \log n} \\
&= \lim_{n\to\infty} \frac{n \log n}{n \log n} - \frac{\alpha n \log \alpha n}{n \log n} = 1 - \alpha,
\end{aligned}$$

where in (a) we have used the fact that $m! \leq m^m$, and (b) follows from Stirling's approximation. This completes the proof. □

Appendix C
Proof of Lemma 3

The proof builds upon some of the techniques developed in [35]. Let $\mathcal{A} = \{(x, y) \in \mathcal{X} \times \mathcal{Y} \big| P_X P_Y(x, y) < P_{X,Y}(x, y)\}$. Let $Z_{(\pi),i}^{\{(x,y)\}} = \mathbb{1}(X_i, Y_{\pi(i)} = (x, y))$. We have:

$$\begin{aligned}
&P((X^n, \pi(Y^n)) \in \mathcal{A}_\epsilon^n(X, Y)) \leq \\
&P\Big(\Big(\bigcap_{(x,y)\in\mathcal{A}} \{\frac{1}{n}\sum_{i=1}^n Z_{(\pi),i}^{\{(x,y)\}} > P_{X,Y}(x, y) - \epsilon\}\Big) \bigcap \Big(\bigcap_{(x,y)\in\mathcal{A}^c} \{\frac{1}{n}\sum_{i=1}^n Z_{(\pi),i}^{\{(x,y)\}} < P_{X,Y}(x, y) + \epsilon\}\Big)\Big)
\end{aligned}$$

For brevity let $\alpha_{x,y} = \frac{1}{n}\sum_{i=1}^n Z_{(\pi),i}^{\{(x,y)\}}$, and $t_{x,y} = \frac{1}{2}\log_e \frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}$, $x, y \in \mathcal{X}$. Then,

$$\begin{aligned}
&Pr\Big(\Big(\bigcap_{(x,y)\in\mathcal{A}} \{n\alpha_{x,y} > nP_{X,Y}(x, y) - n\epsilon\}\Big) \bigcap \Big(\bigcap_{(x,y)\in\mathcal{A}^c} \{n\alpha_{x,y} < nP_{X,Y}(x, y) + n\epsilon\}\Big)\Big) \\
&= Pr\Big(\bigcap_{(x,y)\in\mathcal{X}\times\mathcal{Y}} \{e^{nt_{x,y}\alpha_{x,y}} > e^{nt_{x,y}P_{X,Y}(x,y)+n\epsilon_{x,y}}\}\Big),
\end{aligned}$$

where $\epsilon_{x,y} = t_{x,y}(1 - 2\mathbb{1}(x, y \in \mathcal{A}))\epsilon$ and we have used the fact that by construction:

$$\begin{cases} t_{x,y} > 0 & \text{if} \quad (x, y) \in \mathcal{A} \\ t_{x,y} < 0 & \text{if} \quad (x, y) \in \mathcal{A}^c. \end{cases} \tag{12}$$

So,

$$\begin{aligned}
&P\Big(\Big(\bigcap_{(x,y)\in\mathcal{A}} \{n\alpha_{x,y} > nP_{X,Y}(x, y) - n\epsilon\}\Big) \bigcap \Big(\bigcap_{(x,y)\in\mathcal{A}^c} \{n\alpha_{x,y} < nP_{X,Y}(x, y) + n\epsilon\}\Big)\Big) \\
&\overset{(a)}{\leq} P\Big(\prod_{(x,y)\in\mathcal{X}\times\mathcal{Y}} e^{nt_{x,y}\alpha_{x,y}} > \prod_{(x,y)\in\mathcal{X}\times\mathcal{Y}} e^{nt_{x,y}P_{X,Y}(x,y)-n\epsilon_{x,y}}\Big) \qquad (13) \\
&\overset{(b)}{\leq} e^{-\sum_{x,y} n(t_{x,y}P_{X,Y}(x,y)-\epsilon_{x,y})}\mathbb{E}\Big(\prod_{x,y} e^{nt_{x,y}\alpha_{x,y}}\Big) = e^{-\sum_{x,y} n(t_{x,y}P_{X,Y}(x,y)-\epsilon_{x,y})}\mathbb{E}\Big(e^{\sum_{i=1}^n \sum_{x,y} t_{x,y}Z_{(\pi),i}^{\{(x,y)\}}}\Big) \qquad (14)
\end{aligned}$$

$$\overset{(c)}{\leq} e^{-\sum_{x,y} n(t_{x,y}P_{X,Y}(x,y)-\epsilon_{x,y})}\mathbb{E}^{\frac{1}{2}}(e^{\sum_{i\in\mathcal{O}}\sum_{x,y}2t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}})\mathbb{E}^{\frac{1}{2}}(e^{\sum_{i\in\mathcal{E}}\sum_{x,y}2t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}}) \tag{15}$$

$$= e^{-\sum_{x,y} n(t_{x,y}P_{X,Y}(x,y)-\epsilon_{x,y})}\prod_{i\in\mathcal{O}}\mathbb{E}^{\frac{1}{2}}(e^{\sum_{x,y}2t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}})\prod_{i\in\mathcal{E}}\mathbb{E}^{\frac{1}{2}}(e^{\sum_{x,y}2t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}}), \tag{16}$$

where $\mathcal{O}$ and $\mathcal{E}$ are the odd and even indices in the set $[1,n]$. In (a) we have used the fact that the exponential function is increasing and positive, (b) follows from the Markov inequality and (c) follows from the Cauchy-Schwarz inequality. Note that:

$$\mathbb{E}(e^{\sum_{x,y}2t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}}) \overset{(a)}{=} \sum_{x,y}P_X(x)P_Y(y)e^{2t_{x,y}} = \sum_{x,y}P_X(x)P_Y(y)e^{\log_e\frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}} = \sum_{x,y}P_{X,Y}(x,y) = 1,$$

where in (a) we have used the fact that X_i and $Y_{\pi(i)}$ are independent since the permutation does not have any fixed points. Consequently, we have shown that:

$$Pr((X^n,\pi(Y^n))\in\mathcal{A}^n_\epsilon(X,Y)) \leq e^{-\sum_{x,y} n(t_{x,y}P_{X,Y}(x,y)-\epsilon_{x,y})} = e^{-\sum_{x,y} n(\frac{1}{2}P_{X,Y}(x,y)\log_e\frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}-\epsilon_{x,y})} = 2^{-\frac{1}{2}n(I(X;Y)-\delta)}.$$

This completes the proof.

□

Appendix D
Proof of Lemma 4

The proof follows by similar arguments as that of Lemma 3. Following similar steps, we have

$$P((X^n,\pi(Y^n))\in\mathcal{A}^n_\epsilon(X,Y)) = Pr\Big(\bigcap_{(x,y)\in\mathcal{X}\times\mathcal{Y}}\{e^{\frac{n}{s}t_{x,y}\alpha_{x,y}} > e^{\frac{n}{s}t_{x,y}P_{X,Y}(x,y)+n\epsilon_{x,y}}\}\Big)$$

$$\leq P\Big(\prod_{(x,y)\in\mathcal{X}\times\mathcal{Y}}e^{\frac{n}{s}t_{x,y}\alpha_{x,y}} > \prod_{(x,y)\in\mathcal{X}\times\mathcal{Y}}e^{\frac{n}{s}t_{x,y}P_{X,Y}(x,y)-\frac{n}{s}\epsilon_{x,y}}\Big)$$

$$\leq e^{-\sum_{x,y}\frac{n}{s}(t_{x,y}P_{X,Y}(x,y)-\epsilon_{x,y})}\mathbb{E}(\prod_{x,y}e^{\frac{n}{s}t_{x,y}\alpha_{x,y}})$$

$$= e^{-\sum_{x,y}\frac{n}{s}(t_{x,y}P_{X,Y}(x,y)-\epsilon_{x,y})}\prod_{j\in[1,c]}\mathbb{E}(e^{\frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j}t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}}). \tag{17}$$

