This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3192876

Computing Sum of Sources over a Classical-Quantum MAC

Mohammad Aamir Sohail, *Student Member, IEEE*, Touheed Anwar Atif, *Student Member, IEEE*, Arun Padakandla, *Member, IEEE*, S. Sandeep Pradhan, *Fellow, IEEE*

***Abstract*—We consider the task of communicating a generic bivariate function of two classical correlated sources over a Classical-Quantum Multiple Access Channel (CQ-MAC). The two sources are observed at the encoders of the CQ-MAC, and the decoder aims at reconstructing a bivariate function from the received quantum state. We first propose a coding scheme based on asymptotically good algebraic structured codes, in particular, nested coset codes, and provide a set of sufficient conditions for the reconstruction of the function of the sources over a CQ-MAC. The proposed technique enables the decoder to recover the desired function without recovering the sources themselves. We further improve this by employing a coding scheme based on a classical superposition of algebraic structured codes and unstructured codes. This coding scheme allows exploiting the symmetric structure common amongst the sources and also leverage the asymmetries. We derive a new set of sufficient conditions that strictly enlarges the largest known set of sources whose function can be reconstructed over any given CQ-MAC, and identify examples demonstrating the same. We provide these conditions in terms of single-letter quantum information-theoretic quantities.**

I. INTRODUCTION

Early research in quantum state discrimination led to the investigation of the information carrying capacity of quantum states. Suppose Alice - a sender - can prepare any one of the states in the collection $\{\rho_x \in \mathcal{D}(\mathcal{H}_Z) : x \in \mathcal{X}\}$, and Bob - the receiver - has to rely on a measurement to infer the label x of the state, then what is the largest sub-collection $\mathcal{C} \subseteq \mathcal{X}$ of states that Bob can distinguish perfectly? Here $\mathcal{H}_Z$ is the Hilbert state of the quantum system, and $\mathcal{D}(\mathcal{H}_Z)$ denotes the set of density operators acting on $\mathcal{H}_Z$. Studying this question in a Shannon-theoretic sense, Schumacher, Westmoreland [1] and Holevo [2] characterized the exponential growth of this sub-collection, thereby characterizing the capacity of a classical-quantum (CQ) point-to-point (P2P) channel. In the following years, generalizations of this question with multiple senders and/or receivers have been studied with an aim of characterizing the corresponding information carrying capacity of quantum states in network scenarios [3].

In this work, we consider the problem of computing functions of information sources over a CQ multiple access channel (MAC). Let $(\rho_{x_1x_2} \in \mathcal{D}(\mathcal{H}_Z) : (x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2)$ model a CQ-MAC. Sender j - the party having access to the choice of label $x_j \in \mathcal{X}_j$ - observes a classical information stream $S_{jt} \in \mathcal{S}_j : t \geq 1$. The pairs $(S_{1t}, S_{2t}) : t \geq 1$ are independent and identically distributed (IID) with a single-letter joint distribution $\mathbb{W}_{S_1S_2}$. The receiver, who is provided with the prepared quantum state, intends to reconstruct a specific function $f(S_1, S_2)$ of the information observed by the senders. The question of interest is under what conditions, specified in terms of the CQ-MAC, the source $\mathbb{W}_{S_1S_2}$ and the function f, can the receiver reconstruct the desired function losslessly?

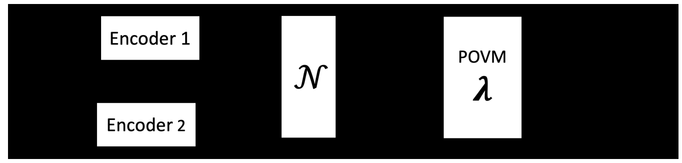

Fig. 1. A schematic of the problem of computing a function f of classical correlated sources with joint distribution $\mathbb{W}_{S_1S_2}$ over a CQ-MAC $\mathcal{N}$.

The conventional approach to characterizing sufficient conditions for this problem relies on enabling the receiver reconstruct the pair of classical source sequences. Since the receiver is only interested in recovering the bivariate function f, and not the pair, this approach can be strictly sub-optimal. Can we exploit this and design a more efficient communication strategy, thereby weakening the set of sufficient conditions? In this work, we present one such communication strategy for a general CQ-MAC that is more efficient than the conventional approach. This strategy is based on asymptotically good random nested coset codes. We analyze its performance and derive new sufficient conditions for a general problem instance and identify examples for which the derived conditions are strictly weaker.

Our findings here are built on the ideas developed in the classical setting. Focusing on a source coding formulation, i.e. a noiseless MAC, Körner and Marton [4] devised a coding technique that enabled the receiver recover the sum of the sources without recovering either source. In [5], the linearity of the Körner-Marton (KM) source coding map was further exploited to enable the receiver recover the sum of the sources using *only* the *sum* of the KM indices, not even requiring the pair. Leveraging this observation and focusing on the subclass of additive MACs, specific MAC channel coding techniques are devised in [5] that enabled the receiver recover the sum of two channel coding message indices. The authors in [6] addressed this CQ-MAC problem where the sources are computed directly without the need for the explicit reconstruction of the individual sources, while restricting their attention to uniform input distributions.

The techniques of [4]–[6] are instances of a broader frame-

Manuscript received; revised; accepted. This work was presented in part at IEEE International Symposium on Information Theory (ISIT) 2021 and 2022. This work was supported by NSF grants CCF-1717523 and CCF-2007878.

M. A. Sohail, T. A. Atif, and S. S. Pradhan are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA. A. Padakandla is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, USA (email:{mdaamir, touheed, pradhanv}@umich.edu, arunpr@utk.edu).

Communicated by S. Beigi, Associate Editor for Quantum.

work of coding strategies based on using random linear codes. Decoding functions of sources or channel inputs efficiently require codes endowed with algebraic closure properties. To emphasize, the conventional approach of deriving inner bounds/achievable rate region by analyzing expected performance of IID random codes is incapable of yielding performance limits - capacity or rate-distortion regions as the case may be in network communication scenarios. To improve upon this, it is necessary to analyze the expected performance of random codes endowed with algebraic closure properties. In a series of works [7], an information-theoretic study of the latter codes has been carried out yielding new inner bounds for multiple network communication scenarios.

A careful observation of the above idea reveals that two MAC channel codes employed by the encoders do not 'blow up' when added, is crucial to the efficiency of the above scheme. A linear code being algebraically closed enables this. However, the codewords of a random linear code are uniformly distributed and cannot achieve the capacity of an arbitrary classical P2P channel, let alone a CQ-P2P channel. We are therefore forced to enlarge a linear code to identify sufficiently many codewords of the desired empirical single-letter distribution. We are thus led to a *nested coset code* (NCC) [8].

In this work, we embark on developing these ideas in the CQ setup. After having provided the problem statement in Sec. II, we focus on a simplified CQ-MAC and illustrate the core idea of our coding scheme. This relies on developing a *nested coset code* (NCC) based communication scheme for a CQ-P2P channel and analyzing its performance (Sec. III-A). Leveraging this building block, we construct and analyze the asymptotic performance of an NCC-based coding scheme for computing sum over a general CQ-MAC (Sec. III-B), and provide sufficient conditions based on single-letter quantum information quantities (see Theorem 2). We also extend the results to the case of a generic QQ-MAC (see Theorem 3 in Sec. III-C).

As our next main contribution, we generalize the above ideas for computing arbitrary functions over a general CQ-MAC. It has been demonstrated in the classical multi-terminal setting, the coding techniques relying on the algebraic structure may show gains for only a certain class of problems and in certain rate regimes [9]. Therefore, a unified technique that captures the gains of both the traditional unstructured coding techniques and the techniques based on algebraic structured codes is needed to approach the performance limits for the multi-terminal problems. Alhswede-Han [9] obtained the best known inner bound for the problem of classical lossless distributed compression by combining the Slepian-Wolf [10] coding scheme with the coding scheme of Körner-Marton [4] based on algebraic structured codes.

Motivated by this, we provide a unified approach for the problem of computing a bivariate function of two sources over CQ-MAC, capitalizing on the gains of the algebraic structured techniques developed in [11], while making the most of the standard approach based on unstructured codes developed for this problem [3]. We propose an approach where each transmitter intends to send two pieces of information about its corresponding source to the receiver. The first piece of information from both the sources needs to be reconstructed individually at the receiver. Then, conditioned on this reconstruction, we let the receiver reconstruct the necessary function f of the second piece. At ith transmitter, the two pieces are constructed on auxiliary variables U_i and V_i, and then fused to form the channel input X_i. We construct a $4-$input CQ-MAC to model this transmission. This poses a challenge concerning the number of messages being decoded. The decoder aims at decoding the triple $(U_1, U_2, V_1 \oplus_q V_2)$, where $\oplus_q$ represents addition with respect to a prime finite field $\mathbb{F}_q$. For this, the decoder needs a CQ simultaneous decoding technique. The ideas of joint typicality using tilting, smoothing, and augmentation introduced by Sen [12], [13] solved the problem of simultaneous decoding of individual messages on CQ-MAC, however, it is based on unstructured coding techniques. We develop a unified coding framework that combines unstructured and structured coding techniques while using this jointly typicality approach that enables the decoder to reconstruct $(U_1, U_2, V_1 \oplus_q V_2)$ simultaneously.

In light of this, the main contribution of the current work is in providing a new set of sufficient conditions (see Theorems 4 and 5 in Sec. III-D), while strictly subsuming the current known conditions, for the reconstruction of an arbitrary function of sources over a generic CQ-MAC. We provide these conditions in terms of single-letter quantum information quantities. Furthermore, we identify examples (see Section III-E) where the gains provided by this framework are demonstrated. We also discuss the potential applications of computation over a CQ-MAC in Section III-F. This work opens up the opportunity to investigate a generic approach encompassing both the conventional and algebraic structured techniques for other multi-terminal problems in the classical-quantum regime [14]–[16].

II. Preliminaries and Problem Statement

We supplement the notation in [17] with the following. For a positive integer n, $[n] \triangleq \{1, \cdots, n\}$. For a Hilbert space $\mathcal{H}$, the spaces $\mathcal{L}(\mathcal{H}), \mathcal{P}(\mathcal{H})$ and $\mathcal{D}(\mathcal{H})$ denote the collection of linear, positive and density operators acting on $\mathcal{H}$, respectively. The von Neumann entropy of a density operator $\rho \in \mathcal{D}(\mathcal{H})$ is denoted by $S(\rho)$. Given any ensemble $\{p_i, \rho_i\}_{i\in[1,m]}$, the Holevo information [18] is denoted as $\chi\big(\{p_i; \rho_i\}\big)$. A POVM acting on $\mathcal{H}$ is a collection $\boldsymbol{\lambda} \triangleq \{\lambda_x\}_{x\in\mathcal{X}}$ of positive operators that form a resolution of the identity: $\sum_{x\in\mathcal{X}} \lambda_x = I$, where $\mathcal{X}$ is a finite set. We employ an underline notation to aggregate objects of similar type. For example, $\underline{s}$ denotes (s_1, s_2), $\underline{x}^n$ denotes (x_1^n, x_2^n), $\underline{\mathcal{S}}$ denotes the Cartesian product $\mathcal{S}_1 \times \mathcal{S}_2$. Let $\mathbb{F}_q$ denote a prime finite field of size q and $\oplus$ the corresponding addition operation.

Consider a (generic) *CQ-MAC* $\mathcal{N}_2$ specified through (i) finite sets $\mathcal{X}_j : j \in [2]$, (ii) Hilbert space $\mathcal{H}_Z$, and (iii) a collection of density operator $(\rho_{x_1,x_2} \in \mathcal{D}(\mathcal{H}_Z) : (x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2)$. This CQ-MAC is employed to enable the receiver reconstruct a bivariate function of the classical information streams observed by the senders. Let $\mathcal{S}_1, \mathcal{S}_2$ be finite sets and $(S_1, S_2) \in \mathcal{S}_1 \times \mathcal{S}_2$ distributed with PMF $\mathbb{W}_{S_1S_2}$, which models the pair of information sources observed at the encoders.

Specifically, sender j observes the sequence $S_{jt} \in \mathcal{S}_j : t \geq 1$, and the sequence $(S_{1t}, S_{2t}) : t \geq 1$ are IID with single-letter PMF $\mathbb{W}_{S_1 S_2}$. The receiver aims to recover the sequence $f(S_{1t}, S_{2t}) : t \geq 1$ losslessly, where $f : \mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{R}$ is a specified function.

Definition 1. *A CQ-MAC code $c_f = (n, e_1, e_2, \boldsymbol{\lambda})$ of block-length n for recovering f consists of two encoding maps $e_j : \mathcal{S}_j^n \to \mathcal{X}_j^n : j \in [2]$, and a POVM $\boldsymbol{\lambda} = \{\lambda_{r^n} \in \mathcal{P}(\mathcal{H}_Z) : r^n \in \mathcal{R}^n\}$. The average error probability of c_f for $\mathcal{N}_2$ is*

$$\bar{\xi}(c_f, \mathcal{N}_2) = 1 - \sum_{\underline{s}^n : f(\underline{s}^n) = r^n} \mathbb{W}^n_{S_1 S_2}(s_1^n, s_2^n) \operatorname{Tr}\left(\lambda_{r^n} \rho^{\otimes n}_{c, \underline{s}^n}\right),$$

where $\rho^{\otimes n}_{c,\underline{s}^n} = \otimes_{i=1}^n \rho_{x_{1i}(s_1^n) x_{2i}(s_2^n)}$, where $e_j(s_j^n) = (x_{j1}(s_j^n), x_{j2}(s_j^n), \cdots, x_{jn}(s_j^n))$ for $j \in [2]$.

Definition 2. *A function f of the sources $\mathbb{W}_{S_1 S_2}$ is said to be reconstructible over a CQ-MAC $\mathcal{N}_2$ if for all $\epsilon > 0$, $\exists$ a sequence $c_f^{(n)} = (n, e_1^{(n)}, e_2^{(n)}, \boldsymbol{\lambda})$ such that $\lim_{n \to \infty} \bar{\xi}(c_f^{(n)}, \mathcal{N}_2) = 0$. Restricting f to a sum, we say that the sum of sources $\mathbb{W}_{S_1 S_2}$ over field $\mathbb{F}_q$ is reconstructible over a CQ-MAC if $\mathcal{S}_1 = \mathcal{S}_2 = \mathbb{F}_q$ and the function $f(S_1, S_2) = S_1 \oplus S_2$ is reconstructible over the CQ-MAC.*

We review the performance limit achievable using unstructured code ensembles in the following.

Proposition 1. *A function f of the sources $\mathbb{W}_{S_1 S_2}$ is reconstructible over a CQ-MAC $\mathcal{N}_2$ if*

$$H(S_1, S_2) < \max_{p_{X_1} p_{X_2}} I(X_1 X_2; Z)_\sigma, \tag{1}$$

where the mutual information is defined for the following classical-quantum state

$$\sigma \triangleq \sum_{x_1 x_2} p_{X_1}(x_1) p_{X_2}(x_2) \rho_{x_1 x_2} \otimes |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| .$$

Proof. The technique involves using the Slepian-Wolf [10] source coding to compress the source to $H(S_1, S_2)$ bits, and followed by the Winter's channel coding over the CQ-MAC $\mathcal{N}_2$ [3]. □

The objective of our work is to characterize improved sufficient conditions under which a generic bivariate function of the sources is reconstructible over a CQ-MAC $\mathcal{N}_2$ by developing a structured coding framework for this problem.

III. Main Results

A. Nested Coset Codes Achieve Capacity of CQ-P2P

We begin by formalizing the notion of a CQ-P2P codes for communicating uniform messages. In the results presented below, we characterize the asymptotic performance of NCCs and demonstrate that it achieves the capacity of a CQ-P2P channel.