We need to investigate $\mathbb{E}(e^{\frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j}t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}})$. Define $T^{(x,y)}_j = \sum_{k=1}^{i_j}Z^{\{(x,y)\}}_{(\pi),i}$, $j\in[1,c], x,y\in\mathcal{X}\times\mathcal{Y}$ as the number of occurrences of the pair (x,y) in the jth cycle. Note that by definition, we have $\sum_{x,y}\sum_{k=1}^{i_j}Z^{\{(x,y)\}}_{(\pi),i} = \sum_{x,y}T^{(x,y)}_j = i_j$. Define $S^{(x,y)}_j = \frac{1}{s}T^{(x,y)}_j$, $j\in[1,c], x,y\in\mathcal{X}\times\mathcal{Y}$. Let $\mathcal{B} = \{(s^{(x,y)}_j)_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}} : \sum_{x,y}s^{(x,y)}_j = \frac{i_j}{s}, j\in[1,c]\}$ be the set of feasible values for the vector $(S^{(x,y)}_j)_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}$. We have:

$$\mathbb{E}(e^{\frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j}t_{x,y}Z^{\{(x,y)\}}_{(\pi),i}}) = \mathbb{E}(e^{\sum_{x,y}t_{x,y}\frac{1}{s}\sum_{k=1}^{i_j}Z^{\{(x,y)\}}_{(\pi),i}}) = \mathbb{E}(e^{\sum_{x,y}t_{x,y}S^{(x,y)}_j})$$

$$= \sum_{(s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}\in\beta} P((s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}) e^{\sum_{x,y} t_{x,y} s_j^{\{(x,y)\}}}.$$

For a fixed vector $(s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}} \in \beta$, let $V^{(x,y)}$ be defined as the random variable for which $P(V^{(x,y)} = t_{(x,y)}) = s_j^{\{(x,y)\}}, x, y \in \mathcal{X}$ and $P(V^{(x,y)} = 0) = 1 - \frac{i_j}{s}$ (note that P_V is a valid probability distribution). We have:

$$\mathbb{E}(e^{\frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j} t_{x,y} Z_{(\pi),i}^{\{(x,y)\}}}) = \sum_{(s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}\in\beta} P((s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}) e^{\sum_{x,y} t_{x,y} s_j^{\{(x,y)\}}}$$

$$= \sum_{(s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}\in\beta} P((s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}) e^{\mathbb{E}(V^{(x,y)})} \leq \sum_{(s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}\in\beta} P((s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}) \mathbb{E}(e^{V^{(x,y)}}),$$

where we have used Jensen's inequality in the last equation. Note that by construction, we have $\mathbb{E}(e^{V^{(x,y)}}) = 1 - \frac{i_j}{s} + \sum_{x,y} s_j^{(x,y)} e^{t_{x,y}}$. Consequently:

$$\mathbb{E}(e^{\frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j} t_{x,y} Z_{(\pi),i}^{\{(x,y)\}}}) \leq \sum_{(s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}\in\beta} P((s_j^{\{(x,y)\}})_{j\in[1,c],x,y\in\mathcal{X}\times\mathcal{Y}}) (1 - \frac{i_j}{s} + \sum_{x,y} s_j^{(x,y)} e^{t_{x,y}})$$

$$= 1 - \frac{i_j}{s} + \sum_{x,y} e^{t_{x,y}} \mathbb{E}(S_j^{(x,y)}) = 1 - \frac{i_j}{s} + \sum_{x,y} e^{t_{x,y}} \mathbb{E}(\frac{1}{s}\sum_{k=1}^{i_j} Z_{(\pi),i}^{\{(x,y)\}})$$

$$= 1 - \frac{i_j}{s} + \frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j} e^{t_{x,y}} \mathbb{E}(Z_{(\pi),i}^{\{(x,y)\}}) = 1 - \frac{i_j}{s} + \frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j} e^{t_{x,y}} P_X(x) P_Y(y)$$

$$= 1 - \frac{i_j}{s} + \frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j} P_{X,Y}(x,y) = 1.$$

Setting $\mathbb{E}(e^{\frac{1}{s}\sum_{x,y}\sum_{k=1}^{i_j} t_{x,y} Z_{(\pi),i}^{\{(x,y)\}}}) \leq 1$ in Equation (17), we get:

$$P((X^n, \pi(Y^n)) \in \mathcal{A}_\epsilon^n(X,Y)) \leq e^{-\sum_{x,y}\frac{n}{s}(t_{x,y}P_{X,Y}(x,y) - \epsilon_{x,y})} = 2^{-\frac{n}{s}(I(X;Y) - \epsilon_{x,y})}.$$

□

Appendix E
Proof of Theorem 2

The proof builds upon the arguments provided in the proof of Theorem 1. Let $Y^n = \pi_j(X_{(j)}^n)_{j\in[m]}$. First, we construct a partition $\mathsf{D} = \{C_{k,l} : k \in [b_m], l \in [m(m-1)]\}$ such that each sequence of vectors $(Y_{(j),C_{k,l}})_{j\in[m]}$ is an collection of independent vectors of i.i.d variables, where $Y_{(j),C_{k,l}} = (Y_{(j),c})_{c\in C_{k,l}}$. Loosely speaking, this partitioning of the indices 'breaks' the multi-letter correlation among the sequences induced due to the permutation and allows the application of standard

information theoretic tools to bound the probability of joint typicality. The partition is constructed in two steps. We first construct a *coarse* partition $\mathsf{C} = \{C_1, C_2, \cdots, C_{b_m}\}$ of the indices $[1, n]$ for which the sequence of vectors $(Y_{(j),C_k}), j \in [m]$ is identically distributed but not necessarily independent. The set $C_k, k \in [b_m]$ is defined as the set of indices corresponding to partition $\mathcal{P}_k$, where correspondence is defined in Definition 13. Clearly, $\mathsf{C} = \{C_1, C_2, \cdots, C_{b_m}\}$ partitions $[1, n]$ since each index corresponds to exactly one partition $\mathcal{P}_k$. To verify that the elements of the sequence $(Y_{(j),C_k}), j \in [m]$ are identically distributed let us consider a fixed $k \in [b_m]$ and an arbitrary index $c \in C_k$. Then the vector $(Y_{(1),c}, Y_{(2),c}, \cdots, Y_{(m),c})$ is distributed according to $P_{X_{\mathcal{P}_k}}$. To see this, note that:

$$P_{Y_{(1),c},Y_{(2),c},\cdots,Y_{(m),c}} = P_{X_{(1),(\pi_1^{-1}(c))},X_{(2),(\pi_2^{-1}(c))},\cdots,X_{(m),(\pi_m^{-1}(c))}}$$

From the assumption that the index c corresponds to the partition $\mathcal{P}_k$, we have that $\pi_j^{-1}(c) = \pi_{j'}^{-1}(c)$ if and only if $j, j' \in \mathcal{A}_{k,r}$ for some integer $r \in [|\mathcal{P}_k|]$. Since by the theorem statement $(X_{(j)}^n)_{j\in[m]}$ is an i.i.d. sequence of vectors, the variables $X_{(j),\pi_j^{-1}(c)}$ and $X_{(j'),\pi_{j'}^{-1}(c)}$ are independent of each other if $\pi_j^{-1}(c) \neq \pi_{j'}^{-1}(c)$. Consequently,

$$P_{Y_{(1),c},Y_{(2),c},\cdots,Y_{(m),c}} = \prod_{r\in[|\mathcal{P}_k|]} P_{X_{l_1},X_{l_2},\cdots,X_{l_{|\mathcal{A}_{k,r}|}}} = P_{X_{\mathcal{P}_k}}.$$

This proves that the sequences $(Y_{(j),C_k}), j \in [m]$ are identically distributed with distribution $P_{X_{\mathcal{P}_k}}$. In the next step, we decompose the partition C to arrive at a finer partition $\mathsf{D} = \{C_{k,l} : k \in [b_m], l \in [m(m-1)]\}$ of $[1, n]$ such that $(Y_{(j),C_{k,l}})_{j\in[m]}$ is an i.i.d sequence of vectors. Let $C_k = \{c_1, c_2, \cdots, c_{|C_k|}\}, k \in [b_m]$. The previous step shows that the sequence consists of identically distributed vectors. In order to guarantee independence, we need to ensure that for any $c, c' \in C_{k,l}$, we have $\pi_j^{-1}(c) \neq \pi_{j'}^{-1}(c'), \forall j, j' \in [m]$. Then, independence of $(Y_{(j),c})_{j\in[m]}$ and $(Y_{(j),c'})_{j\in[m]}$ is guaranteed due to the independence of the sequence of vectors $(X_{(j)}^n)_{j\in[m]}$. To this end we assign the indices in C_k to the sets $C_{k,l}, l \in [m(m-1)]$ as follows:

$$c_1 \in C_{k,1}, \tag{18}$$

$$c_i \in C_{k,l} : l = \min\{l' | \nexists c' \in C_{k,l'}, j, j' \in [m] : \pi_j^{-1}(c_i) = \pi_{j'}^{-1}(c')\}, i > 1. \tag{19}$$