Definition 3. *A CQ-P2P code $c_m = (n, \mathcal{I}, e, \boldsymbol{\lambda})$ for a CQ-P2P $\mathcal{N} : (\rho_x \in \mathcal{D}(\mathcal{H}_Z) : x \in \mathcal{X})$ consists of (i) an index set $\mathcal{I}$, (ii) an encoding map $e : \mathcal{I} \to \mathcal{X}^n$, and (iii) a decoding POVM $\boldsymbol{\lambda} = \{\lambda_m \in \mathcal{P}(\mathcal{H}_Z^{\otimes n}) : m \in \mathcal{I}\}$. For $m \in \mathcal{I}$, we let $\rho^{\otimes n}_{c,m} \triangleq \otimes_{i=1}^n \rho_{x_i}$ where $e(m) = (x_1(m), \cdots, x_n(m))$. The rate of the code is $\frac{1}{n} \log |\mathcal{I}|$, and the average probability of error is*

$$\bar{\xi}(c, \mathcal{N}) = 1 - |\mathcal{I}|^{-1} \sum_{m \in \mathcal{I}} \operatorname{Tr}\left(\lambda_m \rho^{\otimes n}_{c,m}\right).$$

Definition 4. *An $(n, k, l, g_I, g_{O/I}, b^n, \tilde{e})$ NCC built over a finite field $\mathbb{F}_q$ comprises of (i) generator matrices $g_I \in \mathbb{F}_q^{k \times n}$, $g_{O/I} \in \mathbb{F}_q^{l \times n}$ (ii) a bias vector b^n, and (iii) an encoding map $\tilde{e} : \mathbb{F}_q^l \to \mathbb{F}_q^k$. We let $v^n(a, m) = a g_I \oplus m g_{O/I} \oplus b^n$ for $(a, m) \in \mathbb{F}_q^k \times \mathbb{F}_q^l$ denote elements in the coset of the range space of the generator matrix $[g_I^T \; g_{O/I}^T]^T$.*

Remark 1. *Note that in an NCC, the denser (outer) code is generated by the matrix $[g_I^T \; g_{O/I}^T]^T$, whereas the sparser (inner) code is generated by the matrix g_I. Both codes are shifted by a common bias vector. Although this is a packing problem (over the denser code), we additionally perform covering over the sparser code. This additional layer of covering is needed because we generate all codewords not from an arbitrary non-uniform distribution, but from a random coset code that induces a uniform single-letter distribution on the alphabet $\mathbb{F}_q$.*

Definition 5. *A CQ-P2P code $(n, \mathcal{I}, e, \boldsymbol{\lambda})$ is said to be based on NCC if there exists an $(n, k, g_I, g_{O/I}, b^n, \tilde{e})$ NCC such that $\mathcal{I} = \mathbb{F}_q^l$, and $e(m) = g^n(v^n(\tilde{e}(m), m))$, for some mapping $g : \mathbb{F}_q \to \mathcal{X}$.*

Theorem 1. *Given a CQ-P2P $\mathcal{N} : (\rho_x \in \mathcal{D}(\mathcal{H}_Z) : x \in \mathcal{X})$, a PMF p_{VX} on $\mathbb{F}_q \times \mathcal{X}$, and an $\epsilon > 0$, there exists a CQ-P2P code $c = (n, \mathbb{F}_q^l, e, \boldsymbol{\lambda})$ based on NCC such that*

$$(i)\ \bar{\xi}(c, \mathcal{N}) \leq \epsilon, (ii)\ \frac{k}{n} \log_2 q > \log_2 q - H(V) \text{ and}$$
$$\frac{(k+l)}{n} \log_2 q < \log_2 q - H(V) + I(V; Z)_\sigma,$$

for all sufficiently large n, where the classical-quantum state σ is given as

$$\sigma \triangleq \sum_{v \in \mathbb{F}_q} \sum_{x \in \mathcal{X}} p_{VX}(v, x) \, |v\rangle\langle v| \otimes \rho_x.$$

Thus the rate of the code satisfies: $\frac{l}{n} \log q < I(V; Z)_\sigma$.

Proof. The proof is provided in Section V. □

Remark 2. *We interpret the above result as follows. To achieve the capacity, we need an NCC where the rate of the sparser (covering) code is approximately equal to $\log_2 q - H(V)$ (from above), which is the relative entropy between the uniform distribution and p_V. The rate of the denser (packing) code is approximately equal to $\log_2 q - H(V) + I(V; Z)_\sigma$ (from below), which is the capacity with the additional covering cost.*

B. Decoding the Sum over CQ-MAC $\mathcal{N}_2$

As a pedagogical step, our next result is regarding the setup where a centralized receiver of an arbitrary CQ-MAC $\mathcal{N}_2$ intends to reconstruct the sum $f(S_1, S_2) = S_1 \oplus S_2$ of the sources, where $\mathcal{S} \triangleq \mathcal{S}_1 = \mathcal{S}_2 = \mathbb{F}_q$. Toward this, we begin with the following definition.

Definition 6. *Let $\mathbb{F}_q$ be a finite field and $(\rho_{x_1x_2} \in \mathcal{D}(\mathcal{H}_Z) : (x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2)$ be a CQ-MAC $\mathcal{N}_2$. A CQ-MAC code $c_{m\oplus} = (n, \mathbb{F}_q^l, e_1, e_2, \boldsymbol{\lambda})$ of block-length n for recovering $\mathbb{F}_q-$sum of messages consists of two encoders maps $e_j : \mathbb{F}_q^l \to \mathcal{X}_j^n : j \in [2]$, and a POVM $\boldsymbol{\lambda} = \{\lambda_m \in \mathcal{P}(\mathcal{H}_Z^{\otimes n}) : m \in \mathbb{F}_q^l\}$.*

An $\mathbb{F}_q-$message-sum rate $R > 0$ is achievable if given any sequence $l(n) \in \mathbb{N}$, for $n \in \mathbb{N}$, such that $\limsup_{n\to\infty} \frac{l(n)\log q}{n} < R$, any sequence $p^{(n)}_{M_1M_2}$ of PMFs on $\mathbb{F}_q^{l(n)} \times \mathbb{F}_q^{l(n)}$, there exists a CQ-MAC code $c^{(n)}_{m\oplus} = (n, \mathbb{F}_q^{l(n)}, e_1^{(n)}, e_2^{(n)}, \boldsymbol{\lambda})$ of block-length n for recovering $\mathbb{F}_q-$sum of messages such that

$$\lim_{n\to\infty} \bar{\xi}(c^{(n)}_{m\oplus}, \mathcal{N}_2) \triangleq \lim_{n\to\infty} 1 - \sum_{(m_1,m_2)\in\mathbb{F}_q^l\times\mathbb{F}_q^l} p^{(n)}_{M_1M_2}(m_1, m_2)\,\mathrm{Tr}\Big(\lambda_{m_1\oplus m_2}\rho^{\otimes n}_{c,\underline{m}}\Big) = 0,$$

where $\rho^{\otimes n}_{c,\underline{m}} \triangleq \otimes_{i=1}^n \rho_{x_{1i}(m_1)x_{2i}(m_2)}$ and $e_j(m_j) = (x_{j1}(m_j), x_{j2}(m_j), \cdots, x_{jn}(m_j))$ for $j \in [2]$. The closure of the set of all achievable $\mathbb{F}_q-$message-sum rates is the message-sum capacity of $\mathcal{N}_2$.

We now provide a lower bound on the message-sum capacity of a CQ-MAC. Following this, we leverage the above argument in Theorem 2 to characterize sufficient conditions for reconstructing sum of sources over an arbitrary CQ-MAC.

Definition 7. *Given a CQ-MAC $\mathcal{N}_2$ and a prime q, let $\mathscr{P}(\mathcal{N}_2, q)$ be defined as collection of PMFs*

$$\left\{ p_{V_1V_2X_1X_2} : \begin{array}{c} \mathcal{V} = \mathbb{F}_q, \\ p_{V_1V_2X_1X_2} \text{ is a PMF on } \mathcal{V}\times\mathcal{X}_1\times\mathcal{V}\times\mathcal{X}_2, \\ (V_1, X_1) \text{ is independent of } (V_2, X_2) \end{array} \right\}.$$

Let,

$$\mathscr{R}(\mathcal{N}_2, q) \triangleq \sup_{p_{V_1X_1V_2X_2}\in\mathscr{P}(\mathcal{N}_2,q)} \left[I(V;Z)_\sigma - \max\{I(V_1;V), I(V_2;V)\}\right],$$

where $V = V_1 \oplus V_2$, and the classical-quantum state σ is given as

$$\sigma \triangleq \sum_{v\in\mathbb{F}_q} \sum_{\substack{v_1\in\mathbb{F}_q \\ v_2\in\mathbb{F}_q}} \sum_{\substack{x_1\in\mathcal{X}_1, \\ x_2\in\mathcal{X}_2}} p_{V_1X_1}(v_1, x_1) p_{V_2X_2}(v_2, x_2) \times \mathbb{1}_{\{v_1\oplus v_2 = v\}} \rho_{x_1x_2} \otimes |v\rangle\langle v| .$$

Using the above definitions, we provide the following proposition.

Proposition 2. *$\mathbb{F}_q-$message-sum rate $\mathscr{R}(\mathcal{N}_2, q)$ is achievable over any CQ-MAC $\mathcal{N}_2$.*

Proof. The proof is provided in Section VI-A. □

We now state the main contribution of this subsection.

Theorem 2. *The sum of a pair of sources distributed with PMF $\mathbb{W}_{S_1S_2}$ can be reconstructed on a CQ-MAC $\mathcal{N}_2$ if $H(S_1 \oplus S_2) < \mathscr{R}(\mathcal{N}_2, q)$.*

Proof. The proof is provided in Section VI-B. □

Remark 3. *$\mathscr{R}(\mathcal{N}_2, q)$ is the maximum achievable rate of the messages whose sum can be computed reliably at the receiver of the CQ-MAC. $H(S_1 \oplus S_2)$ is the rate needed to compress the sources distributively such that their sum can be computed reliably. The term given by $\max\{I(V_1;V), I(V_2;V)\}$ can be interpreted as the overall informational cost of having non-uniform input distributions p_{V_1} and p_{V_2}. If V_1 and V_2 are uniform, then V becomes independent of V_1 and V_2 individually, and thus this term becomes zero.*

Remark 4. *For the special case where the density operators $\{\rho_{x_1,x_2}\}$ commute, we see that the quantum mutual information (which equals the Holevo information in the present CQ case) reduces to a classical mutual information as given below: $I(V;Z)_\sigma = I(V;Z)$, where $I(V;Z)$ is computed with the following classical PMF*

$$p_{V_1X_1}p_{V_2X_2}\lambda_{Z|X_1X_2},$$

and $\lambda_{Z|X_1X_2}(\cdot|x_1, x_2)$ are the eigenvalues of ρ_{x_1,x_2}. In this case, the asymptotic sufficient condition of the above theorem reduces to that of the classical case as given in [8].

C. Decoding the sum of classical sources over a Quantum-to-Quantum (QQ) MAC $\mathcal{M}_2$

Our next result is regarding a QQ-MAC setup for transmitting classical messages that is composed of a completely-positive trace preserving (CPTP) map $\mathcal{M}_2$. Consider a (generic) QQ-MAC specified through (i) Hilbert spaces $\mathcal{H}_{X_1}$, $\mathcal{H}_{X_2}$, and $\mathcal{H}_Z$ and (ii) a CPTP map $\mathcal{M}_2 : \mathcal{D}(\mathcal{H}_{X_1}) \otimes \mathcal{D}(\mathcal{H}_{X_2}) \to \mathcal{D}(\mathcal{H}_Z)$. In this setting, the centralized receiver of an arbitrary QQ-MAC $\mathcal{M}_2$ intends to reconstruct the sum $f(S_1, S_2) = S_1 \oplus S_2$ of the classical correlated sources, where $\mathcal{S} \triangleq \mathcal{S}_1 = \mathcal{S}_2 = \mathbb{F}_q$. Toward this, we begin with the following definition.

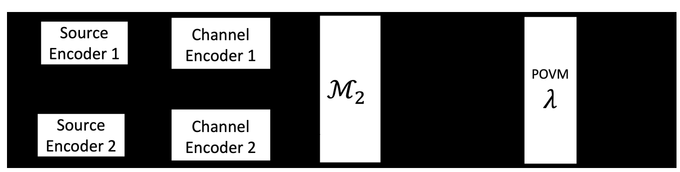

Fig. 2. A schematic of the problem of computing the sum of classical correlated sources with joint distribution $\mathbb{W}_{S_1S_2}$ over a QQ-MAC $\mathcal{M}_2$.

Definition 8. *Let $\mathbb{F}_q$ be a finite field and $\mathcal{M}_2 : \mathcal{D}(\mathcal{H}_{X_1}) \otimes \mathcal{D}(\mathcal{H}_{X_2}) \to \mathcal{D}(\mathcal{H}_Z)$ be a CPTP map. A QQ-MAC code $c_{m\oplus} = (n, \mathbb{F}_q^l, e_1, e_2, \boldsymbol{\lambda})$ of block-length n for recovering $\mathbb{F}_q-$sum of messages consists of two encoder maps $e_j : \mathbb{F}_q^l \to \mathcal{D}(\mathcal{H}_{X_j}^{\otimes n}) : j \in [2]$, and a POVM $\boldsymbol{\lambda} = \{\lambda_m \in \mathcal{P}(\mathcal{H}_Z^{\otimes n}) : m \in \mathbb{F}_q^l\}$. An $\mathbb{F}_q-$message-sum rate $R > 0$ is achievable if given any sequence $l(n) \in \mathbb{N}$, for $n \in \mathbb{N}$, such that $\limsup_{n\to\infty} \frac{l(n)\log q}{n} < R$, any sequence $p^{(n)}_{M_1M_2}$ of PMFs on $\mathbb{F}_q^{l(n)} \times \mathbb{F}_q^{l(n)}$, there exists a QQ-MAC code $c^{(n)}_{m\oplus} = (n, \mathbb{F}_q^{l(n)}, e_1^{(n)}, e_2^{(n)}, \boldsymbol{\lambda})$ of block-length n for recovering $\mathbb{F}_q-$sum of messages such that*

$$\lim_{n\to\infty} \bar{\xi}(c^{(n)}_{m\oplus}, \mathcal{M}_2) \triangleq \lim_{n\to\infty} 1 - \sum_{(m_1,m_2)\in\mathbb{F}_q^l\times\mathbb{F}_q^l} p^{(n)}_{M_1M_2}(m_1, m_2)$$

$$\times \operatorname{Tr}\big(\lambda_{m_1 \oplus m_2}\ \mathcal{M}_2^{\otimes n}(\rho_{m_1} \otimes \rho_{m_2})\big) = 0,$$

where $\rho_{m_j} = e_j(m_j) : j \in [2]$. The closure of the set of all achievable $\mathbb{F}_q-$message-sum rates is the message-sum capacity of $\mathcal{M}_2$.

We now provide a lower bound on the message-sum capacity of a QQ-MAC. Following this, we leverage the above argument in Theorem 3 to characterize sufficient conditions for reconstructing sum of sources over an arbitrary QQ-MAC.

Definition 9. *Given a QQ-MAC $\mathcal{M}_2$ and a prime q, let,*

$$\mathscr{R}_Q(\mathcal{M}_2, q) \triangleq \sup_{\mathcal{N}_2^{X_1}, \mathcal{N}_2^{X_2}} \mathscr{R}(\mathcal{M}_2(\mathcal{N}_2^{X_1} \otimes \mathcal{N}_2^{X_2}), q),$$

where the supremum is over all CQ-P2P channels $\mathcal{N}_2^{X_i} = (\rho_{x_i}^{X_i} \in \mathcal{D}(\mathcal{H}_{X_i}) : x_i \in \mathcal{X}_i)$ for $i \in [2]$, $\mathcal{X}_i$ are finite sets, $\mathcal{M}_2(\mathcal{N}_2^{X_1} \otimes \mathcal{N}_2^{X_2})$ denotes the induced CQ-MAC obtained by concatenating CQ-P2Ps $(\mathcal{N}_2^{X_1}, \mathcal{N}_2^{X_2})$ and QQ-MAC $\mathcal{M}_2$, and $\mathscr{R}(\mathcal{M}_2(\cdot), \cdot)$ follows from Definition 7. Note that the input alphabets of the induced CQ-MAC are $\mathcal{X}_1$ and $\mathcal{X}_2$.

Using the above definitions, we provide the following proposition.

Proposition 3. *$\mathbb{F}_q-$message-sum rate $\mathscr{R}_Q(\mathcal{M}_2, q)$ is achievable over any QQ-MAC $\mathcal{M}_2$.*

Proof. The proof follows the same arguments as those given in the proof of Proposition 2. □

We now state the main contribution of this subsection.

Theorem 3. *The sum of a pair of sources distributed with PMF $\mathbb{W}_{S_1 S_2}$ can be reconstructed on a QQ-MAC $\mathcal{M}_2$ if $H(S_1 \oplus S_2) < \mathscr{R}_Q(\mathcal{M}_2, q)$.*

Proof. The proof follows the same arguments as those given in the proof of Theorem 2. □

D. Decoding arbitrary functions over CQ-MAC

To address this problem, as a building block, we consider the problem of 4-to-3 decoding over a 4-user CQ-MAC, where the receiver aims to compute the sum of messages of user 1 and 2, and the individual messages of users 3 and 4. We obtain a characterization of asymptotic performance limits for this problem. Based on the result we obtain for this problem, and using the result of Ahlswede and Han [9], we derive sufficient conditions for reconstructing arbitrary function of sources over a 2 user CQ-MAC. The former problem may also be of independent interest.

Consider a (generic) 4-user CQ-MAC $\mathcal{N}_4$, which is specified through (i) finite (input) sets $\mathcal{V}_j : j \in [2]$ and $\mathcal{U}_j : j \in [2]$, (ii) a (output) Hilbert space $\mathcal{H}_Z$, and (iii) a collection of density operators $(\rho_{v_1 v_2 u_1 u_2} \in \mathcal{D}(\mathcal{H}_Z) : (v_1, v_2, u_1, u_2) \in \mathcal{V}_1 \times \mathcal{V}_2 \times \mathcal{U}_1 \times \mathcal{U}_2)$.

Definition 10. *A code $c = (n, \mathbb{F}_q, e_{V_j} : j \in [2],\ e_{U_j} : j \in [2], \boldsymbol{\lambda})$ of block-length n, for 4-to-3 decoding over CQ-MAC $\mathcal{N}_4$ consists of four encoding maps $e_{V_j} : \mathbb{F}_q^l \to \mathcal{V}_j^n : j \in [2]$, $e_{U_j} : [q^{l_j}] \to \mathcal{U}_j^n : j \in [2]$, and a POVM $\boldsymbol{\lambda} = \{\lambda_{m^\oplus, m_3, m_4} \in \mathcal{P}(\mathcal{H}_Z) : (m^\oplus, m_3, m_4) \in \mathbb{F}_q^l \times [q^{l_1}] \times [q^{l_2}]\}$, where $m^\oplus \triangleq m_1 \oplus m_2$, l, l_1 and l_2 are positive integers, and q is a prime number.*

Definition 11. *Given a CQ-MAC $\mathcal{N}_4$, and a prime q, a rate triple $(R, R_1, R_2) > \underline{0}$ is said to be achievable for 4-to-3 decoding over the CQ-MAC if given any sequence of triples $(l(n), l_1(n), l_2(n))$, such that $\limsup_{n\to\infty} \frac{l(n)}{n} \log q < R, \limsup_{n\to\infty} \frac{l_i(n)}{n} \log q < R_i : i \in [2]$, and any sequence $p^{(n)}_{M_1 M_2 M_3 M_4}$ of PMFs on $\mathbb{F}_q^l \times \mathbb{F}_q^l \times [q^{l_1}] \times [q^{l_2}]$, there exists a code $c^{(n)} = (n, \mathbb{F}_q, e_{V_j} : j \in [2], e_{U_j} : j \in [2], \boldsymbol{\lambda})$ for 4-to-3 decoding over CQ-MAC $\mathcal{N}_4$ of block-length n such that*

$$\limsup_{n\to\infty} \bar{\xi}(c^{(n)}, \mathcal{N}_4) \triangleq$$
$$\limsup_{n\to\infty} 1 - \sum_{\underline{m}} p_{\underline{M}}(\underline{m}) \operatorname{Tr}\Big(\lambda_{m^\oplus, m_3, m_4} \rho_{\underline{m}}^{\otimes n}\Big) = 0,$$

where $\rho_{\underline{m}}^{\otimes n} \triangleq \rho_{v_1^n(m_1) v_2^n(m_2) u_1^n(m_3) u_2^n(m_4)} = \otimes_{i=1}^n \rho_{v_{1i}(m_1) v_{2i}(m_2) u_{1i}(m_3) u_{2i}(m_4)}$ (assuming n-independent uses of $\mathcal{N}_4$). The union of the set of all achievable rate triples (R, R_1, R_2) is the capacity region of the 4-to-3 decoding over CQ-MAC $\mathcal{N}_4$ and prime number q.

Definition 12. *Given a CQ-MAC $\mathcal{N}_4$ and a prime q, let $\mathscr{P}(\mathcal{N}_4,\ q)$ be defined as collection of PMF $\{p_{\underline{VU}} : p_{\underline{VU}} = p_{V_1} p_{V_2} p_{U_1} p_{U_2}$ is a PMF on $\underline{\mathcal{V}} \times \underline{\mathcal{U}}\}$. For $p_{\underline{VU}} \in \mathscr{P}(\mathcal{N}_4, q)$, let $\mathscr{R}(p_{\underline{VU}}, \mathcal{N}_4, q)$ be the set of rate triples (R, R_1, R_2) such that the following inequalities holds:*

$$\begin{aligned}
R &\leq I(V; Z|U_1, U_2)_\sigma - I_{\max}(V_1, V_2, V)_\sigma, \\
R_1 &\leq I(U_1; Z|V, U_2)_\sigma, \\
R_2 &\leq I(U_2; Z|V, U_1)_\sigma, \\
R + R_1 &\leq I(V, U_1; Z|U_2)_\sigma - I_{\max}(V_1, V_2, V)_\sigma, \\
R + R_2 &\leq I(V, U_2; Z|U_1)_\sigma - I_{\max}(V_1, V_2, V)_\sigma, \\
R_1 + R_2 &\leq I(U_1, U_2; Z|V)_\sigma \\
R + R_1 + R_2 &\leq I(V, U_1, U_2; Z)_\sigma - I_{\max}(V_1, V_2, V)_\sigma,
\end{aligned}$$

where $I_{\max}(V_1, V_2, V)_\sigma = \max\{I(V_1; V), I(V_2; V)\}$, $V = V_1 \oplus V_2$, and the mutual information quantities are taken with respect to the classical-quantum state

$$\sigma \triangleq \sum_{\underline{v}, \underline{u}, v} p_{\underline{VU}}(\underline{v}, \underline{u}) \mathbb{1}_{\{v = v_1 \oplus v_2\}} |v\rangle\langle v|_{\mathrm{V}} \otimes |v_1\rangle\langle v_1|_{\mathrm{V}_1} \otimes |v_2\rangle\langle v_2|_{\mathrm{V}_2}$$
$$\otimes |u_1\rangle\langle u_1|_{\mathrm{U}_1} \otimes |u_2\rangle\langle u_2|_{\mathrm{U}_2} \otimes \rho_{\underline{vu}}.$$

Let

$$\mathscr{R}(\mathcal{N}_4, q) \triangleq \text{c.c.} \bigcup_{p_{\underline{VU}} \in \mathscr{P}(\mathcal{N}_4, q)} \mathscr{R}(p_{\underline{VU}}, \mathcal{N}_4, q),$$

where c.c *stands for convex closure.*

Theorem 4. *The rate triples $(R, R_1, R_2) \in \mathscr{R}(\mathcal{N}_4, q)$ are achievable for 4-to-3 decoding over a CQ-MAC $\mathcal{N}_4$ and prime q.*

Proof. The proof is provided in Section VII-A. □

Remark 5. *As in Theorem 2, if the density operators associated with the channel commute, then the quantum mutual information quantities reduce to the classical counterparts.*

Here we provide our main result characterizing the sufficient conditions on the sources, for any reconstruction of the bivariate function f at the decoder of the given CQ-MAC $\mathcal{N}_2$. Before we proceed, we provide the following definition for embedding a function into a finite field.

Definition 13. *A function $f : \underline{\mathcal{S}} \to \mathcal{R}$ of sources $\mathbb{W}_{S_1S_2}$ is said to be embeddable in a finite field $\mathbb{F}_q$ if there exists (i) a pair of functions $h_j : \mathcal{S}_j \to \mathbb{F}_q$ for $j \in [2]$, and (ii) a function $g : \mathbb{F}_q \to \mathcal{R}$, such that $\mathbb{W}_{S_1S_2}(f(S_1,S_2) = g(h_1(S_1) \oplus h_2(S_2))) = 1$.*

Remark 6. *Note that for any given function f, the set of prime q for which f is embeddable with respect to $\mathbb{F}_q$ is always non-empty. To see this, take $q > |\mathcal{S}_1||\mathcal{S}_2|$, and let h_1 be any one-to-one mapping from $|\mathcal{S}_1|$ to $\{0,1,...,|\mathcal{S}_1|-1\}$, and let h_2 be any one-to-one from $|\mathcal{S}_2|$ to $\{0,|\mathcal{S}_1|,2|\mathcal{S}_1|,...,|\mathcal{S}_1|(|\mathcal{S}_2|-1)\}$. Then, $h_1(\cdot) \oplus h_2(\cdot)$ is a one-to-one map from $|\mathcal{S}_1| \times |\mathcal{S}_2|$ to $\mathbb{F}_q$ (see [7, Def. 3.7]). For example, the nonlinear logical OR ($\vee$) function of binary sources with $\mathcal{S}_1 = \mathcal{S}_2 = \{0,1\}$ can be embedded in $\mathbb{F}_3$, by noting that $S_1 \vee S_2 = g(h_1(S_1) \oplus_3 h_2(S_2))$, where g is given by $g : 0 \mapsto 0,\ 1 \mapsto 1$, and $2 \mapsto 1$, and h_is are identity maps.*

Definition 14. *Given the source $(\mathcal{S}_1,\mathcal{S}_2,\mathbb{W}_{S_1S_2},f)$, consider a prime q such that f is embeddable (according to Definition 13) in $\mathbb{F}_q$. Let $\mathcal{P}$ be the set of PMFs $p_{QW_1W_2|S_1S_2}$ defined on $\mathcal{Q} \times \mathcal{W}_1 \times \mathcal{W}_2$ such that (a) Q and (S_1,S_2) are independent, (b) $W_1 - S_1Q - S_2Q - W_2$ forms a Markov chain, and (c) $\mathcal{Q},\mathcal{W}_1,\mathcal{W}_2$ are finite sets. For $p_{QW_1W_2|S_1S_2} \in \mathcal{P}$, let us define,*

$$\begin{aligned}\mathscr{R}_S(p_{QW_1W_2|S_1S_2},q) \triangleq \Big\{(R,R_1,R_2)\colon & R \geq H(S|W_1W_2Q),\\ & R_1 \geq I(S_1;W_1|QW_2),\\ & R_2 \geq I(S_2;W_2|QW_1),\\ & R_1+R_2 \geq I(S_1S_2;W_1W_2|Q)\Big\},\end{aligned}$$

where $S = h_1(S_1) \oplus h_2(S_2)$. Define

$$\mathscr{R}_s(\mathbb{W}_{S_1S_2},f,q) \triangleq \text{c.c.} \bigcup_{p\in\mathcal{P}} \mathscr{R}_S(p,q).$$

Definition 15. *Given a CQ-MAC $\mathcal{N}_2$, and prime q, let $\mathscr{P}$ be the set of PMFs $p_{X_1|U_1V_1}$ and $p_{X_2|U_2V_2}$ with the input alphabets $(\mathcal{U}_1,\mathcal{V}_1)$ and $(\mathcal{U}_2,\mathcal{V}_2)$, and output alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, respectively. Define,*

$$\mathscr{R}_C(p_{X_1|U_1V_1},p_{X_2|U_2V_2},q) = \mathscr{R}(\mathcal{N}_4,q),$$

where the corresponding 4-user CQ-MAC $\mathcal{N}_4$ is characterized as:

$$\rho_{\underline{vu}} = \sum_{x_1x_2} p_{X_1|U_1V_1}(x_1|u_1v_1)p_{X_2|U_2V_2}(x_2|u_2v_2)\rho_{x_1x_2}.$$

Define,

$$\mathscr{R}_c(\mathcal{N}_2,q) \triangleq \text{c.c} \bigcup_{\{p_{X_j|U_jV_j}\,:\,j\in[2]\}\in\mathscr{P}} \mathscr{R}_C(p_{X_j|U_jV_j} : j \in [2], q).$$

Theorem 5. *If $\mathscr{R}_s(\mathbb{W}_{S_1S_2},f,q) \subset \mathscr{R}_c(\mathcal{N}_2,q)$ for some prime q, then the bivariate function f of the sources $\mathbb{W}_{S_1S_2}$ is reconstructible over the CQ-MAC $\mathcal{N}_2$.*

Proof. The proof is provided in Section VII-B. □

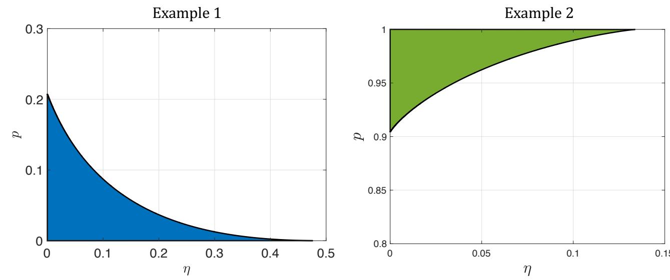

Fig. 3. (Left) A depiction of the set of all pairs (p,η) achievable using the technique of coset codes (Theorem 2) for Example 1. (Right) A depiction of the set of all pairs (p,η) achievable using the technique of coset codes (Theorem 2) for Example 2. The functions in both examples 1 and 2 are not reconstructible using unstructured codes (Proposition 1) for any pair (p,η).

E. Examples

In the following examples, for ease of exposition, we express the quantum mutual information in terms of the Holevo information [17], [18].

Example 1. *Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{S}_1 = \mathcal{S}_2 = \mathcal{X} = \{0,1\}$, $\mathcal{H}_Z = \mathbb{C}^2$, and $\rho_{x_1x_2} = (1-\eta)\sigma_x + \eta\sigma_{\bar{x}}$, where $x \triangleq x_1 \oplus_2 x_2$ and $\sigma_0,\sigma_1 \in \mathcal{D}(\mathcal{H}_Z)$ be arbitrary. Let $\rho(\eta) \triangleq (1-\eta)\sigma_0 + \eta\sigma_1$. Consider correlated symmetric individually uniform sources with $\mathbb{W}_{S_1|S_2}(1|0) = \mathbb{W}_{S_1|S_2}(0|1) = p$ for $p \in (0,1)$. Let $f(S_1,S_2) = S_1 \oplus_2 S_2$. Consider the sufficient conditions given by the unstructured coding scheme as provided in Proposition 1,*

$$H(S_1,S_2) < \max_{p_{X_1X_2}} \chi(\{p_{X_1X_2}(x_1,x_2),\rho_{x_1,x_2}\}),$$

with X_1 and X_2 being independent. Since, $\chi(\{p_{X_1X_2}(x_1,x_2),\rho_{x_1x_2}\}) = \chi(\{p_X(x),\rho_x\}) \leq 1,\ \forall\ \eta \in [0,1]$, where $X \triangleq X_1 \oplus_2 X_2$, and $\rho_x \triangleq \rho_{x_1x_2}$ for any (x_1,x_2) that satisfies $x = x_1 \oplus x_2$, and $H(S_1,S_2) = 1 + h_b(p) \geq 1$, the function f is never reconstructible using the unstructured codes. Now consider the sufficient condition obtained using the coset codes (Theorem 2), i.e. $H(S_1 \oplus S_2) < \mathscr{R}(\mathcal{N}_2,q)$, which can be simplified as

$$\begin{aligned}h_b(p) < \max_{\theta} \big[&h_b(\theta) - h_b(2\theta(1-\theta)) + S(\rho(2\theta(1-\theta) * \eta))\\ &- [\theta^2 + (1-\theta)^2]S(\rho(\eta)) - 2\theta(1-\theta)S(\rho(1-\eta))\big].\end{aligned}$$

Figure 3 (left) depicts all pairs (p,η) that satisfy the above inequality for the following choice of σ_0, σ_1:

$$\sigma_0 \triangleq \begin{pmatrix} 0.9545 & 0.0455i \\ -0.0455i & 0.0455 \end{pmatrix},\ \sigma_1 \triangleq \begin{pmatrix} 0.0455 & 0.0455i \\ -0.0455i & 0.9545 \end{pmatrix} \quad (2)$$

Note that the above σ_0 and σ_1 do not commute.

Example 2. *Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{S}_1 = \mathcal{S}_2 = \mathcal{X} = \{0,1\}$, $\mathcal{H}_Z = \mathbb{C}^2$, and $\rho_{x_1x_2} = (1-\eta)\sigma_{(x_1\vee x_2)} + \eta\sigma_{(\bar{x}_1\wedge\bar{x}_2)}$, where $\sigma_0,\sigma_1 \in \mathcal{D}(\mathcal{H}_Z)$ be arbitrary. Let $\rho(\eta) \triangleq (1-\eta)\sigma_0 + \eta\sigma_1$. Consider correlated symmetric individually uniform sources with $\mathbb{W}_{S_1|S_2}(1|0) = \mathbb{W}_{S_1|S_2}(0|1) = p$ for $p \in (0,1)$. Let $f(S_1,S_2) = S_1 \vee S_2$. Consider the sufficient conditions given by the unstructured coding scheme: $H(S_1,S_2) < \max_{p_{X_1X_2}} \chi(\{p_{X_1,X_2}(x_1,x_2),\rho_{x_1x_2}\})$, with X_1 and X_2 being independent, This again implies that the f is not reconstructible using the unstructured codes. We embed f in the* *ternary field. In other words, the encoders and decoder work toward reconstructing $S_1 \oplus_3 S_2$. The sufficient condition given by the algebraic coding scheme turns out to be*

$$H(S_1 \oplus_3 S_2) < \max_{p_{X_1} p_{X_2}} \left[\min\{H(X_1), H(X_2)\} - H(X) + \chi(\{p_X(x), \rho_x\}) \right],$$

where $X \triangleq X_1 \oplus_3 X_2$ and $\rho_x \triangleq \sum_{x_1 x_2} p_{X_1 X_2 | X}(x_1, x_2 | x) \rho_{x_1 x_2}$. This can be further simplified as

$$\begin{aligned}(1-p) + h_b(p) < \max_{\theta_1, \theta_2} \Big[& \min\{h_b(\theta_1), h_b(\theta_2)\} \\ & - h_b(\theta_1 + \theta_2 - \theta_1\theta_2) \\ & - (\theta_1 + \theta_2 - \theta_1\theta_2) h_b(\theta_1\theta_2/(\theta_1 + \theta_2 - \theta_1\theta_2)) \\ & + S(\rho((\theta_1 + \theta_2 - \theta_1\theta_2) * \eta)) \\ - (1-\theta_1)(1-\theta_2) S(\rho(\eta)) & - [\theta_1 + \theta_2 - \theta_1\theta_2] S(\rho(1-\eta)) \Big].\end{aligned}$$

It can be shown that there exists p, η, σ_0 and σ_1 such that the above condition is satisfied. For instance, Figure 3 (right) depicts all the achievable pairs (p, η) for the σ_0 and σ_1 chosen as in Example 1.