Note that the set $C_{k,l}$ defined in Equation (19) always exists since for any given $j \in [m]$, the value $\pi_j^{-1}(c)$ can be the same for at most m distinct indices c since each of the m permutations maps one index to $\pi_j^{-1}(c)$. Furthermore, since j takes m distinct values, there are at most $m(m-1)-1$ indices c' not equal to c for which there exists $j, j' \in [m]$ such that $\pi_j(c) = \pi_{j'}(c')$. Since there are

a total of $m(m-1)$ sets $C_{k,l}$, by the Pigeonhole Principle, there exists at least one set for which there is no element c' such that $\pi_j(c) = \pi_{j'}(c')$ for any value of j, j'. Consequently, $(Y_{(j),C_{k,l}})_{j\in[m]}$ is an i.i.d. sequence with distribution $P_{X_{\mathcal{P}_k}}$.

Let $\underline{T}_{k,l}, k \in [b_m], l \in [m(m-1)]$ be the type of the sequence of vectors $(Y_{(j),C_{k,l}})_{j\in[m]}$, so that $T_{k,l,x^m} = \frac{\sum_{c\in C_{k,l}} \mathbb{1}((Y_{(1),c},Y_{(2),c},\cdots,Y_{(m),c})=x^m)}{|C_{k,l}|}, x^m \in \mathcal{X}^m$. We are interested in the probability of the event $(Y^n_{(j)})_{j\in[m]} \in \mathcal{A}^n_\epsilon(X^m)$. From Definition 11 this event can be rewritten as follows:

$$\begin{aligned} P\left(\left(Y^n_{(j)}\right)_{j\in[m]}\right) \in \mathcal{A}^n_\epsilon(X^m)\right) &= P\left(T((Y^n_{(j)})_{j\in[m]}, x^m) \doteq P_{X^m}(x^m) \pm \epsilon, \forall x^m\right) \\ &= P(\sum_{k,l} \alpha_{k,l} T_{k,l,x^m} \doteq P_{X^m}(x^m) \pm \epsilon, \forall x^m), \end{aligned}$$

where $\alpha_{k,l} = \frac{|C_{k,l}|}{n}, k \in [b_m], l \in [m(m-1)]$, we write $a \doteq x \pm \epsilon$ to denote $x - \epsilon \leq a \leq x_\epsilon$, and addition is defined element-wise. We have:

$$P\left(\left(Y^n_{(j)}\right)_{j\in[m]}\right) \in \mathcal{A}^n_\epsilon(X^m)\right) = \sum_{(\underline{t}^{b_m,m(m-1)})\in\mathcal{T}} P(\underline{T}_{k,l} = \underline{t}_{k,l}, k \in [b_m], l \in [m(m-1)]),$$

where $\mathcal{T} = \{(\underline{t}^{b_m,m(m-1)} : \sum_{k,l} \alpha_{k,l} T_{k,l,x^m} \doteq P_{X^m}(x^m) \pm \epsilon, \forall x^m\}$. Using the property that for any set of events, the probability of the intersection is less than or equal to the geometric average of the individual probabilities, we have:

$$P((Y^n_{(j)})_{j\in[m]} \in \mathcal{A}^n_\epsilon(X^m)) \leq \sum_{(\underline{t}^{b_m,m(m-1)})\in\mathcal{T}} \sqrt[m(m-1)b_m]{\Pi_{i\in[k,l]} P(\underline{T}_{k,l} = \underline{t}_{k,l})}.$$

Since the elements $(Y_{(j),C_{k,l}}), k \in [b_m], l \in [m(m-1)]$ are i.i.d by construction, it follows from standard information theoretic arguments [32] that:

$$P(\underline{T}_{k,l} = \underline{t}_{k,l}) \leq 2^{-|C_{k,l}|(D(\underline{t}_i \| P_{X_{\mathcal{P}_k}}) - \prod_{j\in[m]} |\mathcal{X}_j|\epsilon)}, k \in [b_m], l \in [m(m-1)].$$

We have,

$$\begin{aligned} P((Y^n_{(j)})_{j\in[m]} \in \mathcal{A}^n_\epsilon(X^m)) &\leq \sum_{(\underline{t}^{b_m,m(m-1)})\in\mathcal{T}} \sqrt[m(m-1)b_m]{\Pi_{i\in[k,l]} 2^{-|C_{k,l}|(D(\underline{t}_i \| P_{X_{\mathcal{P}_k}}) - \prod_{j\in[m]} |\mathcal{X}_j|\epsilon)}} \\ &\overset{(a)}{\leq} \sum_{(\underline{t}^{b_m,m(m-1)})\in\mathcal{T}} \sqrt[m(m-1)b_m]{2^{-n(D(\sum_{k,l} \alpha_{k,l} \underline{t}_{k,l} \| \sum_k P_{X_{\mathcal{P}_k}}) - \prod_{j\in[m]} |\mathcal{X}_j|\epsilon)}} \\ &\overset{(b)}{\leq} 2^{-\frac{n}{m(m-1)b_m}(D(P_{X,Y} \| \sum_{k\in[b_m]} \frac{|C_k|}{n} P_{X_{\mathcal{P}_k}}) - \epsilon \prod_{j\in[m]} |\mathcal{X}_j| + O(\frac{\log n}{n}))}. \end{aligned}$$

where the (a) follows from the convexity of the divergence function and (b) follows by the fact that the number of joint types grows polynomially in n.

□

Appendix F

Proof of Lemma 5

The upper-bound follows by the fact that for r-fold derangement $(\pi_1(\cdot), \pi_2(\cdot), \cdots, \pi_m(\cdot))$, the first permutation is $\pi_1(\cdot)$ is the identity permutation, and the rest of derangements with respect to $\pi_1(\cdot)$, so by the counting principle there are at most $(!n)^{r-1}$ choices for $(\pi_1(\cdot), \pi_2(\cdot), \cdots, \pi_m(\cdot))$. Next we prove the lower bound. Note that $\pi_1(\cdot)$ is the identity permutation. By the same arguments as in the proof of Lemma 2, there are at least $(n-1)!$ choices of distinct $\pi_2(\cdot)$, and for any fixed $\pi_2(\cdot)$ there are at least $(n-2)!$ distinct $\pi_3(\cdot)$. Generally, for fixed $\pi_2(\cdot), \pi_3(\cdot), \cdots, \pi_j(\cdot)$, there are at least $(n-j+1)!$ choices of distinct $\pi_{j+1}(\cdot)$. By the counting principle, there are at least $\prod_{j\in[r]}(n-j+1)! \geq ((n-r+1)!)^r$ distinct $(\pi_1(\cdot), \pi_2\cdot, \cdots, \pi_r(\cdot))$. This completes the proof. □

Appendix G

Proof of Lemma 6

First, we prove the upper-bound in Equation (7). As an initial step, we count the number of distinct allocations of partition correspondence to indices $i \in [1, n]$. Since we are considering $(i_1, i_2, \cdots, i_{b_m})$-Bell permutation vectors, there are a total of i_k indices corresponding to $\mathcal{P}_k$ for $k \in [b_m]$. So, there are $\binom{n}{i_1, i_2, \cdots, i_{b_m}}$ allocations of partition correspondence to different indices. Now assume that the i^{th} index corresponds to the kth partition. Then, we argue that there are at most $n^{|\mathcal{P}_k|}$ possible values for the vector $(\pi_j(i) : j \in [m])$. The reason is that by definition, for any two $\pi_j(i)$ and $\pi_{j'}(i)$, their value are equal if and only if $j, j' \in \mathcal{A}_{k,r}$ for some integer $r \in [|\mathcal{P}_k|]$. So, the elements of $(\pi_j(i) : j \in [m])$ take $|\mathcal{P}_k|$ distinct values among the set $[1, n]$. Consequently $(\pi_j(i) : j \in [m])$ takes at most $n^{|\mathcal{P}_k|}$ distinct values. By the counting principle, the sequence of vectors $(\pi_j(i) : j \in [m]), i \in [n]$ takes at most $n^{\sum_{k\in[b_m]} |\mathcal{P}_k| i_k - n}$ distinct values given a specific partition correspondence, since $\pi_1(\cdot)$ is assumed to be the identity permutation. Since there are a total of $\binom{n}{i_1, i_2, \cdots, i_{b_m}}$ partition correspondences, we have:

$$N_{i_1, i_2, \cdots, i_{b_m}} \leq \binom{n}{i_1, i_2, \cdots, i_{b_m}} n^{\sum_{k\in[b_m]} |\mathcal{P}_k| i_k - n}.$$