Finally, we provide the following example to compare the sufficient conditions obtained in Theorem 2 and Theorem 5.

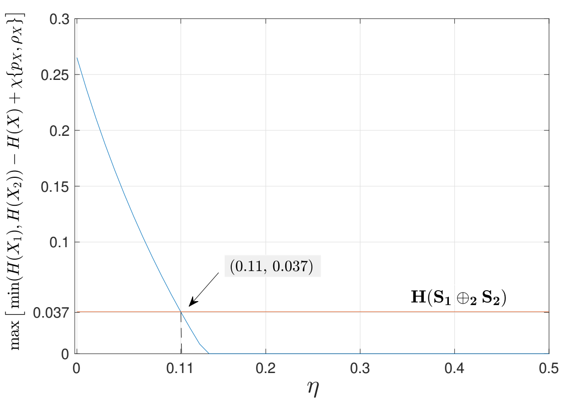

Fig. 4. The variation of the right hand side of (3), and its intersection with $H(S_1 \oplus S_2)$. This implies that the inequality in (3) is not satisfied for all $\eta > 0.11$, and hence the function f cannot be reconstructed using the approach of Theorem 2.

Example 3. *Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{S}_1 = \mathcal{S}_2 = \mathcal{X} = \{0, 1\}$, $\mathcal{H}_Z = \mathbb{C}^2$, and $\rho_{x_1, x_2} = (1-\eta)\sigma_x + \eta\sigma_{\bar{x}}$, where $x = x_1 \oplus_2 x_2$ and $\sigma_0, \sigma_1 \in \mathcal{D}(\mathcal{H}_Z)$ be as defined in (2). Furthermore, to induce asymmetry in the rate region, we constrain one of the inputs with a cost constraint: $\mathbb{E}(X_1) \leq c$. We choose $c = 0.1$ for the illustration. Let S_1 and S_2 be two highly asymmetric correlated sources (as considered in [9, Example 4]) with the following distribution:*

$$\mathbb{W}_{S_1, S_2}(0,0) = 0.003920, \mathbb{W}_{S_1, S_2}(0,1) = 0.976080,$$
$$\mathbb{W}_{S_1, S_2}(1,0) = 0.019920, \mathbb{W}_{S_1, S_2}(1,1) = 0.000080,$$

and $P(S_1 = 0) = 0.98, P(S_2 = 0) = 0.023840$. Let $f(S_1, S_2) = S_1 \oplus_2 S_2$. Using Theorem 2 and the fact that $H(S_1 \oplus S_2) = 0.0376223$, we obtain the sufficient conditions for the function f to be reconstructible as

$$0.0376223 < \max_{p_{X_1} p_{X_2}} \min\{H(X_1), H(X_2)\} - H(X) + \chi(\{p_X(x), \rho_x\}), \quad (3)$$

where $X \triangleq X_1 \oplus_2 X_2$ and $\rho_x \triangleq \rho_{x_1 x_2}$ for any (x_1, x_2) such that $x = x_1 \oplus x_2$. Figure 4 depicts the behaviour of the right hand side of the above inequality for different values of η. In particular, the inequality fails for $\eta > 0.11$, and as a result the function f cannot be reconstructed using the approach of Theorem 2 for all $\eta \in (0.11, 0.5)$. Now, we consider the sufficient conditions obtained from Theorem 5. Figure 5, found at the top of the following page, shows the regions $\mathscr{R}_s(\mathbb{W}_{S_1 S_2}, f, 2)$ and $\mathscr{R}_c(\mathcal{N}_2, 2)$ for different values of η, which demonstrates a clear overlap between $\mathscr{R}_s$ and $\mathscr{R}_c$ for $\eta = 0.12$ and $\eta = 0.2$, which implies that the function remains reconstructible for these η values.

F. Applications

The problem of reconstructing functions of sources over a classical MAC, i.e. computation over a MAC, finds extensive applications in several network problems [19]. Examples include coding for many-to-one interference channels [7], compute-and-forward (CAF) strategy for wireless networks [20], network coding for cooperative wireless networks [21], sensor network estimation [22], interference management for cellular uplink channel [23], and wireless network coding [24]. As for the CQ setup, recent works have explored the compute-and-forward (CAF) relaying technique in quantum one-hop relay network and symmetric private information retrieval (SPIR) over a quantum internet network [6]. In this subsection, we discuss some additional applications of computation over a CQ-MAC.

1) Many-to-one classical-to-quantum interference network (CQIC): Interference is often seen as an impediment in a communication network, and decoding messages at the receivers in a multi-user interference channel setting is a challenging problem. However, computing sum over a CQ-MAC can be used to manage interference. Consider a 3-to-1 CQIC with three inputs X_1, X_2 and X_3 and with quantum outputs characterized using density operators $\rho^{Y_1}_{X_1 \oplus X_2 \oplus X_3}$, $\rho^{Y_2}_{X_2}$, and $\rho^{Y_3}_{X_3}$. As illustrated in Figure 6, users 2 and 3 enjoy interference-free CQ-P2P channels. However, receiver 1 suffers interference from users 2 and 3, and it needs to decode the message X_1. A naive approach is to treat the pair (X_2, X_3) as noise and decode X_1. But this is highly sub-optimal because X_2, X_3 encode information corresponding to messages of users 2 and 3, respectively, and is not just a noise. A better strategy is to decode the message pair (X_2, X_3) and then use the successive cancellation technique to decode X_1. It can be noted that the interference is in the form of the sum $X_2 \oplus X_3$. Hence, an even better strategy is to decode only this sum and then apply the successive cancellation technique. This can be improved even further by simultaneous decoding of the sum $X_2 \oplus X_3$ and the

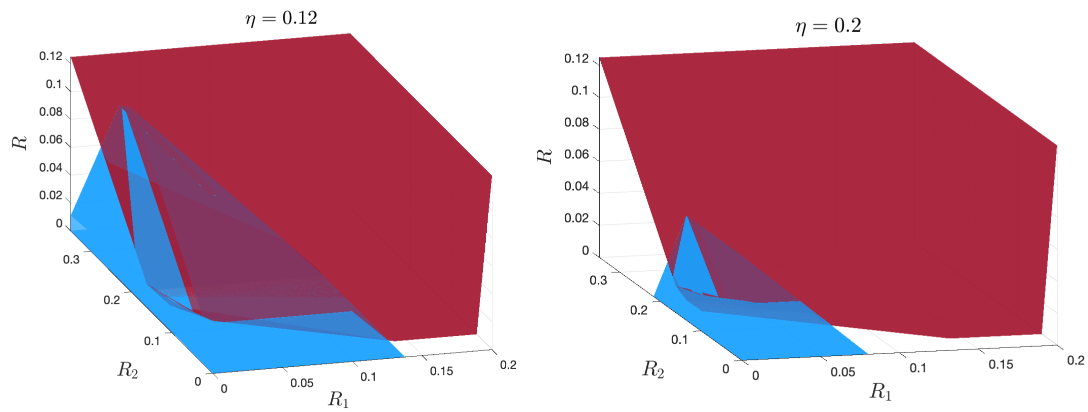

Fig. 5. A depiction of the intersection of $\mathscr{R}_s$ (in red) and $\mathscr{R}_c$ (in blue) for $\eta = 0.12$ and $\eta = 0.2$, using the technique provided in Theorem 5.

intended message X_1 [16]. This demonstrates the need of simultaneous decoding technique as discussed in the previous sections.

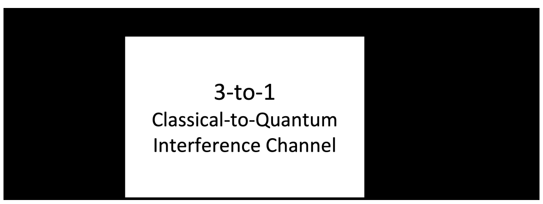

Fig. 6. 3-to-1 classical-to-quantum interference channel (CQIC).

2) Network coding for a cooperative quantum network: Computing sum of messages provides a feasible solution to decrease the number of message transmissions needed within a cooperative quantum network. Consider three satellites that are connected via a free-space quantum optical network and satellite S wants to communicate messages m_1 and m_2 to satellites S_1 and S_2, as shown in Figure 7. In the noncooperative setup, the satellite needs to transmit a total of four messages to S_1 and S_2. Next, in the cooperative decode-and-forward (DAF) setup, satellites S_1 and S_2 can communicate with a relay, however, they cannot directly communicate among themselves. In this case, the missing messages are relayed to S_1 and S_2 as shown. In the cooperative compute-and-forward (CAF) setup, the relay now decodes the sum $(m_1 \oplus m_2)$, instead of the individual messages m_1 and m_2. It then broadcasts the sum of the messages which are received by satellites S_1 and S_2 simultaneously. In the contrast to the previous scenarios, the computation at the relay reduces the total number of transmissions required compared to the other setups. In addition, as the relay is only interested in decoding the sum, it can now receive the information at a larger rate.

IV. The Central Idea

Here we provide an informal review of the central ideas involved in obtaining the main results of this work. The formal proofs are provided in the subsequent sections. Let us consider

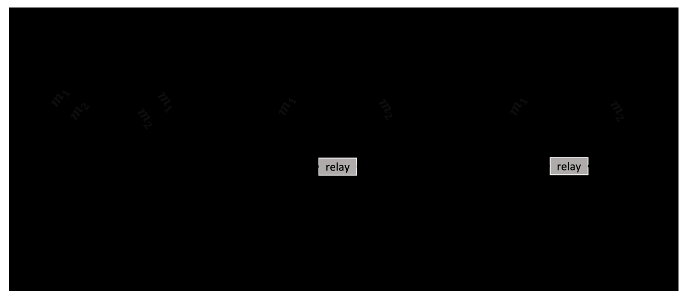

Fig. 7. Compute-and-Forward (CAF) strategy for cooperative free-space quantum optical network.

the specific problem of reconstructing the sum of sources each taking values in $\mathcal{S}_1 = \mathcal{S}_2 = \mathbb{F}_q$. We begin by reviewing the KM coding scheme for the case of a noiseless classical MAC. It was shown in [4], the existence of linear code with a parity check matrix $H \in \mathbb{F}_q^{l \times n}$, and a decoder map $d : \mathbb{F}_q^l \to \mathbb{F}_q^n$ such that for any $\epsilon > 0$ and sufficiently large n, we have

$$\sum_{\underline{s}^n \in \underline{\mathcal{S}}^n} \mathbb{W}^n_{\underline{S}}(\underline{s}^n) \mathbb{1}_{\{d(Hs_1^n \oplus Hs_2^n) \neq s_1^n \oplus s_2^n\}} \leq \epsilon,$$

provided that $\frac{l}{n} \log_2 q > H(S_1 \oplus S_2)$. This implies that a receiver equipped with the decoding map d can recover the sum if it possesses the sum $M_1^l \oplus M_2^l$ of the Körner-Marton indices: $M_j^l = HS_j^l : j \in [2]$.

We are therefore led to a construction of an efficient CQ-MAC coding scheme that enables the receiver only reconstruct the sum of the two message indices. Indeed, if the two senders send the KM indices to such a CQ-MAC channel encoder, and the receiver employs the above source decoder d on the decoded sum of the KM indices, then it can recover the sum of sources. To illustrate the design of the desired CQ-MAC channel code, let us consider a CQ-MAC $(\rho_{x_1 x_2} \in \mathcal{D}(\mathcal{H}_Z) : (x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2)$ wherein $\mathcal{X}_1 = \mathcal{X}_2 = \mathbb{F}_q$ and the collection $\rho_{\underline{x}} : \underline{x} \in \underline{\mathcal{X}}$ satisfies $\rho_{x_1 x_2} = \rho_{\hat{x}_1 \hat{x}_2}$ whenever $x_1 \oplus x_2 = \hat{x}_1 \oplus \hat{x}_2$. Consider a CQ-P2P $(\mathcal{X} = \mathbb{F}_q, \sigma_u : u \in \mathcal{X})$ where $\sigma_u = \rho_{x_1 x_2}$ for any (x_1, x_2) satisfying $x_1 \oplus x_2 = u$. Suppose we are able to communicate over this CQ-P2P via a *linear CQ-P2P code* $\mathcal{C} \subseteq \mathcal{X}^n$. Specifically, suppose there exists a generator matrix $G \in \mathbb{F}_q^{l\times n}$ and a POVM $\boldsymbol{\lambda} \triangleq \{\lambda_{m^l} : m^l \in \mathbb{F}_q^l\}$ such that for any $\epsilon > 0$ and sufficiently large n, we have

$$1 - q^{-l}\sum_{m^l} \mathrm{Tr}\big(\lambda_{m^l}\sigma_{m^lG}^{\otimes n}\big) \leq \epsilon,$$

where $\sigma_{m^lG}^{\otimes} = \sigma_{x_1}\otimes\cdots\otimes\sigma_{x_n}$ where $m^lG = x^n$. We can then use this linear CQ-P2P code as our desired CQ-MAC channel code. Indeed, observe that, suppose both senders employ this same linear CQ-P2P code, then sender j maps its KM index $m_j^l = Hs_j^n$ to the channel codeword as $x_j^n = m_j^lG$. Observe that the structure of the CQ-MAC implies $\rho_{x_1^n,x_2^n}^{\otimes n} = \sigma_{x_1^n\oplus x_2^n}^{\otimes n} = \sigma_{(m_1^l\oplus m_2^l)G}^{\otimes}$. If the receiver employs the POVM $\{\lambda_{m^l} : m^l \in \mathbb{F}_q^l\}$ designed for the CQ-P2P, it ends up decoding the sum of the KM indices $m_1^l \oplus m_2^l$, and consequently, recover the sum of the sources.

A careful analysis of the above idea reveals that two MAC channel codes employed by the encoders do not 'blow up' when added, is crucial to the efficiency of the above scheme. A linear code being algebraically closed enables this. However, the codewords of a random linear code are uniformly distributed and cannot achieve the capacity of an arbitrary classical P2P channel, let alone a CQ-P2P channel. We are therefore forced to enlarge a linear code to identify sufficiently many codewords of the desired empirical single-letter distribution. We are thus led to a *nested coset code* (NCC) [8]. A NCC comprises of cosets of a coarse linear code within a fine code. Within each coset, we can identify a codeword of the desired empirical distribution. We choose as many cosets as the number of messages. Analogous to our illustration above where we chose a linear code that achieves the capacity of the CQ-P2P $(\mathcal{X} = \mathbb{F}_q, \sigma_u : u \in \mathcal{X})$, our first step (Sec. V) is to design a NCC with its POVM that can achieve capacity of an arbitrary CQ-P2P. Our second step is to endow both senders with this same NCC and analyze decoding the sum of the messages. This gets us to our next challenge - How do we analyze decoding their message sum, for a general CQ-MAC $\rho_{\underline{x}} : \underline{x} \in \underline{\mathcal{X}}$ for which $x_1 \oplus x_2 = \hat{x}_1 \oplus \hat{x}_2$ does *not* necessarily imply $\rho_{x_1x_2} = \rho_{\hat{x}_1\hat{x}_2}$. In Sec. III-B, we address this challenge, leverage our findings in Sec. V and generalize the idea for any arbitrary CQ-MAC, and presents a proof of the second set of results (Theorem 2).

The next question we ask is, how can we reconstruct arbitrary functions of the sources? We use the concept of embedding of bivariate functions in finite fields to address this (see Definition 13). Recall that in KM coding, each source encoder produces bits at the rate given by $H(S_1 \oplus S_2)$. This approach works fairly well when the sources are symmetric and uniform. As the source distribution becomes more asymmetric and non-uniform, this approach may become less efficient. For example, if $H(S_2) < H(S_1 \oplus S_2)$, then the second encoder may as well send S_2 losslessly at the rate $H(S_2)$ (while the first encoder still sends HS_1^n) and let the decoder compute HS_2^n, and proceed as before. To address such asymmetry, in the source coding setting, Ahlswede and Han proposed a two-layered coding scheme, where in the first layer, the encoders produce a coarse quantized version of their respective sources, say W_1 and W_2, respectively. The pair is produced such that it is intended to be reconstructed individually, i.e., as a pair (W_1, W_2) at the joint receiver. This is based on the unstructured random coding approach, more akin to the conventional Berger-Tung [25] source coding (lossy Slepian-Wolf coding). Then in the second layer, the KM encoding of the sources is performed, and the resulting information is sent conditioned on the fact that the receiver has access to the coarse version of the sources (W_1, W_2). In essence, this is a (classical) superposition of Berger-Tung source coding and KM source coding, which leads to a smooth transition between KM coding based on structured codes and Slepian-Wolf coding based on unstructured codes. We use this approach on the source coding side. How do we interface this scheme with the two-user CQ-MAC? Encoder i receives two messages (M_{i1}, M_{i2}) at rates R_i and R, respectively. These four messages need to be encoded distributively such that the joint receiver may be able to reconstruct the triple $(M_{11}, M_{21}, M_{12} \oplus M_{22})$. This necessitates using a classical superposition of both unstructured coding as well as structured coding schemes for the CQ-MAC. Noting that the receiver wishes to decode three independent messages simultaneously, we therefore require a CQ simultaneous decoding technique. In Sec. VII, we adapt the technique of tilting, smoothing, and augmentation introduced by Sen [12], [13] to the setting of a superposition of unstructured and structured code (NCC) ensembles to enable this, and provide a proof of Theorem 4. This yields a new set of sufficient conditions, that strictly enlarges the one achievable using solely structured codes (Theorem 2), and thus allows us to obtain a proof of the third main result of our work (Theorem 5).