Next, we prove the lower-bound in Equation (7). The proof follows by constructing enough distinct $(i_1, i_2, \cdots, i_{b_m})$-Bell permutation vectors. First, we choose a partition correspondence for the indices $i \in [n]$ similar to the proof for the lower-bound. There are $\binom{n}{i_1, i_2, \cdots, i_{b_m}}$ distinct ways of allocating the partition correspondence. We argue that for every fixed partition correspondence,

there are at least $\prod_{k\in[b_m]]} d_{|\mathcal{P}_k|}(i_k)$ permutations which are $(i_1, i_2, \cdots, i_{b_m})$-Bell permutation vectors. To see this, without loss of generality, assume that the first i_1 indices $[1, i_1]$ correspond to $\mathcal{P}_1$, the next i_2 indices $[i_1+1, i_1+i_2]$ correspond to $\mathcal{P}_2$, and in general the indices $[\sum_{t=1}^{k-1} i_t + 1, \sum_{t=1}^{k} i_t]$ correspond to $\mathcal{P}_k$. Let $(\pi'_{1,k}, \pi'_{2,k}, \cdots, \pi'_{|\mathcal{P}_k|,k})$ be vectors of $|\mathcal{P}_k|$-fold derangements of $[\sum_{t=1}^{k-1} i_t + 1, \sum_{t=1}^{k} i_t]$, where $k \in [b_m]$. Then, the following is an $(i_1, i_2, \cdots, i_{b_m})$-Bell permutation vector.

$$\pi_j([\sum_{t=1}^{k-1} i_t + 1, \sum_{t=1}^{k} i_t]) = \pi'_{l,k}([\sum_{t=1}^{k-1} i_t + 1, \sum_{t=1}^{k} i_t]), \quad \text{if } j \in \mathcal{A}_{l,k}, l \in [|\mathcal{P}_k|], k \in [b_m].$$

There are a total of $d_{|\mathcal{P}_k|(i_k)}$ choices of $(\pi'_{1,k}, \pi'_{2,k}, \cdots, \pi'_{|\mathcal{P}_k|,k})$. So, by the counting principle, there are a total of $\prod_{k\in[b_m]} d_{|\mathcal{P}_k|}(i_k)$ choices of $(\pi_1(\cdot), \pi_2(\cdot), \cdots, \pi_m(\cdot))$ for a fixed partition correspondence. As argued previously, there are a total of $\binom{n}{i_1, i_2, \cdots, i_{b_m}}$ distinct choices for partition correspondence. Consequently we have shown that,

$$\binom{n}{i_1, i_2, \cdots, i_{b_m}} \prod_{k\in[b_m]} d_{|\mathcal{P}_k|}(i_k) \leq N_{i_1, i_2, \cdots, i_{b_m}}.$$

This completes the proof of Equation (7). We proceed with to prove Equation (8). Note that from the right hand side of Equation (7), we have:

$$\lim_{n\to\infty} \frac{\log_e N_{i_1,i_2,\cdots,i_{b_m}}}{n \log_e n} \leq \lim_{n\to\infty} \frac{\log_e \binom{n}{i_1,i_2,\cdots,i_{b_m}} n^{(\sum_{k\in[b_m]} |\mathcal{P}_k| i_k - n)}}{n \log_e n} = \lim_{n\to\infty} \frac{\log_e n^{(\sum_{k\in[b_m]} |\mathcal{P}_k| i_k - n)}}{n \log_e n} + \lim_{n\to\infty} \frac{\log_e \binom{n}{i_1,i_2,\cdots,i_{b_m}}}{n \log_e n}$$
$$= \lim_{n\to\infty} \frac{(\sum_{k\in[b_m]} |\mathcal{P}_k| i_k - n)}{n} + \lim_{n\to\infty} \frac{\log_e 2^n}{n \log_e n} = \sum_{k\in[b_m]} |\mathcal{P}_k| \alpha_k - 1.$$

On the other hand, from the left hand side of Equation (7), we have:

$$\lim_{n\to\infty} \frac{\log N_{i_1,i_2,\cdots,i_{b_m}}}{n \log n} \geq \lim_{n\to\infty} \frac{\log \binom{n}{i_1,i_2,\cdots,i_{b_m}} \prod_{k\in[b_m]} d_{|\mathcal{P}_k|}(i_k)}{n \log n}$$
$$\overset{(a)}{\geq} \lim_{n\to\infty} \frac{\log 2^n \prod_{k\in[b_m]} d_{|\mathcal{P}_k|}(i_k)}{n \log n} \overset{(b)}{\geq} \lim_{n\to\infty} \frac{\log \prod_{k\in[b_m]} ((i_k - |\mathcal{P}_k| + 1)!^{|\mathcal{P}_k|-1})}{n \log n}$$
$$= \lim_{n\to\infty} \frac{\sum_{k\in[b_m]} (|\mathcal{P}_k| - 1) \log (i_k - |\mathcal{P}_k| + 1)!}{n \log n}$$
$$\overset{(c)}{=} \lim_{n\to\infty} \frac{\sum_{k\in[b_m]} (|\mathcal{P}_k| - 1)((i_k - |\mathcal{P}_k| + 1) \log (i_k - |\mathcal{P}_k| + 1) - (i_k - |\mathcal{P}_k| + 1) + O(\log (i_k - |\mathcal{P}_k| + 1)))}{n \log n}$$
$$= \sum_{k\in[b_m]} |\mathcal{P}_k| \alpha_k - 1,$$

where (a) follows from the fact that $\binom{n}{i_1,i_2,\cdots,i_{b_m}} \leq 2^n$, (b) follows from Lemma 5, and in (c) we have used Stirling's approximation. □

Appendix H
Proof of Theorem 3

First, note that for the correct labeling the two UTs are jointly typical with probability approaching one as $n \to \infty$:

$$P((U^1_{\sigma^1}, U^2_{\sigma^2}) \in \mathcal{A}_\epsilon^{\frac{n(n-1)}{2}}(X_1, X_2)) \to 1 \quad \text{as} \quad n \to \infty.$$

So, $P(\widehat{\Sigma} = \phi) \to 0$ as $n \to \infty$ since the correct labeling is a member of the set $\widehat{\Sigma}$. We will show that the probability that a labeling in $\widehat{\Sigma}$ labels $n(1-\alpha_n)$ vertices incorrectly goes to 0 as $n \to \infty$. Define the following:

$$\mathcal{E} = \{\sigma'^2 \Big| \|\sigma^2 - \sigma'^2\|_0 \geq n(1-\alpha_n)\},$$

where $\|\cdot\|_0$ is the L_0-norm. The set $\mathcal{E}$ is the set of all labelings which match more than $n\alpha_n$ vertices incorrectly. We show the following:

$$P(\mathcal{E} \cap \widehat{\Sigma} \neq \phi) \to 0, \qquad \text{as} \qquad n \to \infty.$$