V. Proof of Theorem 1

As discussed in Sec. IV we shall build and analyze a NCC comprising of cosets of a linear code wherein each coset contains a codeword of the desired empirical distribution for communication over a CQ-P2P $\mathcal{N}$.

Proof. In order to achieve a rate $R = I(V;Z)_\sigma$, the standard approach is to pick 2^{nR} codewords uniformly and independently from $T_\delta^n(p_V)$, for some $\delta > 0$ sufficiently small. However, the resulting code is not algebraically closed. On the other hand, if we pick a random generator matrix $G \in \mathbb{F}_q^{l\times n}$, with $l = \frac{nR}{\log_2 q}$, whose entries from $\mathbb{F}_q$ are IID uniform, then its range space - the resulting collection of 2^{nR} codewords - are uniformly distributed and pairwise independent but not p_V-typical.

To satisfy the dual requirements of algebraically closure and p_V-typicality, we observe the following. If a collection of q^k codewords are uniformly distributed in $\mathbb{F}_q^n$ and pairwise independent, as we found the range space of G to be, then the expected number of codewords that are p_V-typical is $\frac{q^k}{q^n}|T_\delta^n(p_V)| = \exp\{n\log_2 q\left(\frac{k}{n} - \left[1 - \frac{H(V)}{\log_2 q}\right]\right)\}$. This indicates that if we pick a generator matrix $G_I \in \mathbb{F}_q^{k\times n}$ with entries uniformly distributed and IID, such that $\frac{k}{n} > 1 - \frac{H(V)}{\log_2 q}$, then its range space will contain codewords that are p_V-typical. The latter codewords can be used for communication.

Each coset of $G_I \in \mathbb{F}_q^{k\times n}$ where $\frac{k}{n} > 1 - \frac{H(V)}{\log_2 q}$ will play an analogous role as a single codeword in a conventional IID random code. Just as we pick 2^{nR} of the latter, we consider 2^{nR} cosets of G_I within a larger linear code with generator matrix $G = [G_I^T \ G_{O/I}^T]^T \in \mathbb{F}_q^{(k+l)\times n}$ with $l = \frac{nR}{\log_2 q}$. The messages index the 2^{nR} cosets of G_I. A predetermined element in each coset that is p_V-typical is the assigned codeword for the message and chosen for communication.[1] A formal proof we provide below has two parts - error probability analysis for a generic fixed code followed by an upper bound on the latter via code randomization.

Upper bound on error probability for a generic fixed code : Define the following

$$\rho_v \triangleq \sum_{x\in\mathcal{X}} p_{X|V}(x|v)\rho_x,$$

and let $\mathcal{V} = \mathbb{F}_q$. Consider a generic NCC $(n,k,l,g_I,g_{O/I},b^n,\tilde{e})$ with its range space $v^n(a,m) = ag_I \oplus_q mg_{O/I} \oplus_q b^n : (a,m) \in \mathcal{V}^k \times \mathcal{V}^l$. We shall use this and define a CQ-P2P code $(n, \mathcal{I} = \mathcal{V}^l, e, \lambda_{\mathcal{I}})$ that is an NCC CQ-P2P. Towards that end, let $\theta(m) \triangleq \sum_{a\in\mathcal{V}^k} \mathbb{1}_{\{v^n(a,m)\in T_\delta^n(p_V)\}}$ and

$$s(m) \triangleq \begin{cases} \{a \in \mathcal{V}^k : v^n(a,m) \in T_\delta^n(p_V)\} & \text{if } \theta(m) \geq 1 \\ \{0^k\} & \text{if } \theta(m) = 0, \end{cases}$$

for each $m \in \mathcal{V}^l$. For $m \in \mathcal{V}^l$, a predetermined element $a_m = \tilde{e}(m) \in s(m)$ is chosen. On receiving message $m \in \mathcal{V}^l$, the encoder prepares the quantum state $\rho_m^{\otimes n} \triangleq \rho_{v^n(a_m,m)}^{\otimes n} \triangleq \otimes_{i=1}^n \rho_{v_i(a_m,m)}$, and is communicated. The encoding map $\tilde{e}$ is therefore determined via the collection $(a_m \in s(m) : m \in \mathbb{F}_q^l)$.

Towards specifying the decoding POVM let $\rho_v = \sum_{y\in\mathcal{Y}} p_{Y|V}(y|v) \left|e_{y|v}\right\rangle \left\langle e_{y|v}\right|$ be a spectral decomposition for $v \in \mathcal{V}$. We let $p_{VY} \triangleq p_V p_{Y|V}$. For any $v^n \in \mathcal{V}^n$, let π_{v^n} be the conditional typical projector as in [17, Defn. 15.2.4] with respect to the ensemble $\{\rho_v : v \in \mathcal{V}\}$ and distribution p_V. Similarly, let π_ρ be the (unconditional) typical projector of the state $\rho \triangleq \sum_{v\in\mathcal{V}} p_V(v)\rho_v$ as defined in [17, Defn. 15.1.3]. For $(a,m) \in \mathcal{V}^k \times \mathcal{V}^l$, we let $\pi_{a,m} \triangleq \pi_{v^n(a,m)} \mathbb{1}_{\{v^n(a,m)\in T_\delta^n(p_V)\}}$. We let $\boldsymbol{\lambda} \triangleq \{\sum_{a\in\mathcal{V}^k} \lambda_{a,m} : m \in \mathcal{I} = \mathbb{F}_q^l, \lambda_{-1}\}$, where

$$\lambda_{a,m} \triangleq \Big(\sum_{\hat{a}\in\mathcal{V}^k}\sum_{\hat{m}\in\mathcal{V}^l}\gamma_{\hat{a},\hat{m}}\Big)^{-1/2}\gamma_{a,m}\Big(\sum_{\tilde{a}\in\mathcal{V}^k}\sum_{\tilde{m}\in\mathcal{V}^l}\gamma_{\tilde{a},\tilde{m}}\Big)^{-1/2}, \quad (4)$$

$\lambda_{-1} \triangleq I - \sum_{m\in\mathcal{V}^l}\sum_{a\in\mathcal{V}^k}\lambda_{a,m}$ and $\gamma_{a,m} \triangleq \pi_\rho \pi_{a,m} \pi_\rho$. Since $0 \leq \gamma_{a,m} \leq I$, we have $0 \leq \lambda_{a,m} \leq I$. The latter lower bound implies $\boldsymbol{\lambda} \subseteq \mathcal{P}(\mathcal{H})$. The same lower bound coupled with the definition of the generalized inverse implies $I \geq \sum_{a\in\mathcal{V}^k}\sum_{m\in\mathcal{V}^l}\lambda_{a,m} \geq 0$. We thus have $0 \leq \lambda_{-1} \leq I$. It can now be verified that $\boldsymbol{\lambda}$ is a POVM. In essence, the elements of this POVM is identical to the standard POVMs except the POVM elements corresponding to a coset have been added together. Indeed, since each coset corresponds to one message, there is no need to disambiguate within the coset.

[1]The reader is encouraged to relate to the bounds stated in theorem statement and induced bounds on the rate of communication $\frac{l}{n}\log_2 q$.

We have thus associated an NCC $(n,k,l,g_I,g_{O/I},b^n,\tilde{e})$ and a collection $(a_m \in s(m) : m \in \mathcal{V}^l)$ with a CQ-P2P code. The error probability of this code is

$$\begin{aligned} q^{-l}\sum_{m\in\mathcal{I}} \operatorname{tr}((I - \sum_{a\in\mathcal{V}^k}\lambda_{a,m})\rho_m^{\otimes n}) &\leq \\ q^{-l}\sum_{m\in\mathcal{I}} \operatorname{tr}((I - \lambda_{a_m,m})\rho_m^{\otimes n}). & \quad (5) \end{aligned}$$

Denoting event $\mathscr{E} = \{\theta(m) > 1\}$, its complement $\mathscr{E}^c$ and the associated indicator functions $\mathbb{1}_{\mathscr{E}}, \mathbb{1}_{\mathscr{E}^c}$ respectively, a generic term in the RHS of the above sum satisfies

$$\begin{aligned} \operatorname{tr}((I - \lambda_{a_m,m})\rho_m^{\otimes n})\mathbb{1}_{\mathscr{E}^c} + \operatorname{tr}((I - \lambda_{a_m,m})\rho_m^{\otimes n})\mathbb{1}_{\mathscr{E}} \\ \leq \mathbb{1}_{\mathscr{E}^c} + \sum_{i=1}^3 T_{2i}, \end{aligned}$$

where

$$\begin{aligned} T_{21} &\triangleq 2\operatorname{Tr}\big((I - \gamma_{a_m,m})\rho_m^{\otimes n}\big)\mathbb{1}_{\mathscr{E}}, \\ T_{22} &\triangleq 4\sum_{\hat{a}\neq a_m}\operatorname{Tr}\big(\gamma_{\hat{a},m}\rho_m^{\otimes n}\big)\mathbb{1}_{\mathscr{E}}, \\ T_{23} &\triangleq 4\sum_{\hat{m}\neq m}\sum_{\tilde{a}}\operatorname{Tr}\big(\gamma_{\tilde{a},\hat{m}}\rho_m^{\otimes n}\big)\mathbb{1}_{\mathscr{E}}, \end{aligned}$$

where we have used Hayashi-Nagaoka inequality [26].

Distribution of the Random Code : The objects $g_I \in \mathcal{V}^{k\times n}, g_{O/I} \in \mathcal{V}^{l\times n}, b^n \in \mathcal{V}^n$ and the collection $(a_m \in s(m) : m \in \mathcal{V}^l)$ specify an NCC CQ-P2P code unambiguously. A distribution for a random code is therefore specified through a distribution of these objects. We let upper case letters denote the associated random objects, and obtain

$$\mathcal{P}\begin{pmatrix} G_I = g_I, G_{O/I} = g_{O/I} \\ B^n = b^n, A_m = a_m : m \in S(m) \end{pmatrix} = q^{-(k+l+1)n} \times \prod_{m\in\mathcal{V}^l}\frac{1}{\Theta(m)},$$

and analyze the expectation of $\mathscr{E}$ and the terms $T_{2i}; i \in [1,3]$ in regards to the above random code. We begin by $\mathbb{E}_{\mathcal{P}}[\mathscr{E}] = \mathcal{P}(\sum_{a\in\mathcal{V}^k}\mathbb{1}_{\{V^n(a,m)\in T_\delta^n(p_V)\}} < 1)$. For this, we provide the following proposition.

Proposition 4. *For any $\epsilon \in (0,1)$, and for all sufficiently small $\delta > 0$ and sufficiently large n, we have $\mathbb{E}_{\mathcal{P}}[\mathscr{E}] \leq \epsilon$, if $\frac{k}{n} \geq \log q - H(V) + \epsilon$.*

Proof. The proof follows from [7, Proof of Thm. 2.5] with the identification of $\mathcal{S} = \phi$. ☐

We now consider T_{21}. For each a, m, denote the events

$$\mathcal{V} \triangleq \{V^n(a,m) = v^n\}, \quad \mathcal{A} \triangleq \{A_m = a\}.$$

We have

$$\begin{aligned} \mathbb{E}_{\mathcal{P}}[T_{21}] = 1 - \sum_m\sum_a\sum_{v^n\in T_\delta(p_V)} p_M(m)\operatorname{Tr}\big(\pi_{v^n}\pi_\rho\rho_{v^n}^{\otimes n}\pi_\rho\big) \\ \times\mathbb{E}_{\mathcal{P}}\left[\mathbb{1}_{\mathcal{A}}\mathbb{1}_{\mathcal{V}}\right] \leq \delta_1, \end{aligned}$$

where the last inequality follows from the pinching argument, also provided in Lemma 1 (see Appendix B), with the identification $\mathcal{A} = \mathcal{B} = \mathcal{V}$, $p_A = p_V$, $B = A$, and the density operators correspondingly. With this choice, we obtain for any $\epsilon \in (0,1)$, $\mathbb{E}_{\mathcal{P}}\{T_{21}\} \leq \epsilon$, for all sufficiently large n and sufficiently small δ. Next, we provide the following proposition to bound the terms corresponding to T_{22} and T_{23} in an expected sense.

Proposition 5. *For any $\epsilon \in (0,1)$, and for all sufficiently small $\delta > 0$ and sufficiently large n, we have $\mathbb{E}_{\mathcal{P}}[T_{22} + T_{23}] \leq \epsilon$ if the following inequalities hold:*

$$\frac{2k}{n}\log q \leq 2\log q + I(V;Z)_\sigma - 2H(V) - \epsilon$$
$$\frac{(2k+l)}{n}\log q \leq 2\log q + I(V;Z)_\sigma - 2H(V) - \epsilon.$$

Proof. The proof is provided in Appendix A-A. □

We have therefore obtained three bounds $\frac{k}{n} > 1 - \frac{H(p_V)}{\log_2 q}$, $\frac{2k}{n} < 2 + \frac{I(V;Z)_\sigma - 2H(p_V)}{\log_2 q}$, $\frac{2k+l}{n} < 2 + \frac{I(V;Z)_\sigma - 2H(p_V)}{\log_2 q}$. A rate of $I(V;Z)_\sigma - \epsilon$ is achievable by choosing $\frac{k}{n} = 1 - \frac{H(p_V)}{\log_2 q} + \frac{\epsilon}{2}$, $\frac{l}{n} = \frac{I(V;Z)_\sigma - \epsilon \log_2 \sqrt{q}}{\log_2 q}$ thus completing the proof. □

VI. Decoding Sum over CQ-MAC

Throughout this section, the source alphabets $\mathcal{S} \triangleq \mathcal{S}_1 = \mathcal{S}_2 = \mathbb{F}_q$, and the receiver intends to reconstruct the sum $f(S_1, S_2) = S_1 \oplus_q S_2$ of the sources.

A. Proof of Proposition 2

Let $p_{V_1V_2X_1X_2} \in \mathscr{P}(\mathcal{N}_2, q)$ with associated collection $(\rho_{v_1v_2} : (v_1, v_2) \in \mathcal{V} \times \mathcal{V})$ of density operators where

$$\rho_{v_1v_2} \triangleq \sum_{x_1,x_2} p_{X_1|V_1}(x_1|v_1)p_{X_2|V_2}(x_2|v_2)\rho_{x_1x_2} \quad \text{and}$$
$$\rho_v \triangleq \sum_{v_1,v_2} p_{V_1V_2|V}(v_1, v_2|v)\rho_{v_1v_2}.$$

We now describe the coding scheme in terms of a specific code. It is instructive to revisit Sec. IV, wherein we specified the import of both encoders employing cosets of the the *same* linear code. In order to choose codewords of a desired empirical distribution p_{V_j}, we employ NCCs (as was done for the same reason in Sec. V). Following the same notation as in proof of Theorem 1, we now specify the random coding scheme.

Let $G_I \in \mathbb{F}_q^{k\times n}, G_{O/I} \in \mathbb{F}_q^{l\times n}, B_j \in \mathbb{F}_q^n : j \in [2]$ be mutually independent and uniformly distributed on their respective range spaces. Let $V_j^n(a, m_j) \triangleq aG_I \oplus m_jG_{O/I} \oplus B_j^n : (a, m_j) \in \mathbb{F}_q^{k+l}$ for $j \in [2]$ and $V^n(a, m) \triangleq aG_I \oplus mG_{O/I} \oplus B_1^n \oplus B_2^n : (a, m) \in \mathbb{F}_q^{k+l}$. For $j \in [2]$, let

$$S_j(m_j) \triangleq \begin{cases} \{a \in \mathcal{V}^k : V_j^n(a, m_j) \in T_\delta^n(p_{V_j})\}, \\ \qquad \text{if } \displaystyle\sum_{a\in\mathcal{V}^k} \mathbb{1}_{\{V_j^n(a,m_j)\in T_\delta^n(p_{V_j})\}} \geq 1 \\ \{0^k\} \qquad \text{otherwise,} \\ \qquad \text{i.e. } \displaystyle\sum_{a\in\mathcal{V}^k} \mathbb{1}_{\{V_j^n(a,m_j)\in T_\delta^n(p_{V_j})\}} = 0, \end{cases}$$

for each $m_j \in \mathcal{V}^l$. For $m_j \in \mathcal{V}^l$, a predetermined element $A_{j,m_j} \in S_j(m_j)$ is chosen. We let $\Theta_j(m_j) \triangleq |S_j(m_j)|$. For $m_j \in \mathcal{V}^l$, a predetermined $X_j^n(m_j) \in \mathcal{X}_j^n$ is chosen. As we shall see later, the choice of $X_j^n(m_j)$ is based on $V_j^n(A_{j,m_j}, m_j)$. We are thus led to the encoding rule.