Note that:

$$\begin{aligned}
P(\mathcal{E} \cap \widehat{\Sigma} \neq \phi) &= P\left(\bigcup_{\sigma'^2 : \|\sigma^2 - \sigma'^2\|_0 \geq n(1-\alpha_n)} \{\sigma'^2 \in \widehat{\Sigma}\}\right) \overset{(a)}{\leq} \sum_{i=0}^{n\alpha_n} \sum_{\sigma'^2 : \|\sigma^2 - \sigma'^2\|_0 = n-i} P(\sigma'^2 \in \widehat{\Sigma}) \\
&\overset{(b)}{=} \sum_{i=0}^{n\alpha_n} \sum_{\sigma'^2 : \|\sigma^2 - \sigma'^2\|_i = n-i} P((U^1_{\sigma^1}, \Pi_{\sigma^2, \sigma'^2}(U^2_{\sigma^2})) \in \mathcal{A}_\epsilon^{\frac{n(n-1)}{2}}) \\
&\overset{(c)}{\leq} \sum_{i=0}^{n\alpha_n} \sum_{\sigma'^2 : \|\sigma^2 - \sigma'^2\|_i = n-i} 2^{-\frac{n(n-1)}{8}(D(P_{X,Y}\|(1-\frac{i(i-1)}{n(n-1)})P_X P_Y + \frac{i(i-1)}{n(n-1)}P_{X,Y}) - |\mathcal{X}\|\mathcal{Y}|\epsilon + O(\frac{\log n}{n^2}))} \\
&\overset{(d)}{=} \sum_{i=0}^{n\alpha_n} \binom{n}{i} (!(n-i)) 2^{-\frac{n(n-1)}{8}(D(P_{X,Y}\|(1-\frac{i(i-1)}{n(n-1)})P_X P_Y + \frac{i(i-1)}{n(n-1)}P_{X,Y}) - |\mathcal{X}\|\mathcal{Y}|\epsilon + O(\frac{\log n}{n^2}))} \\
&\leq \sum_{i=0}^{n\alpha_n} n^{n-i} 2^{-\frac{n(n-1)}{8}(D(P_{X,Y}\|(1-\frac{i(i-1)}{n(n-1)})P_X P_Y + \frac{i(i-1)}{n(n-1)}P_{X,Y}) - |\mathcal{X}\|\mathcal{Y}|\epsilon + O(\frac{\log n}{n^2}))} \\
&\leq \sum_{i=0}^{n\alpha_n} 2^{(n-i)\log n - \frac{n(n-1)}{8}(D(P_{X,Y}\|(1-\frac{i(i-1)}{n(n-1)})P_X P_Y + \frac{i(i-1)}{n(n-1)}P_{X,Y}) - |\mathcal{X}\|\mathcal{Y}|\epsilon + O(\frac{\log n}{n^2}))}.
\end{aligned}$$

where (a) follows from the union bound, (b) follows from the definition of $\widehat{\Sigma}$, in (c) we have used Theorem 1 and the fact that $\|\sigma^2 - \sigma'^2\|_0 = n - i$ so that $\Pi_{\sigma^2, \sigma'^2}$ has $\frac{i(i-1)}{2}$ fixed points, in (d) we have denoted the number of derangement of sequences of length i by $!i$. Note that the right hand side in the last inequality approaches 0 as $n \to \infty$ as long as:

$$(n-i)\log n \leq \frac{n(n-1)}{8}(D(P_{X,Y}\|(1 - \frac{i(i-1)}{n(n-1)})P_X P_Y + \frac{i(i-1)}{n(n-1)}P_{X,Y}) - |\mathcal{X}\|\mathcal{Y}|\epsilon + O(\frac{\log n}{n^2})), i \in [0, n\alpha_n]$$

$$\leftrightarrow (1-\alpha)\log n \leq \frac{(n-1)}{8}(D(P_{X,Y}||(1-\alpha^2)P_XP_Y + \alpha^2 P_{X,Y}) - |\mathcal{X}||\mathcal{Y}|\epsilon + O(\frac{\log n}{n^2})), \alpha \in [1, 1-\alpha_n],$$

where we have defined $\alpha = \frac{i}{n}$. The last equation is satisfied by the theorem assumption for small enough ϵ. □

Appendix I
Proof of Theorem 4

Let $\epsilon_n = O(\frac{\log n}{n})$ be a sequence of positive numbers. Fix $n \in \mathbb{N}$ and let $\epsilon = \epsilon_n$. For a given labeling σ'', define the event $\mathcal{B}_{\sigma''}$ as the event that the sub-matrices corresponding to each community pair are jointly typical:

$$\mathcal{B}_{\sigma''} : (U_{\sigma,C_i,C_i}, U'_{\sigma'',C'_i,C'_i}) \in \mathcal{A}_\epsilon^{\frac{n_i(n_i-1)}{2}}(P_{X,X'|C_i,C_i,C'_i,C'_i}), \forall i \in [c],$$
$$(G_{\sigma,C_i,C_j}, \widetilde{G'}_{\sigma'',C'_i,C'_j}) \in \mathcal{A}_\epsilon^{n_i \cdot n_j}(P_{X,X'|C_i,C_j,C'_i,C'_j}), \forall i,j \in [c], i \neq j\},$$

Particularly, $\beta_{\sigma'}$ is the event that the sub-matrices are jointly typical under the canonical labeling for the second graph. From standard typicality arguments it follows that:

$$P(\mathcal{B}_{\sigma'}) \to 1 \quad \text{as} \quad n \to \infty.$$

So, $P(\widehat{\Sigma}_{C.C'} = \phi) \to 0$ as $n \to \infty$ since the correct labeling is a member of the set $\widehat{\Sigma}_{C.C'}$. Let $(\lambda_n)_{n\in\mathbb{N}}$ be an arbitrary sequence of numbers such that $\lambda_n = \Theta(n)$. We will show that the probability that a labeling in $\widehat{\Sigma}_{C.C'}$ labels λ_n vertices incorrectly goes to 0 as $n \to \infty$. Define the following:

$$\mathcal{E} = \{\sigma'^2 \Big| ||\sigma^2 - \sigma'^2||_1 \geq \lambda_n\},$$

where $\|\cdot\|_1$ is the L_1-norm. The set $\mathcal{E}$ is the set of all labelings which match more than λ_n vertices incorrectly.

We show the following:

$$P(\mathcal{E} \cap \widehat{\Sigma}_{C.C'} \neq \phi) \to 0, \qquad \text{as} \qquad n \to \infty.$$

We use the union bound on the set of all permutations along with Theorem 1 as follows:

$$P(\mathcal{E} \cap \widehat{\Sigma}_{C.C'} \neq \phi) = P(\bigcup_{\sigma'':||\sigma'-\sigma''||_1 \geq \lambda_n} \{\sigma'' \in \widehat{\Sigma}_{C.C'}\}) \overset{(a)}{\leq} \sum_{k=\lambda_n}^{n} \sum_{\sigma'':||\sigma'-\sigma''||_1=k} P(\sigma'' \in \widehat{\Sigma}_{C.C'})$$
$$\overset{(b)}{=} \sum_{k=\lambda_n}^{n} \sum_{\sigma'':||\sigma'-\sigma'''||_1=k} P(\beta_{\sigma''}) \overset{(c)}{\leq} \sum_{k=\lambda_n}^{n} \sum_{\sigma'^2:||\sigma^2-\sigma'^2||_0=k} 2^{O(nlogn))} \times$$

$$\prod_{i,j\in[c],i<j} 2^{-\frac{n_i\cdot n_j}{4}(D(P_{X,X'|C_i,C_j,C_i',C_j'}\|(1-\beta_{i,j})P_{X|C_i,C_j}P_{X'|C_i',C_j'}+\beta_{i,j}P_{X,X'|C_i,C_j,C_i',C_j'}))}$$
$$\times\prod_{i\in[c]} 2^{-\frac{n_i(n_i-1)}{8}(D(P_{X,X'|C_i,C_i,C_i',C_i'}\|(1-\beta_i)P_{X|C_i,C_i}P_{X'|C_i',C_i'}+\beta_i P_{X,X'|C_i,C_i,C_i',C_i'})}$$
$$\overset{(d)}{\leq}\sum_{k=\lambda_n}^{n}\binom{n}{k}(!k)\max_{[\alpha_i]_{i\in[c]}\in\mathcal{A}}(2^{-\frac{n^2}{4}(\Phi([\alpha_i]_{i\in[c]})+O(\frac{\log n}{n}))})$$
$$\leq\max_{\alpha\in[0,1-\frac{\lambda_n}{n}]}\max_{[\alpha_i]_{i\in[c]}}(2^{-\frac{n^2}{4}(-(1-\alpha)\frac{\log n}{n}+\Phi([\alpha_i]_{i\in[c]})+O(\frac{\log n}{n}))}),$$