Encoding Rule: On receiving message $(m_1, m_2) \in \mathcal{V}^l \times \mathcal{V}^l$, the quantum state $\rho_{m_1m_2} \triangleq \rho_{X_1^n(m_1)X_2^n(m_2)} \triangleq \otimes_{t=1}^n \rho_{X_{1t}(m_1)X_{2t}(m_2)}$ is (distributively) prepared.

Distribution of the Random Code: The distribution of the random code is completely specified through the distribution $\mathcal{P}(\cdot)$ of $G_I, G_{O/I}, B_1^n, B_2^n, (A_{1,m_1} : m_1 \in \mathbb{F}_q^l), (A_{2,m_2} : m_2 \in \mathbb{F}_q^l)$ and $(X_j^n(m_j) : m_j \in \mathcal{V}^l)$. We let

$$\mathcal{P}\begin{pmatrix} (A_{1,m_1} = a_{1,m_1} : m_1 \in \mathcal{V}^l), \\ (A_{2,m_2} = a_{2,m_2} : m_2 \in \mathcal{V}^l), \\ B_j^n = b_j^n : j \in [2], \\ G_I = g_I, G_{O/I} = g_{O/I}, \\ (X_1(m_1) = x_1^n(m_1) : m_1 \in \mathcal{V}^l), \\ (X_2(m_2) = x_2^n(m_2) : m_2 \in \mathcal{V}^l) \end{pmatrix} = \frac{1}{q^{kn+ln+2n}}$$
$$\times \left[\prod_{m_1} \frac{\mathbb{1}_{\{a_{1,m_1}\in s_1(m_1)\}}}{\Theta(m_1)} p_{X_1|V_1}^n(x_1^n(m_1)|v_1^n(a_{1,m_1}, m_1))\right]$$
$$\times \left[\prod_{m_2} \frac{\mathbb{1}_{\{a_{2,m_2}\in s_2(m_2)\}}}{\Theta(m_2)} p_{X_2|V_2}^n(x_2^n(m_2)|v_2^n(a_{2,m_2}, m_2))\right]. \tag{6}$$

Towards specifying a decoding POVM, we state the associated density operators modeling the quantum systems, their spectral decompositions and projectors. Let

$$\rho \triangleq \sum_{y\in\mathcal{Y}} s_Y(y) |h_y\rangle \langle h_y|,$$
$$\rho_{x_1x_2} \triangleq \sum_{y\in\mathcal{Y}} p_{Y|X_1X_2}(y|x_1, x_2) |e_{y|x_1x_2}\rangle \langle e_{y|x_1x_2}| : \underline{x} \in \underline{\mathcal{X}},$$
$$\rho_{v_1v_2} \triangleq \sum_{y\in\mathcal{Y}} q_{Y|V_1V_2}(y|v_1, v_2) |f_{y|v_1v_2}\rangle\langle f_{y|v_1v_2}| : \underline{v} \in \underline{\mathcal{V}},$$
$$\rho_v \triangleq \sum_{y\in\mathcal{Y}} r_{Y|V}(y|v) |g_{y|v}\rangle \langle g_{y|v}| : v \in \mathcal{V}.$$

Decoding POVM: Unlike a generic CQ-MAC decoder [3], which aims at decoding both the classical messages from the quantum state received, the decoder here is designed to decode only the sum of messages transmitted. For this, the decoder employs the nested coset code $(n, k, l, G_I, G_{O/I}, B^n)$, where $B^n = B_1^n \oplus B_2^n$. We define $V^n(a, m) \triangleq aG_I + mG_{O/I} + B^n$ to represent a generic codeword. We let $\Pi_{a,m} \triangleq \pi_{V^n(a,m)}\mathbb{1}_{\{V^n(a,m)\in T_\delta^{(n)}(p_V)\}}$, where p_V is as defined in the theorem statement. The decoder is provided with a sub-POVM $\mathbf{\Lambda} \triangleq \{\Lambda_m \triangleq \sum_{a\in\mathbb{F}_q^k} \Lambda_{a,m} : m \in \mathbb{F}_q^l\}$ where

$$\Lambda_{a,m} \triangleq \Bigg(\sum_{\hat{a}\in\mathbb{F}_q^k}\sum_{\hat{m}\in\mathbb{F}_q^l} \Gamma_{\hat{a},\hat{m}}\Bigg)^{-1/2} \Gamma_{a,m} \Bigg(\sum_{\hat{a}\in\mathbb{F}_q^k}\sum_{\hat{m}\in\mathbb{F}_q^l} \Gamma_{\hat{a},\hat{m}}\Bigg)^{-1/2},$$

$\Lambda_{-1} \triangleq I - \sum_{a\in\mathbb{F}_q^k}\sum_{m\in\mathbb{F}_q^l} \Lambda_{a,m}$ and $\Gamma_{a,m} \triangleq \pi_\rho \Pi_{(a,m)}\pi_\rho$. We note that

$$\pi_\rho \triangleq \sum_{y^n\in T_\delta^n(s_Y)} \bigotimes_{t=1}^n |h_{y_t}\rangle \langle h_{y_t}| \quad \text{and}$$

$$\pi_{v^n} \triangleq \sum_{y^n:(v^n,y^n)\in T_\delta^n(p_V r_{Y|V})} \bigotimes_{t=1}^{n} |g_{y_t|v_t}\rangle\langle g_{y_t|v_t}|,$$

denote the typical and conditional typical projectors (as stated in Definition 15.2.4 [17]) with respect to $\rho \triangleq \sum_{v\in\mathbb{F}_q} p_V(v)\rho_v$ and $(\rho_v : v \in \mathcal{V})$, respectively.

Error Analysis: We derive upper bounds on $\mathbb{E}_{\mathcal{P}}\{\bar{\xi}(c_{m\oplus})\}$. Our derivation will be similar to those adopted in proof of Thm. 1. Let us define event

$$\mathscr{E} \triangleq \left\{ \begin{pmatrix} V_1^n(A_{1.m_1}, m_1), X_1^n(m_1), \\ V_2^n(A_{2.m_2}, m_2), X_2^n(m_2), \\ V_1^n(A_{1.m_1}, m_1) \oplus V_2^n(A_{2.m_2}, m_2) \end{pmatrix} \in T_{8\delta}(p_{V_1X_1V_2X_2V}) \right\}. \quad (7)$$

We have

$$\mathbb{E}_{\mathcal{P}}\left\{\sum_{m_1,m_2} p_{M_1M_2}(m_1,m_2)\,\mathrm{Tr}([I-\Lambda_{m_1\oplus m_2}])\rho^{\otimes n}_{m_1m_2}\right\} \le \underbrace{\mathbb{E}_{\mathcal{P}}\left\{\sum_{m_1,m_2} p_{M_1M_2}(m_1,m_2)\mathrm{Tr}([I-\Lambda_{m_1\oplus m_2}])\rho^{\otimes n}_{m_1m_2}\mathbb{1}_{\mathscr{E}^c}\right\}}_{T_1} + \underbrace{\mathbb{E}_{\mathcal{P}}\left\{\sum_{m_1,m_2} p_{M_1M_2}(m_1,m_2)\mathrm{Tr}([I-\Lambda_{m_1\oplus m_2}])\rho^{\otimes n}_{m_1m_2}\mathbb{1}_{\mathscr{E}}\right\}}_{T_2}. \quad (8)$$

In regards to T_1, the sub-POVM nature of $\Lambda_{\mathcal{I}}$ and the fact that $\rho^{\otimes n}_{m_1,m_2}$ is a density operator enables us conclude $T_1 \le \mathbb{E}_{\mathcal{P}}\{\mathbb{1}_{\mathscr{E}^c}\}$. Furthermore, observe that $X_j(m_j)$ is distributed with PMF $p^n_{X_j|V_j}$ conditionally on $V_j^n(A_{j,m_j,m_j})$ (See (6)). In addition, $p_{V_1X_1V_2X_2} = p_{V_1X_1}p_{V_2X_2}$ implies that standard conditional typicality arguments yields

$$\mathbb{E}_{\mathcal{P}}\{\mathbb{1}_{\mathscr{E}^c}\} \le \mathbb{E}_{\mathcal{P}}\Big\{\sum_{m_1} p_{M_1}(m_1)\mathbb{1}_{\{\Theta_1(m_1)=0\}} + \sum_{m_2} p_{M_2}(m_2)\mathbb{1}_{\{\Theta_1(m_2)=0\}}\Big\} + \exp\{-n\epsilon\}, \quad (9)$$

for all sufficiently large n, and for all sufficiently small δ. In the above inequality, the second term on the RHS is an upper bound on the probability of the event $(X_1^n(m_1), X_2^n(m_2)) \notin T_\delta^n(p_{V_1X_1V_2X_2V}|v_1^n, v_2^n, v_1^n \oplus v_2^n)$ conditioned on $(V_1^n(A_{1.m_1}, m_1), V_2^n(A_{2.m_2}, m_2), V_1^n(A_{1.m_1}, m_1) \oplus V_2^n(A_{2.m_2}, m_2)) = (v_1^n, v_2^n, v_1^n \oplus v_2^n) \in T_\delta^n(p_{V_1V_2V})$, and the first term provides an upper bound on the complement of the latter event. An upper bound on T_1 therefore reduces to deriving an upper bound on the first term on the RHS of (9). This task - deriving an upper bound on the first term on the RHS of (9) - being a classical analysis, has been detailed in several earlier works, in particular [7, Proof of Thm. 2.5]. Following this, we have

$$\mathbb{E}_{\mathcal{P}}\Big\{\sum_{m_j} p_{M_j}(m_j)\mathbb{1}_{\{\Theta_j(m_j)=0\}}\Big\} \le \exp\left\{-n\left(\frac{k\log q}{n} - [\log q - H(V_j)]\right)\right\}, \quad (10)$$

thereby ensuring $T_1 \le 2\exp\{-n\delta\}$, if

$$\frac{k\log q}{n} \ge \max\{\log q - H(V_1), \log q - H(V_2)\} + \epsilon = \log q - \min\{H(V_1), H(V_2)\} + \epsilon, \quad (11)$$

for sufficiently large n and sufficiently small δ. We now analyze T_2. Applying the Hayashi-Nagaoka inequality, we have

$$T_2 \le \mathbb{E}_{\mathcal{P}}[T_{21} + T_{22} + T_{23}], \quad (12)$$

where

$$\begin{aligned} T_{21} &\triangleq 2\sum_{m_1}\sum_{m_2} p_{\underline{M}}(\underline{m})\,\mathrm{Tr}\Big([I - \Gamma_{A^{\oplus}_{\underline{m}},\underline{m}^{\oplus}}]\rho^{\otimes n}_{m_1m_2}]\Big)\mathbb{1}_{\mathscr{E}}, \\ T_{22} &\triangleq 4\sum_{m_1}\sum_{m_2}\sum_{\hat{a}\neq A^{\oplus}_{\underline{m}}} p_{\underline{M}}(\underline{m})\,\mathrm{Tr}\big(\Gamma_{\hat{a},\underline{m}^{\oplus}}\rho^{\otimes n}_{m_1m_2}\big)\mathbb{1}_{\mathscr{E}}, \\ T_{23} &\triangleq 4\sum_{m_1}\sum_{m_2}\sum_{\hat{a}\neq A^{\oplus}_{\underline{m}}}\sum_{\hat{m}\neq\underline{m}^{\oplus}} p_{\underline{M}}(\underline{m})\,\mathrm{Tr}\big(\Gamma_{\hat{a},\hat{m}}\rho^{\otimes n}_{m_1m_2}\big)\mathbb{1}_{\mathscr{E}}, \end{aligned} \quad (13)$$

and $A^{\oplus}_{\underline{m}} \triangleq A_{1,m_1} \oplus A_{2,m_2} \in \mathcal{V}^k$, $\underline{m}^{\oplus} \triangleq m_1 \oplus m_2 \in \mathcal{V}^l$. Note that (12) follows from an argument analogous to the one in (5). We now analyze T_{21}, T_{22} and T_{23}. We begin with T_{21}. For each m_1 and m_2, denote the events

$$\mathcal{J} \triangleq \Big\{ (V_1^n(A_{1.m_1}, m_1), X_1^n(m_1), V_2^n(A_{2.m_2}, m_2), X_2^n(m_2)) = (v_1^n, x_1^n, v_2, x_2) \in T_\delta(p_{V_1X_1V_2X_2})\Big\},$$

$$\mathcal{V} \triangleq \{V_j^n(a_j, m_j) = v_j^n : j \in [2]\},$$

$$\hat{\mathcal{V}} \triangleq \{V^n(\underline{a}^{\oplus}, m_1 \oplus m_2) = \underline{v}^n_{\oplus}\}, \mathcal{A} \triangleq \{A_{j,m_j} = a_j : j \in [2]\},$$

abbreviating $\underline{v}^n_{\oplus} = v_1^n \oplus v_2^n$, $\underline{a}^{\oplus} = a_1 \oplus a_2$. We have

$$\mathbb{E}_{\mathcal{P}}[T_{21}] = 1 - \sum_{\underline{m}}\sum_{a_1,a_2}\sum_{\substack{(\underline{v}^n,\underline{x})\in \\ T_\delta(p_{\underline{V}\,\underline{X}})}} p_{\underline{M}}(\underline{m})\,\mathrm{Tr}\Big(\pi_{v^n}\pi_\rho\rho^{\otimes n}_{x_1^n x_2^n}\pi_\rho\Big) \times \mathbb{E}_{\mathcal{P}}\left[\mathbb{1}_{\mathcal{J}}\mathbb{1}_{\mathcal{A}}\mathbb{1}_{\mathcal{V}}\mathbb{1}_{\hat{\mathcal{V}}}\right] \le \epsilon$$

for all sufficiently large n and sufficiently small δ, where the last inequality follows from the pinching argument, also provided in Lemma 1 (see Appendix B). Set $\mathcal{A} = \mathcal{V} = \mathbb{F}_q$, $\mathcal{B} = \mathcal{X}$, $p_{AB} = p_{V_1\oplus V_2,X}$ and the density operators correspondingly. The proposition below bounds the terms T_{22} and T_{23} as follows.

Proposition 6. *For any $\epsilon \in (0,1)$, and for all sufficiently small $\delta > 0$ and sufficiently large n, we have $\mathbb{E}_{\mathcal{P}}[T_{22} + T_{23}] \le \epsilon$ if the following inequalities hold:*

$$\frac{3k}{n}\log q \le 3\log q + I(V;Z)_\sigma - H(V_1,V_2) - H(V) - \epsilon,$$
$$\frac{(3k+l)}{n}\log q \le 3\log q + I(V;Z)_\sigma - H(V_1,V_2) - H(V) - \epsilon.$$

Proof. The proof is provided in Appendix A-B. □

This completes the proof of the proposition.

B. Proof of Theorem 2

We provide a brief outline of a proof. As stated in Sec. IV, we propose a 'separation based approach' with two modules - source and channel. The source coding module employs a (distributed) Körner Marton (KM) source code. Specifically, [4] guarantees the existence of a parity check matrix $h \in \mathbb{F}_q^{l\times n} = \mathcal{S}^{l\times n}$ and a decoder map $d : \mathbb{F}_q^l \to \mathcal{S}^n$ such that $\sum_{\underline{s}^n\in\underline{\mathcal{S}}^n} \mathbb{W}^n_{\underline{S}}(\underline{s}^n)\mathbb{1}_{\{d(hs_1^n\oplus_q hs_2^n)\neq s_1^n\oplus_q s_2^n\}} \leq \epsilon$, for any $\epsilon > 0$, and sufficiently large n, so long as $\frac{l\log_2 q}{n} \geq H(S_1\oplus_q S_2)+\epsilon$.

Both encoders of this KM source coding module employ one such parity check matrix $h \in \mathbb{F}_q^{l\times n}$. The decoder of the KM source code employs the corresponding decoder map d. KM source encoder j outputs $M_j^l = h(S_j^n)$. If the KM source decoder is provided $M_1^l \oplus_q M_2^l$, then it can reconstruct $S_1^n \oplus_q S_2^n$ with reliability at least $1-\epsilon$. The task of the CQ-MAC channel coding module is to make $M_1^l \oplus_q M_2^l$ available to the KM source decoder. Specifically, this channel coding module must communicate $M_1^l \oplus_q M_2^l \in \mathbb{F}_q^l$ within n channel uses. From the result of Proposition 6, we have a CQ-MAC receiver that can decode the sum of messages $M_1^l \oplus_q M_2^l \in \mathbb{F}_q^l$ having an arbitrary distribution $p_{M_1M_2}$, given the rate constraints provided hold. Concatenating the two source and channel coding schemes yields the desired result.