where $\mathcal{A}=\{([\alpha_i]_{i\in[c]}):\alpha_i\leq\frac{n_i}{n},\sum_{i\in[c]}\alpha_i=\frac{n-\lambda_n}{n}\}$ and

$$\Phi([\alpha_i]_{i\in[c]})=\sum_{i,j\in[c],i<j}n_in_j\cdot D(P_{X,X'|C_i,C_j,C_i',C_j'}\|(1-\beta_{i,j})P_{X|C_i,C_j}P_{X'|C_i',C_j'}+\beta_{i,j}P_{X,X'|C_i,C_j,C_i',C_j'})$$
$$+\sum_{i\in[c]}\frac{n_i(n_i-1)}{2}D(P_{X,X'|C_i,C_i,C_i',C_i'}\|(1-\beta_i)P_{X|C_i,C_i}P_{X'|C_i',C_i'}+\beta_iP_{X,X'|C_i,C_i,C_i',C_i'}),$$

and $\beta_{i,j}=\frac{n^2}{n_in_j}\alpha_i\alpha_j$ and $\beta_i=\frac{n\alpha_i(n\alpha_i-1)}{n_i(n_i-1)}$. Here, α_i is the number of fixed points in the i^{th} community divided by n, and β_i is the number of fixed points in $U'_{\sigma'',C_i',C_i'}$ divided by $\frac{n_i(n_i-1)}{2}$, and $\beta_{i,j}$ is the number of fixed points in $U'_{\sigma'',C_i',C_j'}$ divided by n_in_j. Inequality (a) follows from the union bound, (b) follows from the definition of $\widehat{\Sigma}_{C.C'}$, in (c) we have used Theorem 1, in (d) we have denoted the number of derangement of sequences of length i by $!i$. Note that the right hand side in the (d) goes to 0 as $n\to\infty$ as long as (10) holds. □

,

Appendix J
Proof of Theorem 6

The proof build upon the arguments used in the proof of Theorem 3. First, note that for the correct labeling the UTs are jointly typical with probability approaching one as $n\to\infty$. So, $P(\widehat{\Sigma}=\phi)\to 0$ as $n\to\infty$ since the correct labeling is a member of the set $\widehat{\Sigma}$. On the other hand, the probability that a labeling in $\widehat{\Sigma}$ labels $n(1-\alpha_n)$ vertices incorrectly goes to 0 as $n\to\infty$. Define the following:

$$\mathcal{E}=\{(\sigma'_i)_{i\in[m]}\Big|\|(\sigma'_i)_{i\in[m]}-(\sigma_i)_{i\in[m]}\|_0\geq n(1-\alpha_n)\},$$

where $\|\cdot\|_0$ is the L_0-norm. Without loss of generality, we assume that the labeling for the denonymized graph is the trivial labeling, i.e. $\sigma_1=\sigma'_1=id(\cdot)$, where $id(\cdot)$ is the identity

function. The set $\mathcal{E}$ is the set of all labelings which match more than $n\alpha_n$ vertices incorrectly. We show the following:

$$P(\mathcal{E} \cap \widehat{\Sigma} \neq \phi) \to 0, \qquad \text{as} \qquad n \to \infty.$$

We partition the set $\mathcal{E}$ into subsets of Bell permutation vectors with the same parameters. We define the following:

$$\mathcal{E}_{i_1,i_2,\cdots,i_{b_m}} = \{(\sigma'_i)_{i\in[m]} \Big| (\sigma'_i)_{i\in[m]} \text{ is a } (i_1, i_2, \cdots, i_{b_m})\text{-Bell permutation vector}\},$$

where $i_1, i_2, \cdots, i_{b_m} \in [0, n]$ and $\sum_{k\in[b_m]} i_{\mathcal{P}_k} = n$. Then the family of sets $\{\mathcal{E}_{i_1,i_2,\cdots,i_{b_m}} : \sum_{k\in[b_m]} i_{\mathcal{P}_k} = n\}$ partitions the set $\mathcal{E}$.

Note that similar to the proof of Theorem 3, we have:

$$P(\mathcal{E} \cap \widehat{\Sigma} \neq \phi) = P\left(\bigcup_{(\sigma'_i)_{i\in[m]}:\|\sigma^2-\sigma'^2\|_0\geq n(1-\alpha_n)} \{\sigma'^2 \in \widehat{\Sigma}\}\right)$$

$$P(\mathcal{E} \cap \widehat{\Sigma} \neq \phi) = P\left(\bigcup_{\substack{(i_1,i_2,\cdots,i_{b_m}):\\ \sum_{k\in[b_m]} i_k=n}} \bigcup_{\substack{(\sigma'_i)_{i\in[m]}\in\mathcal{E}_{i_1,i_2,\cdots,i_{b_m}}:\\ \|\sigma^2-\sigma'^2\|_0\geq n(1-\alpha_n)}} \{\sigma'^2 \in \widehat{\Sigma}\}\right)$$

$$\leq \sum_{\substack{(i_1,i_2,\cdots,i_{b_m}):\\ \sum_{k\in[b_m]} i_k=n}} \sum_{\substack{(\sigma'_i)_{i\in[m]}\in\mathcal{E}_{i_1,i_2,\cdots,i_{b_m}}:\\ \|\sigma^2-\sigma'^2\|_0\geq n(1-\alpha_n)}} P\left(\{\sigma'^2 \in \widehat{\Sigma}\}\right)$$

$$\leq \sum_{\substack{(i_1,i_2,\cdots,i_{b_m}):\\ \sum_{k\in[b_m]} i_k=n}} \sum_{\substack{(\sigma'_i)_{i\in[m]}\in\mathcal{E}_{(i_1,i_2,\cdots,i_{b_m}):}\\ \|\sigma^2-\sigma'^2\|_0\geq n(1-\alpha_n)}} 2^{-\frac{\frac{n(n-1)}{2}}{m(m-1)b_m}(D(P_{X^m}\|\sum_{k\in[b_m]} \frac{i'_k}{\frac{n(n-1)}{2}} P_{X_{\mathcal{P}_k}})-\epsilon\prod_{j\in[m]}|\mathcal{X}_j|+O(\frac{\log n}{n^2}))}$$

$$= \sum_{\substack{(i_1,i_2,\cdots,i_{b_m}):\\ \sum_{k\in[b_m]} i_k=n, i_{b_m}\geq n(1-\alpha_n)}} N_{i_1,i_2,\cdots,i_{b_m}} 2^{-\frac{\frac{n(n-1)}{2}}{m(m-1)b_m}(D(P_{X^m}\|\sum_{k\in[b_m]} \frac{i'_k}{\frac{n(n-1)}{2}} P_{X_{\mathcal{P}_k}})-\epsilon\prod_{j\in[m]}|\mathcal{X}_j|+O(\frac{\log n}{n^2}))}$$

$$\leq \sum_{\substack{(i_1,i_2,\cdots,i_{b_m}):\\ \sum_{k\in[b_m]} i_k=n, i_{b_m}\geq n(1-\alpha_n)}} 2^{n\log n(\sum_{k\in[b_m]}|\mathcal{P}_k|\frac{i_k}{n}-1)+O(n\log n)} 2^{-\frac{\frac{n(n-1)}{2}}{m(m-1)b_m}(D(P_{X^m}\|\sum_{k\in[b_m]} \frac{i'_k}{\frac{n(n-1)}{2}} P_{X_{\mathcal{P}_k}})-\epsilon\prod_{j\in[m]}|\mathcal{X}_j|+O(\frac{\log n}{n^2}))}$$

$$\leq \sum_{\substack{(i_1,i_2,\cdots,i_{b_m}):\\ \sum_{k\in[b_m]} i_k=n, i_{b_m}\geq n(1-\alpha_n)}} 2^{n\log n(\sum_{k\in[b_m]}|\mathcal{P}_k|\frac{i_k}{n}-1)+O(n\log n)-\frac{\frac{n(n-1)}{2}}{m(m-1)b_m}(D(P_{X^m}\|\sum_{k\in[b_m]} \frac{i'_k}{\frac{n(n-1)}{2}} P_{X_{\mathcal{P}_k}})-\epsilon\prod_{j\in[m]}|\mathcal{X}_j|+O(\frac{\log n}{n^2}))},$$