VII. Decoding arbitrary functions over CQ-MAC

A. Proof of Theorem 4

Let $p_{V_1V_2U_1U_2} \in \mathscr{P}(\mathcal{N}_4, q)$ be a PMF on $\mathcal{V}_1\times\mathcal{V}_2\times\mathcal{U}_1\times\mathcal{U}_2$ where $\mathcal{V}_1 = \mathcal{V}_2 = \mathbb{F}_q$. We begin by describing the coding scheme in terms of a specific class of codes. In order to choose codewords of a desired empirical distribution p_{V_j}, we again employ Nested Coset Codes (NCCs). Both the encoders $e_{V_j} : j \in [2]$ employ cosets of the *same* linear code. We then consider a 4-to-3 decoding over a 'perturbed' variant of CQ-MAC (as introduced by [13]), which we denote as $\mathcal{N}_4'$. Note that in the current problem, the decoder wishes to decode three messages simultaneously, and hence we use the framework of CQ joint typicality developed using the ideas of tilting, smoothing and augmentation [13]. This allows us to perform *intersection of non-commuting POVM elements* to construct a set of POVMs for $\mathcal{N}_4'$. Finally, towards bounding the average error probability for $\mathcal{N}_4$, we use an argument, similar to [13, Equation 5], which shows that the outputs of the channel $\mathcal{N}_4'$ and $\mathcal{N}_4$ are indistinguishable in trace norm. Thus, the POVMs constructed for $\mathcal{N}_4'$ can be used for $\mathcal{N}_4$ with an additional boundable error term.

We now define a 4-to-3 decoding over 'perturbed' CQ-MAC $\mathcal{N}_4'$ that consists of the following: (i) finite (augmented input) sets $(\mathcal{V}_j\times\mathcal{W}_{V_j})$, $(\mathcal{U}_j\times\mathcal{W}_{U_j}) : j \in [2]$, (ii) an (extended output) Hilbert space

$$\mathcal{H}_Z' = \bar{\mathcal{H}}_Z \bigoplus (\bar{\mathcal{H}}_Z\otimes\mathcal{W}_{V_1}) \bigoplus (\bar{\mathcal{H}}_Z\otimes\mathcal{W}_{V_2}) \bigoplus (\bar{\mathcal{H}}_Z\otimes\mathcal{W}_{U_1}) \bigoplus (\bar{\mathcal{H}}_Z\otimes\mathcal{W}_{U_2}),$$

where $\bar{\mathcal{H}}_Z = (\mathcal{H}_Z\otimes\mathbb{C}^2)$, and $\mathcal{W}_{V_j}$ and $\mathcal{W}_{U_j}$ denote both a finite alphabet as well as a Hilbert space with dimension given by $|\mathcal{W}| \triangleq |\mathcal{W}_{V_j}| = |\mathcal{W}_{U_j}|$, and $\bigoplus$ denotes external direct sum of Hilbert spaces, and (iii) a collection of density operators

$$\{\rho'_{\underline{vuw}} \in \mathcal{D}(\mathcal{H}_Z') : (\underline{v},\underline{u},\underline{w}_V,\underline{w}_U) \in \underline{\mathcal{V}}\times\underline{\mathcal{U}}\times\underline{\mathcal{W}}_V\times\underline{\mathcal{W}}_U\},$$

where $\underline{w} = (w_{V_1}, w_{V_2}, w_{U_1}, w_{U_2})$, $\underline{w}_V = (w_{V_1}, w_{V_2})$, and $\underline{\mathcal{W}}_V = \mathcal{W}_{V_1}\times\mathcal{W}_{V_2}$. Similarly $\underline{w}_U$ and $\underline{\mathcal{W}}_U$ are defined. Note that the states in the Hilbert spaces $\mathcal{W}_{V_j}$ and $\mathcal{W}_{U_j}$ are used as quantum registers to store classical values. Define $\rho'_{\underline{vuw}} \triangleq \mathcal{T}^{\mathrm{V}\underline{\mathrm{U}}}_{\underline{w};\tau}(\tilde{\rho}_{\underline{vu}})$, where $\tilde{\rho}_{\underline{vu}} \triangleq \rho_{\underline{vu}}\otimes|0\rangle\langle 0|^{\mathbb{C}^2}$, and $\mathcal{T}^{\mathrm{V}\underline{\mathrm{U}}}_{\underline{w};\tau}$ is a *tilting map* [13, Section 4] from $\bar{\mathcal{H}}_Z$ to $\mathcal{H}_Z'$ defined as:

$$\mathcal{T}^{\mathrm{V}\underline{\mathrm{U}}}_{\underline{w};\tau}(|z\rangle) \triangleq \frac{(|z\rangle \bigoplus_{i=1}^2 \tau\,|z, w_{V_i}\rangle \bigoplus_{j=1}^2 \tau\,|z, w_{U_j}\rangle}{\sqrt{1+4\tau^2}},$$

and τ will be chosen appropriately in the sequel.

Encoding: Consider two NCCs $(n, k, l, g_I, g_{O/I}, b_j^n, e_j)$ having the same parameters except with different bias vectors b_js and encoding maps e_js. For each $j \in [2]$ and $m_j \in \mathbb{F}_q^l$, let

$$\mathcal{A}_j(m_j) \triangleq \begin{cases} \{a_{m_j} : v_j^n(a_{m_j}, m_j) \in T_\delta^n(p_{V_j})\} & \text{if } \theta(m_j)\geq 1 \\ \{0^k\} & \text{otherwise,} \end{cases}$$

where $\theta(m_j) \triangleq \sum_{a\in\mathbb{F}_q^k} \mathbb{1}_{\{v_j^n(a,m_j)\in T_\delta^n(p_V)\}}$. For $m_j \in \mathbb{F}_q^l : j \in [2]$, a pre-determined element $a_{m_j} \in \mathcal{A}_j(m_j)$ is chosen and let $v_j^n(a_{m_j}, m_j) \triangleq a_{m_j}g_I \oplus m_j g_{O/I} \oplus b_j^n$ for $(a_{m_j}, m_j) \in \mathbb{F}_q^{k+l}$ for $j \in [2]$. Moreover, for each $j \in [2]$ and $m_{j+2} \in [q^{l_j}]$, construct a codeword $u_j^n(m_{j+2}) \in \mathcal{U}_j^n$. Similarly, for each $j \in [2]$, $m_j \in \mathbb{F}_q^l$ and $m_{j+2} \in [q_j^l]$, construct the codewords $w^n_{V_j}(m_j) \in \mathcal{W}^n_{V_j}$ and $w^n_{U_j}(m_{j+2}) \in \mathcal{W}^n_{U_j}$. For later convenience, we define an additional identical map $w_V^n(m) = w^n_{V_1}(m)$ for all $m \in \mathbb{F}_q^l$. On receiving the message $\underline{m} \in \mathbb{F}_q^l\times\mathbb{F}_q^l\times[q^{l_1}]\times[q^{l_2}]$, the quantum state $\rho'^{\otimes n}_{\underline{m}} \triangleq$

$$\rho'_{v_1^n(a_{m_1},m_1)w^n_{V_1}(m_1)v_2^n(a_{m_2},m_2)w^n_{V_2}(m_2)(u_1^n,w^n_{U_1})(m_3)(u_2^n,w^n_{U_2})(m_4)}$$

is (distributively) prepared. Towards specifying a decoding POVM's, we define the following associated density operators.

$$\rho \triangleq \sum_{\underline{v}^n,\underline{u}^n} p^n_{\underline{V}}(\underline{v}^n)p^n_{\underline{U}}(\underline{u}^n)\rho_{\underline{v}^n\underline{u}^n},$$

$$\rho_{v^n} \triangleq \sum_{\underline{v}^n,\underline{u}^n} p^n_{\underline{V}|V}(\underline{v}^n|v^n)p^n_{\underline{U}}(\underline{u}^n)\rho_{\underline{v}^n\underline{u}^n},$$

$$\rho_{u_i^n} \triangleq \sum_{\underline{v}^n u_j^n} p^n_{U_j}(u_j^n)\rho_{\underline{v}^n\underline{u}^n} : i\neq j, i,j\in[2],$$

$$\rho_{v^n u_i^n} \triangleq \sum_{\underline{v}^n,u_j^n} p^n_{\underline{V}|V}(\underline{v}^n|v^n)p^n_{U_j}(u_j^n)\rho_{\underline{v}^n\underline{u}^n} : i\neq j, i,j\in[2],$$

$$\rho_{v^n\underline{u}^n} \triangleq \sum_{\underline{v}^n} p^n_{\underline{V}|V}(\underline{v}^n|v^n)\rho_{\underline{v}^n\underline{u}^n},$$

where $p^n_{\underline{V}|V}(\underline{v}^n|v^n) \triangleq p^n_{\underline{V}}(\underline{v}^n)/p^n_V(v^n)\mathbb{1}_{\{v_1^n\oplus v_2^n = v^n\}}$.

Decoding: The decoder is designed to decode the sum of the messages $m^\oplus$ along with the individual messages m_3 and m_4 transmitted over the 'perturbed' 4-to-3 CQ-MAC $\mathcal{N}_4'$. To decode m_3 and m_4, we use the codebook used by the encoder, but to decode $m^\oplus$, we use the NCC $(n, k, l, g_I, g_{O/I}, b^n, e)$, with all the parameters same as the NCCs used in the encoding, except that $b^n = b_1^n \oplus b_2^n$, and e to be specified later.

Define $v^n(a,m) \triangleq ag_I + mg_{O/I} + b^n$, representing a generic codeword in a generic coset.

POVM construction: We start by defining the sub-POVMs for channel $\mathcal{N}$, subsequently we will construct the sub-POVMs for the 'perturbed' CQ-MAC $\mathcal{N}_4'$ using the process of *tilting* [13]. Let π_ρ be the typical projector for the state ρ. Furthermore, for $j \in [2]$ and for all jointly typical vectors $(v^n, \underline{u}^n) \in T_\delta^{(n)}(p_{V\underline{U}})$, let $\pi_{v^n}, \pi_{u_j^n}, \pi_{v^n u_j^n}, \pi_{\underline{u}^n}$ and $\pi_{v^n\underline{u}^n}$ be the conditional typical projector [17, Def. 15.2.4] with respect to the states $\rho_{v^n}, \rho_{u_i^n}, \rho_{v^n u_i^n}, \rho_{\underline{u}^n}$ and $\rho_{v^n\underline{u}^n}$, respectively.

Now, we define the following sub-POVMs in the Hilbert space $\mathcal{H}_Z^{\otimes n}$:

$$\Pi^{\mathrm{V}}_{v^n\underline{u}^n} \triangleq \pi_\rho\pi_{v^n}\pi_{v^n\underline{u}^n}\pi_{v^n}\pi_\rho,\ \Pi^{\mathrm{U_j}}_{v^n\underline{u}^n} \triangleq \pi_\rho\pi_{u_j^n}\pi_{v^n\underline{u}^n}\pi_{u_j^n}\pi_\rho,$$
$$\Pi^{\mathrm{VU_j}}_{v^n\underline{u}^n} \triangleq \pi_\rho\pi_{v^n u_j^n}\pi_{v^n\underline{u}^n}\pi_{v^n u_j^n}\pi_\rho,\ \Pi^{\underline{\mathrm{U}}}_{v^n\underline{u}^n} \triangleq \pi_\rho\pi_{\underline{u}^n}\pi_{v^n\underline{u}^n}\pi_{\underline{u}^n}\pi_\rho,$$
$$\Pi^{\mathrm{V\underline{U}}}_{v^n\underline{u}^n} \triangleq \pi_\rho\pi_{v^n\underline{u}^n}\pi_\rho : i \neq j, i, j \in [2]. \tag{14}$$

The following are well-known results regarding typical projectors and $(\underline{v}^n, \underline{u}^n) \in T_{8\delta}^{(n)}(p_{\underline{VU}})$.

Proposition 7. *For all $\epsilon > 0$, and $\delta \in (0,1)$ sufficiently small and n sufficiently large, and $i, j \in [2]$ with $i \neq j$ the following inequality holds for the sub-POVMs defined in (14).*

$$\mathrm{Tr}\left(\Pi^{\Phi}_{v^n\underline{u}^n}\rho_{\underline{v}^n\underline{u}^n}\right) \geq 1-\epsilon,$$
$$\textit{for all } \Phi \in \{\mathrm{V}, \mathrm{U_j}, \mathrm{VU_j}, \underline{\mathrm{U}}, \mathrm{V\underline{U}}\},$$
$$\mathrm{Tr}\left(\Pi^{\mathrm{V\underline{U}}}_{v^n\underline{u}^n}\rho\right) \leq 2^{-n(I(V,U_1,U_2;Z)_\sigma - \epsilon)},$$
$$\sum_{\underline{u}^n} p^n_{\underline{U}}(\underline{u}^n)\,\mathrm{Tr}\left(\Pi^{\mathrm{V}}_{v^n\underline{u}^n}\rho_{v^n}\right) \leq 2^{-n(I(U_1,U_2;Z|V)_\sigma - \epsilon)},$$
$$\sum_{v^n} p^n_V(v^n)\,\mathrm{Tr}\left(\Pi^{\underline{\mathrm{U}}}_{v^n\underline{u}^n}\rho_{\underline{u}^n}\right) \leq 2^{-n(I(V;Z|U_1,U_2)_\sigma - \epsilon)},$$
$$\sum_{u_i^n} p^n_{U_i}(u_i^n)\,\mathrm{Tr}\left(\Pi^{\mathrm{VU_j}}_{v^n\underline{u}^n}\rho_{v^n u_j^n}\right) \leq 2^{-n(I(U_i;Z|U_j,V)_\sigma - \epsilon)},$$
$$\sum_{v^n u_i^n} p^n_V(v^n)p^n_{U_i}(u_i^n)\,\mathrm{Tr}\left(\Pi^{\mathrm{U_j}}_{v^n\underline{u}^n}\rho_{u_j^n}\right) \leq 2^{-n(I(V,U_i;Z|U_j)_\sigma - \epsilon)}.$$

where the mutual information quantities are taken with respect to the classical-quantum state σ same as in Definition 12.

After constructing the sub-POVMs, we now construct the projectors. It is worth to observe that by the Gelfand-Naimark theorem [18], there exists orthogonal projectors $\bar{\Pi}^{\mathrm{V}}_{v^n\underline{u}^n}, \bar{\Pi}^{\mathrm{U_j}}_{v^n\underline{u}^n}, \bar{\Pi}^{\mathrm{VU_j}}_{v^n\underline{u}^n}, \bar{\Pi}^{\underline{\mathrm{U}}}_{v^n\underline{u}^n}$ and $\bar{\Pi}^{\mathrm{V\underline{U}}}_{v^n\underline{u}^n}$ in $\bar{\mathcal{H}}_Z^{\otimes n}$ that gives the same measurements statistics on the states $(\sigma \otimes |0\rangle\langle 0|^{\mathbb{C}^{2n}}) \in \mathcal{D}(\bar{\mathcal{H}}_Z^{\otimes n})$ that sub-POVMs defined in (14) give on the states $\sigma \in \mathcal{D}(\mathcal{H}_Z^{\otimes n})$. To summarize upto this point, we have constructed the projectors in $\bar{\mathcal{H}}_Z^{\otimes n}$ for the channel $\mathcal{N}_4$ using the sub-POVMs defined in (14), and we are now equipped to construct the sub-POVMs for $\mathcal{N}_4'$. Let us define $\bar{\Omega}^{\mathrm{V}}_{v^n\underline{u}^n}$ as the orthogonal complement of the support of $\bar{\Pi}^{\mathrm{V}}_{v^n\underline{u}^n}$. Analogously, we define $\bar{\Omega}^{\mathrm{U_j}}_{v^n\underline{u}^n}, \bar{\Omega}^{\mathrm{VU_j}}_{v^n\underline{u}^n}, \bar{\Omega}^{\underline{\mathrm{U}}}_{v^n\underline{u}^n}$, and $\bar{\Omega}^{\mathrm{V\underline{U}}}_{v^n\underline{u}^n}$. Then we define the corresponding tilted subspace in $\mathcal{H}_Z'^{\otimes n}$ as: $\Omega^{\mathrm{V}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n} \triangleq \mathcal{T}^{\mathrm{V}}_{w_V^n;\tau}(\bar{\Omega}^{\mathrm{V}}_{v^n\underline{u}^n})$, for all $w_V^n \in \mathcal{W}_{V_1}^n$. Likewise, define $\Omega^{\mathrm{U_j}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n}, \Omega^{\mathrm{VU_j}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n}$ and $\Omega^{\underline{\mathrm{U}}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n}$. Also, let us define a new subspace $\widehat{\Omega}_{v^n\underline{u}^n w_V^n \underline{w}_U^n}$, which is analogous to the 'union' of 'complement' of orthogonal projectors corresponding to the sub-POVMs defined in (14):

$$\widehat{\Omega}_{v^n\underline{u}^n w_V^n \underline{w}_U^n} \triangleq \bar{\Omega}^{\mathrm{V\underline{U}}}_{v^n\underline{u}^n} \bigoplus \Omega^{\mathrm{V}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n} \bigoplus_{j\in[2]} \Omega^{\mathrm{U_j}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n}$$
$$\bigoplus_{j\in[2]} \Omega^{\mathrm{VU_j}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n} \bigoplus \Omega^{\underline{\mathrm{U}}}_{v^n\underline{u}^n w_V^n \underline{w}_U^n}. \tag{15}$$

Consider a collection of orthogonal projectors $\widehat{\Pi}'_{v^n\underline{u}^n w_V^n \underline{w}_U^n}$ in $\mathcal{H}_Z'^{\otimes n}$ projecting onto $\widehat{\Omega}_{v^n\underline{u}^n w_V^n \underline{w}_U^n}$, and the orthogonal projector $\widetilde{\Pi}'$ also in $\mathcal{H}_Z'^{\otimes n}$ projecting onto $\bar{\mathcal{H}}_Z^{\otimes n}$.