where $i'_k = \frac{i_k(i_k-1)}{2} + \sum_{k',k'':\mathcal{P}_{k',k''}=\mathcal{P}_l} i_{k'} i_{k''}$, and $\mathcal{P}_{k',k''} = \{\mathcal{A}' \cap \mathcal{A}'' : \mathcal{A}' \in \mathcal{P}_{k'}, \mathcal{A}'' \in \mathcal{P}_{k''}\}, k', k'' \in [b_m]$. Note that the right hand side in the last inequality approaches 0 as $n \to \infty$ as long as:

$$n\log n(\sum_{k\in[b_m]}|\mathcal{P}_k|\alpha_k - 1) \leq \frac{n(n-1)}{2b_m m(m-1)}(D(P_{X^m}\|\sum_{k\in[b_m]}\alpha'_k P_{X_{\mathcal{P}_k}}) - \epsilon\prod_{j\in[m]}|\mathcal{X}_j| + O(\frac{\log n}{n^2}))$$

$$\leftrightarrow \log n(\sum_{k\in[b_m]} |\mathcal{P}_k|\alpha_k - 1) \leq \frac{(n-1)}{2b_m m(m-1)}(D(P_{X^m}\| \sum_{k\in[b_m]} \alpha'_k P_{X_{\mathcal{P}_k}}) - \epsilon \prod_{j\in[m]} |\mathcal{X}_j| + O(\frac{\log n}{n^2})),$$

for all $\alpha_1, \alpha_2, \cdots, \alpha_{b_m} : \sum_{k\in[b_m]} \alpha_k = n, \alpha_{b_m} \in [1, 1-\alpha_n]$, where we have defined $\alpha'_k = \frac{i'_k}{\frac{n(n-1)}{2}}$. The last equation is satisfied by the theorem assumption for small enough ϵ. □

Appendix K
Proof of Theorem 7

Let $n \in \mathcal{N}$, and G and G' be the adjacency matrices of the two graphs under a pre-defined labeling. Let $\hat{\sigma}$ be the output of the matching algorithm. Let $\mathbb{1}_C$ be the indicator of the event that the matching algorithm mislabels at most ϵ_n fraction of the vertices with probability at least P_e, where $\epsilon_n, P_e \to 0$ as $n \to \infty$. Note that $\hat{\sigma}$ is a function of σ', G, G'. So:

$$0 = H(\hat{\sigma}|\sigma, G, G') \overset{(a)}{=} H(\sigma', \hat{\sigma}, \mathbb{1}_C|\sigma, G, G') - H(\sigma', \mathbb{1}_C|\hat{\sigma}, \sigma, G, G') = H(\sigma', \hat{\sigma}, \mathbb{1}_C|\sigma, G, G') -$$
$$H(\sigma'|\mathbb{1}_C, \hat{\sigma}, \sigma, G, G') - H(\mathbb{1}_C|\hat{\sigma}, \sigma, G, G') \overset{(b)}{\geq} H(\sigma', \hat{\sigma}, \mathbb{1}_C|\sigma, G, G') - H(\sigma'|\mathbb{1}_C, \hat{\sigma}, \sigma, G, G') - 1$$
$$= H(\sigma', \hat{\sigma}, \mathbb{1}_C|\sigma, G, G') - P(\mathbb{1}_C = 1)H(\sigma'|\mathbb{1}_C = 1, \hat{\sigma}, \sigma, G, G') - P(\mathbb{1}_C = 0)H(\sigma'|\mathbb{1}_C = 0, \hat{\sigma}, \sigma, G, G') - 1$$
$$\overset{(c)}{\geq} H(\sigma', \hat{\sigma}, \mathbb{1}_C|\sigma, G, G') - \epsilon_n n \log n - P_e n \log n - 1 \overset{(d)}{\geq} H(\sigma'|\sigma, G, G') - (\epsilon_n + P_e) n \log n - 1,$$

where in (a) we have used the chain rule of entropy, in (b) we have used the fact that $\mathbb{1}_C$ is binary, in (c) we define the probability of mismatching more than ϵ_n fraction of the vertices by P_e, and (d) follows from the fact that entropy is non-negative. As a result,

$$H(\sigma'|\sigma, G, G') \leq (\epsilon_n + P_e) n \log n + 1.$$

Consequently,

$$n \log n \overset{(a)}{=} \log n! + n + O(\log n) = H(\sigma') \overset{(b)}{=} I(\sigma'; \sigma, G, G') + O(n \log n),$$

where in (a) we have used Stirling's approximation, and in (b) we have used the fact that $\epsilon, P_e \to 0$ as $n \to \infty$. We have:

$$n \log n \leq I(\sigma'; \sigma, G, G') + O(n \log n)$$
$$= I(\sigma'; G') + I(\sigma'; \sigma, G|G') + O(n \log n) \overset{(a)}{=} I(\sigma'; \sigma, G|G') + O(n \log n)$$
$$= I(\sigma'; G|G') + I(\sigma'; G|G', \sigma) + O(n \log n) \overset{(b)}{=} I(\sigma'; G|G', \sigma) + O(n \log n)$$

$$\overset{(c)}{\leq} I(\sigma', G'; G|\sigma) + O(n\log n) \overset{(d)}{=} I(G'; G|\sigma, \sigma')$$

$$\overset{(e)}{=} \sum_{i,j\in[c],i<j} n_i n_j I(X, X'|C_i, C_j, C_i'C_j') + \sum_{i\in[c]} \frac{n_i(n_i-1)}{2} I(X, X'|C_i, C_i, C_i', C_i') + O(n\log n),$$

where (a) follows from $\sigma' \perp\!\!\!\perp G'$, (b) follows from the fact that $\sigma' \perp\!\!\!\perp G, G'$, (c) is true due to the non-negativity of the mutual inforamtion, (d) follows from $\sigma, \sigma' \perp\!\!\!\perp G$, and (e) follows from the fact that the edges whose vertices have different labels are independent of each other given the labels.

□

Appendix L
Proof of Lemma 7

The ambiguity set $\mathcal{L}$ is defined as:

$$\mathcal{L} = \{v_j \big| \nexists! i : (\underline{F}_i, \underline{F}'_j) \in \mathcal{A}_\epsilon^n(X, X')\}.$$

From the Chebychev inequality, we have:

$$P\left(|\mathcal{L}| > 2\mathbb{E}(|\mathcal{L}|)\right) = P\left(\left||\mathcal{L}| - \mathbb{E}(|\mathcal{L}|)\right| > \mathbb{E}(|\mathcal{L}|)\right) \leq \frac{Var(|\mathcal{L}|)}{\mathbb{E}^2(|\mathcal{L}|)}. \tag{20}$$

Let B_j be the event that $v_j \in \mathcal{L}$, then

$$\mathbb{E}(|\mathcal{L}|) = \mathbb{E}\left(\sum_{j=1}^n \mathbb{1}(v_j \in \mathcal{L})\right) = \sum_{j=1}^n P(vj \in \mathcal{L}) = \sum_{j=1}^n P(B_j)$$

$$Var(|\mathcal{L}|) = \sum_{j=1}^n P(B_j) + \sum_{i\neq j} P(B_i, B_j) - \left(\sum_{j=1}^n P(B_j)\right)^2$$

$$= \sum_{j=1}^n P(B_j) - \sum_{j=1}^n P^2(B_j) \leq \mathbb{E}(|\mathcal{L}|).$$

So, from (20), we have:

$$P\left(|\mathcal{L}| > 2\mathbb{E}(|\mathcal{L}|)\right) \leq \frac{1}{\mathbb{E}(|\mathcal{L}|)},$$

which goes to 0 as $n \to \infty$ provided that $\mathbb{E}(|\mathcal{L}|) \to \infty$ (otherwise the claim is proved since $\mathbb{E}(|\mathcal{L}|)$ is finite.). It remains to find an upper bound on $\mathbb{E}(|\mathcal{L}|)$. Let C_j be the event that the fingerprint $\underline{F}'_j$ is not typical with respect to $P_{X'}$ and let $D_{i,j}$ be the event that there exists $i \in [1, n]$ such that $\underline{F}_i$ and $\underline{F}'_j$ are jointly typical with respect to $P_{X,X'}$. Then,

$$P(B_j) \leq P\left(C_j \bigcup \left(\bigcup_{i\neq j} D_{i,j}\right)\right) \leq P(C_j) + \sum_{i\neq j} P(D_{i,j}|C_j^c) \overset{(a)}{\leq} \frac{1}{\Lambda\epsilon^2} + n2^{-\Lambda(I(X;X')-\epsilon)},$$

where (a) follows from the standard information theoretic arguments (e.g proof of Theorem 3 in [34]). So,

$$\mathbb{E}(|\mathcal{L}|) \leq \frac{n}{\Lambda\epsilon^2} + n^2 2^{-\Lambda(I(X;X')-\epsilon)}.$$

From $\Lambda > \frac{2\log n}{I(X;X')}$, we conclude that the second term approaches 0 as $n \to \infty$. This completes the proof. □

Appendix M
Proof of Theorem 8

Let H_1 be the event the algorithm fails and H_2 the event that $|\mathcal{L}| > \frac{2n}{\Lambda\epsilon^2}$. Then:

$$P(H_1) \leq P(H_2) + P(H_1|H_2^c).$$

From Claim 1, we know that $P(H_2) \to 0$ as $n \to \infty$. For the second term, let $\mathcal{L}'$ be the set of vertices which are not matched in the second iteration. The algorithm fails if $\mathcal{L}' \neq \phi$. However, by a similar argument as in the proof of claim 1, we have:

$$P(|\mathcal{L}'| > \frac{1}{2}\Big||\mathcal{L}| < \frac{2n}{\Lambda\epsilon^2}) \to 0 \text{ as } n \to \infty.$$

So, $P(|\mathcal{L}'| = 0) \to 1$ as $n \to \infty$. This completes the proof.

□

References

[1] Donatello Conte, Pasquale Foggia, Carlo Sansone, and Mario Vento. Thirty years of graph matching in pattern recognition. *International journal of pattern recognition and artificial intelligence*, 18(03):265–298, 2004.

[2] Frank Emmert-Streib, Matthias Dehmer, and Yongtang Shi. Fifty years of graph matching, network alignment and network comparison. *Information Sciences*, 346:180–197, 2016.

[3] Paul Erdos and Alfréd Rényi. On the evolution of random graphs. *Publ. Math. Inst. Hung. Acad. Sci*, 5(1):17–60, 1960.

[4] Edward M Wright. Graphs on unlabelled nodes with a given number of edges. *Acta Mathematica*, 126(1):1–9, 1971.

[5] László Babai, Paul Erdos, and Stanley M Selkow. Random graph isomorphism. *SIAM Journal on computing*, 9(3):628–635, 1980.

[6] Béla Bollobás. Random graphs. 2001. *Cambridge Stud. Adv. Math*, 2001.

[7] Tomek Czajka and Gopal Pandurangan. Improved random graph isomorphism. *Journal of Discrete Algorithms*, 6(1):85–92, 2008.

[8] Ehsan Kazemi. Network alignment: Theory, algorithms, and applications. 2016.

[9] Lyudmila Yartseva and Matthias Grossglauser. On the performance of percolation graph matching. In *Proceedings of the first ACM conference on Online social networks*, pages 119–130. ACM, 2013.

[10] Pedram Pedarsani, Daniel R Figueiredo, and Matthias Grossglauser. A bayesian method for matching two similar graphs without seeds. In *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1598–1607. IEEE, 2013.

[11] Shouling Ji, Weiqing Li, Mudhakar Srivatsa, and Raheem Beyah. Structural data de-anonymization: Quantification, practice, and implications. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1040–1053. ACM, 2014.

[12] Daniel Cullina and Negar Kiyavash. Exact alignment recovery for correlated erdos renyi graphs. *arXiv preprint arXiv:1711.06783*, 2017.

[13] Vince Lyzinski. Information recovery in shuffled graphs via graph matching. *arXiv preprint arXiv:1605.02315*, 2016.

[14] Daniel Cullina, Negar Kiyavash, Prateek Mittal, and H Vincent Poor. Partial recovery of erd\h {o} sr\'{e} nyi graph alignment via *k*-core alignment. *arXiv preprint arXiv:1809.03553*, 2018.

[15] Michelle Girvan and Mark EJ Newman. Community structure in social and biological networks. *Proceedings of the national academy of sciences*, 99(12):7821–7826, 2002.

[16] Santo Fortunato and Claudio Castellano. Community structure in graphs. *Computational Complexity: Theory, Techniques, and Applications*, pages 490–512, 2012.

[17] Shirin Nilizadeh, Apu Kapadia, and Yong-Yeol Ahn. Community-enhanced de-anonymization of online social networks. In *Proceedings of the 2014 acm sigsac conference on computer and communications security*, pages 537–548. ACM, 2014.

[18] Kushagra Singhal, Daniel Cullina, and Negar Kiyavash. Significance of side information in the graph matching problem. *arXiv preprint arXiv:1706.06936*, 2017.

[19] Efe Onaran, Siddharth Garg, and Elza Erkip. Optimal de-anonymization in random graphs with community structure. In *Signals, Systems and Computers, 2016 50th Asilomar Conference on,*, pages 709–713. IEEE, 2016.

[20] Daniel Cullina and Negar Kiyavash. Improved achievability and converse bounds for erdos-renyi graph matching. *SIGMETRICS Perform. Eval. Rev.*, 44(1):63–72, June 2016.

[21] Ehsan Kazemi, S Hamed Hassani, and Matthias Grossglauser. Growing a graph matching from a handful of seeds. *Proceedings of the VLDB Endowment*, 8(10):1010–1021, 2015.

[22] Carla-Fabiana Chiasserini, Michele Garetto, and Emilio Leonardi. Social network de-anonymization under scale-free user relations. *IEEE/ACM Transactions on Networking*, 24(6):3756–3769, 2016.

[23] Vince Lyzinski, Donniell E Fishkind, and Carey E Priebe. Seeded graph matching for correlated erdös-rényi graphs. *Journal of Machine Learning Research*, 15(1):3513–3540, 2014.

[24] Marcelo Fiori, Pablo Sprechmann, Joshua Vogelstein, Pablo Musé, and Guillermo Sapiro. Robust multimodal graph matching: Sparse coding meets graph matching. In *Advances in Neural Information Processing Systems*, pages 127–135, 2013.

[25] Farhad Shirani, Siddharth Garg, and Elza Erkip. Seeded graph matching: Efficient algorithms and theoretical guarantees. In *2017 51st Asilomar Conference on Signals, Systems, and Computers*, pages 253–257. IEEE, 2017.

[26] E. Kazemi, L. Yartseva, and M. Grossglauser. When can two unlabeled networks be aligned under partial overlap? In *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 33–42, Sept 2015.

[27] Elchanan Mossel and Jiaming Xu. Seeded graph matching via large neighborhood statistics. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1005–1014. SIAM, 2019.

[28] Donniell E Fishkind, Sancar Adali, Heather G Patsolic, Lingyao Meng, Digvijay Singh, Vince Lyzinski, and Carey E Priebe. Seeded graph matching. *Pattern Recognition*, 87:203–215, 2019.

[29] Vince Lyzinski and Daniel L Sussman. Matchability of heterogeneous networks pairs. *arXiv preprint arXiv:1705.02294*, 2017.

[30] Si Zhang and Hanghang Tong. Final: Fast attributed network alignment. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 1345–1354. ACM, 2016.

[31] Mark Heimann, Haoming Shen, Tara Safavi, and Danai Koutra. Regal: Representation learning-based graph alignment. In *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, pages 117–126. ACM, 2018.

[32] I. Csiszár and J. Korner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Academic Press Inc. Ltd., 1981.

[33] I Martin Isaacs. *Algebra: a graduate course*, volume 100. American Mathematical Soc., 1994.

[34] F. Shirani, S. Garg, and E. Erkip. An information theoretic framework for active de-anonymization in social networks based on group memberships. In *2017 55rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2017.

[35] Xinjia Chen. Concentration inequalities for bounded random vectors. *arXiv preprint arXiv:1309.0003*, 2013.