Subsequently, define the sub-POVMs in $\mathcal{H}_Z'^{\otimes n}$ for channel $\mathcal{N}_4'$ as follows:

$$\gamma_{v^n\underline{u}^n w_V^n \underline{w}_U^n} \triangleq \left(I - \widehat{\Pi}'_{v^n\underline{u}^n w_V^n \underline{w}_U^n}\right)\widetilde{\Pi}'\left(I - \widehat{\Pi}'_{v^n\underline{u}^n w_V^n \underline{w}_U^n}\right). \tag{16}$$

The decoder now uses the sub-POVMs $\gamma_{v^n\underline{u}^n w_V^n \underline{w}_U^n}$ as defined above to construct a *square root measurement* [17], [18] to decode the messages. We define following operators,

$$\lambda_{(a,m),m_3,m_4} \triangleq \left(\sum_{\hat{a},\hat{m}}\sum_{\hat{m}_3,\hat{m}_4}\gamma_{(\hat{a},\hat{m}),\hat{m}_3,\hat{m}_4}\right)^{-1/2}\gamma_{(a,m),m_3,m_4}\left(\sum_{\hat{a},\hat{m}}\sum_{\hat{m}_3,\hat{m}_4}\gamma_{(\hat{a},\hat{m}),\hat{m}_3,\hat{m}_4}\right)^{-1/2}, \tag{17}$$

where $\gamma_{(a,m),m_3,m_4}$ is an abbreviation for $\gamma_{v^n(a,m)u_1^n(m_3)u_2^n(m_4)w_V^n(m)w_{U_1}^n(m_3)w_{U_2}^n(m_4)}$, and we let the perturbation w_V used by the decoder is identical to that of either user 1 or user 2, and without loss of generality $w_V = w_{V_1}$, as mentioned earlier (in the discussion on encoding).

Distribution of Random Code: The distribution of the random code is completely specified through the distribution $\mathcal{P}(\cdot)$ of $G_I, G_{O/I}, B_j^n, A_{m_j},, W^n_{V_j}(m_j), U_j^n(m_{j+2}), W^n_{U_j}(m_{j+2}) : j \in [2]$. We let

$$\mathcal{P}\begin{pmatrix} G_I = g_I, G_{O/I} = g_{O/I}, B_j^n = b_j^n, A_{m_j} = a_{m_j}, \\ U_j^n(m_{j+2}) = u_j^n(m_{j+2}), \\ W^n_{V_j}(m_j) = w^n_{v_j}(m_j), W^n_{U_j}(m_{j+2}) = w^n_{u_j}(m_{j+2}) \\ : j \in [2]\ ,\ \underline{m} \in \mathbb{F}_q^l \times \mathbb{F}_q^l \times [q^{l_1}] \times [q^{l_2}] \end{pmatrix}$$
$$= \prod_{j\in[2]} \frac{\mathbb{1}_{\{a_{m_j}\in\mathcal{A}_j(m_j)\}}}{\theta(m_j)|\mathcal{W}_{V_j}||\mathcal{W}_{U_j}|} p^n_{U_j}(u_j^n(m_{j+2}))\frac{1}{q^{kn+ln+2n}}. \tag{18}$$

Also define $A^{\oplus} \triangleq A_{m_1} \oplus A_{m_2}$.

Error Analysis: We derive an upper bound on $\bar{\xi}(c^{(n)}, \mathcal{N}_4')$, by averaging over the above ensemble. Using the encoding and decoding rule stated above, the average probability of error of the code is given as,

$$\bar{\xi}(c^{(n)}, \mathcal{N}_4') = \sum_{\underline{m}} p_{\underline{M}}(\underline{m})\mathrm{Tr}\left\{\left(I - \sum_a \lambda_{(a,m^{\oplus}),m_3,m_4}\right)\rho'^{\otimes n}_{\underline{m}}\right\}$$
$$\leq \sum_{\underline{m}} p_{\underline{M}}(\underline{m})\mathrm{Tr}\left\{\left(I - \lambda_{(a^{\oplus},m^{\oplus}),m_3,m_4}\right)\rho'^{\otimes n}_{\underline{m}}\right\},$$

where $a^{\oplus} \triangleq a_{m_1} \oplus a_{m_2}$, and $\rho'^{\otimes n}_{\underline{m}}$ is as defined above (in the discussion on encoding). Now consider the event,

$$\mathscr{E} \triangleq \left\{ \begin{pmatrix} V_1^n(A_{m_1}, m_1), V_2^n(A_{m_2}, m_2), \\ U_1^n(m_3), U_2^n(m_4), V^n(A^{\oplus}, m^{\oplus}) \end{pmatrix} \in T_{8\delta}^{(n)}(p_{\underline{V}\underline{U}V}) \right\},$$

where we recall that $V^n(A^{\oplus}, m^{\oplus}) = A^{\oplus} G_I \oplus m^{\oplus} G_{O/I} \oplus B^n = V_1^n(A_{m_1}, m_1) \oplus V_2^n(A_{m_2}, m_2)$. Then,

$$\mathbb{E}_{\mathcal{P}}\left\{\bar{\xi}(c^{(n)}, \mathcal{N}_4')\right\} = \mathbb{E}_{\mathcal{P}}\left\{\bar{\xi}(c^{(n)}, \mathcal{N}_4')\mathbb{1}_{\mathscr{E}^c} + \bar{\xi}(c^{(n)}, \mathcal{N}_4')\mathbb{1}_{\mathscr{E}}\right\}$$
$$\leq \underbrace{\mathbb{E}_{\mathcal{P}}\left\{\mathbb{1}_{\mathscr{E}^c}\right\}}_{T_1} + \underbrace{\mathbb{E}_{\mathcal{P}}\left\{\bar{\xi}(c^{(n)}, \mathcal{N}_4')\mathbb{1}_{\mathscr{E}}\right\}}_{T_2}.$$

As observed in the earlier section, for all $\epsilon > 0$, and for all sufficiently large n and sufficiently small $\delta > 0$, we have $T_1 \leq \epsilon$, if

$$\frac{k}{n}\log q \geq \log q - \min\{H(V_1), H(V_2)\} + \delta.$$

To bound the error probability corresponding to T_2, we apply the Hayashi-Nagaoka inequality and obtain

$$T_2 \leq \mathbb{E}_{\mathcal{P}}\Big[2\, T_{20} + 4$$
$$\times \underbrace{\Big\{T_{2V} + \sum_{j\in[2]} T_{2U_j} + \sum_{j\in[2]} T_{2VU_j} + T_{2\underline{U}} + T_{2V\underline{U}}\Big\}}_{T_{21}}\Big],$$

where,

$$T_{20} \triangleq 1 - \sum_{\underline{m}} p_{\underline{M}}(\underline{m}) \operatorname{Tr}\left(\Gamma_{(A^{\oplus},m^{\oplus}),m_3,m_4}\rho'^{\otimes n}_{\underline{m}}\right)\mathbb{1}_{\mathscr{E}},$$

$$T_{2U_1} \triangleq \sum_{\underline{m}} \sum_{\hat{m}_3 \neq m_3} p_{\underline{M}}(\underline{m}) \operatorname{Tr}\left(\Gamma_{(A^{\oplus},m^{\oplus}),\hat{m}_3,m_4}\rho'^{\otimes n}_{\underline{m}}\right)\mathbb{1}_{\mathscr{E}},$$

$$T_{2V} \triangleq \sum_{\underline{m}} \sum_{\hat{a}} \sum_{\hat{m} \neq m^{\oplus}} p_{\underline{M}}(\underline{m}) \operatorname{Tr}\left(\Gamma_{(\hat{a},\hat{m}),m_3,m_4}\rho'^{\otimes n}_{\underline{m}}\right)\mathbb{1}_{\mathscr{E}},$$

$$T_{2VU_1} \triangleq \sum_{\underline{m}} \sum_{\hat{a}} \sum_{\substack{\hat{m} \neq m^{\oplus} \\ \hat{m}_3 \neq m_3}} p_{\underline{M}}(\underline{m}) \operatorname{Tr}\left(\Gamma_{(\hat{a},\hat{m}),\hat{m}_3,m_4}\rho'^{\otimes n}_{\underline{m}}\right)\mathbb{1}_{\mathscr{E}},$$

$$T_{2\underline{U}} \triangleq \sum_{\underline{m}} \sum_{\substack{\hat{m}_3 \neq m_3 \\ \hat{m}_4 \neq m_4}} p_{\underline{M}}(\underline{m}) \operatorname{Tr}\left(\Gamma_{(A^{\oplus},m^{\oplus}),\hat{m}_3,\hat{m}_4}\rho'^{\otimes n}_{\underline{m}}\right)\mathbb{1}_{\mathscr{E}},$$

$$T_{2V\underline{U}} \triangleq \sum_{\underline{m}} \sum_{\hat{a}} \sum_{\substack{\hat{m} \neq m^{\oplus} \\ \hat{m}_3 \neq m_3 \\ \hat{m}_4 \neq m_4}} p_{\underline{M}}(\underline{m}) \operatorname{Tr}\left(\Gamma_{(\hat{a},\hat{m}),\hat{m}_3,\hat{m}_4}\rho'^{\otimes n}_{\underline{m}}\right)\mathbb{1}_{\mathscr{E}},$$

$\Gamma_{(A^{\oplus},m^{\oplus}),\hat{m}_3,\hat{m}_4}$ is a randomized version of $\gamma_{(a^{\oplus},m^{\oplus}),\hat{m}_3,\hat{m}_4}$. Similary we can define T_{2U_2} and T_{2VU_2}. Below, we provide the following propositions that summarize all the rate constraints obtained from bounding these error terms.

Proposition 8. *For any $\epsilon \in (0,1)$, and for all sufficiently small $\delta, \tau > 0$ and sufficiently large n, we have $\mathbb{E}_{\mathcal{P}}[T_{20}] \leq \epsilon$.*

Proof. The proof is provided in Appendix A-C. □

Proposition 9. *For any $\epsilon \in (0,1)$, and for all sufficiently small $\delta, \tau > 0$ and sufficiently large n, we have $\mathbb{E}_{\mathcal{P}}[T_{21}] \leq \epsilon$ if the following inequalities hold:*

$$\frac{2k+l_j}{n}\log q \leq 2\log q + I(U_j;Z|V,U_i)_\sigma - H(V_1,V_2) - \epsilon,$$
$$\frac{2k+l_1+l_2}{n}\log q \leq 2\log q + I(U_1,U_2;Z|V)_\sigma - H(V_1,V_2) - \epsilon,$$
$$\frac{3k+l}{n}\log q \leq 3\log q + I(V;Z|U_1,U_2)_\sigma - H_{V_1,V_2} - \epsilon,$$
$$\frac{3k+l+l_j}{n}\log q \leq 3\log q + I(V,U_j;Z|U_i)_\sigma - H_{V_1,V_2} - \epsilon,$$
$$\frac{3k+l+l_1+l_2}{n}\log q \leq 3\log q + I(V,U_1,U_2;Z)_\sigma - H_{V_1,V_2} - \epsilon,$$

where $i,j \in [2], i \neq j, H_{V_1,V_2} = H(V_1,V_2) + H(V)$, and the mutual information quantities are taken with respect to the classical-quantum state σ same as in Definition 12.

Proof. The proof is provided in Appendix A-D. □

Now, we need to bound average error probability for $\mathcal{N}_4$. For any $\epsilon \in (0,1)$, if we let $\tau = \epsilon^{1/4}$, and use the following argument, $\left\|\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n} - \tilde{\rho}_{\underline{v}^n\underline{u}^n}\right\|_1 \leq 4\tau$ (similar to the provided in [13, Equation 5]) and the trace inequality $\operatorname{Tr}\{\Delta\rho\} \leq \operatorname{Tr}\{\Delta\sigma\} + \frac{1}{2}\|\rho - \sigma\|_1$, where $0 \leq \Delta, \rho, \sigma \leq I$, then for all sufficiently large n, we have $\bar{\xi}(c^{(n)}, \mathcal{N}_4) \leq \bar{\xi}(c^{(n)}, \mathcal{N}_4') + 2\epsilon^{1/4}$. In other words, the average decoding error for CQ-MAC $\mathcal{N}_4$ is bounded from above by the average decoding error for CQ-MAC $\mathcal{N}_4'$ with an additional error of $2\epsilon^{1/4}$ for the same rate constraints and decoding strategy used for $\mathcal{N}_4'$. This concludes the proof of Theorem 4.

B. Proof of Theorem 5

We again use the approach of source channel separation with two modules. Consider a source given by $(\mathbb{W}_{S_1,S_2}, f)$. For the source part, the theorem requires showing the above source can be compressed to rates (R, R_1, R_2) that belongs to $\mathscr{R}_s(\mathbb{W}_{S_1,S_2}, f, q)$. Ahlswede-Han [9] source coding scheme achieves this. This forms the source coding module. This module produces messages M_{j1}, M_{j2} at encoder $j \in [2]$, at rates R_j, R, respectively. As for the channel part, its task is to recover $(M_{11}, M_{21}, M_{12} \oplus M_{22})$ reliably, and to provide it to the source decoder. For this, we employ the result from Theorem 4, which shows that if the triple (R, R_1, R_2) belongs to $\mathscr{R}_c(\mathcal{N}_2, q)$, then for any arbitrary distribution of $p_{M_{11}M_{12}M_{21}M_{22}}$, such a recovery is guaranteed. This completes the proof of the theorem.

VIII. Conclusion

We considered the task of communicating a bivariate function of two classical sources over a CQ-MAC. We proposed a coding scheme based on algebraic structured codes, in particular, nested coset codes, and provided a set of sufficient conditions that allow the receiver of the CQ-MAC to reconstruct an addition function, with respect to a prime field, without necessarily recovering the individual sources themselves. As the natural next step, we considered the task of computing any generic function. Using the coding scheme based on a classical superposition of algebraic structured codes and unstructured codes, and the idea of embedding functions on a prime field, we provided a new set of sufficient conditions for communicating any arbitrary function over a generic CQ-MAC. We provided these conditions in terms of single-letter quantum information-theoretic quantities. We also identified examples, establishing the efficacy of our approach.

Our work opens further directions for exploration such developing an outer bound to the performance limit, and formulating the problem and characterizing a performance limit in the one-shot case. One may extend the proposed method to the case with entanglement assistance. Another questions with potential wide-reaching implications is how to extend the results to a *fully* quantum-quantum (QQ) setup with quantum sources. In section III-C, we have been able to show sufficient conditions required for reconstructing sum of classical sources over a QQ-MAC. It is of interest to develop the codes for reconstructing a CPTP map of quantum sources over a QQ-MAC.

Acknowledgement: We thank the anonymous reviewers for their comments that greatly helped in preparing a better manuscript.

Appendix A
Proof of Propositions

A. *Proof of Proposition 5*

We begin by denoting the event

$$\mathcal{J} \triangleq \left\{ \begin{array}{c} \Theta(m) \geq 1, V^n(\hat{a},\hat{m}) = \hat{x}^n \\ A_m = d, V^n(d,m) = x^n \end{array} \right\} \subseteq \mathcal{K} \triangleq \left\{ \begin{array}{c} V^n(\hat{a},\hat{m}) = \hat{x}^n \\ V^n(d,m) = x^n \end{array} \right\}. \tag{19}$$

Considering $\mathbb{E}_{\mathcal{P}}[T_{22}]$, we perform the following steps.

$$\begin{aligned}\mathbb{E}_{\mathcal{P}}[T_{22}] &= \sum_{\hat{a}\in\mathcal{V}^k} \mathbb{E}_{\mathcal{P}}[\mathrm{tr}(\Gamma_{\hat{a},m}\rho_m^{\otimes n})\mathbb{1}_{\{\theta(m)\geq 1\}}\mathbb{1}_{\{\hat{a}\neq A_m\}}] \\ &= \sum_{d\in\mathcal{V}^k}\sum_{\hat{a}\in\mathcal{V}^k}\sum_{x^n\in T_\delta^n(p_V)}\sum_{\hat{x}^n\in\mathcal{V}^n} \mathbb{E}\left[\mathrm{tr}(\Gamma_{\hat{a},m}\rho_m^{\otimes n})\mathbb{1}_{\{\hat{a}\neq d\}}\mathbb{1}_{\mathcal{J}}\right] \\ &= \sum_{d\in\mathcal{V}^k}\sum_{\hat{a}\neq d}\sum_{x^n\in T_\delta^n(p_V)}\sum_{\hat{x}^n\in\mathcal{V}^n} \mathbb{E}\left[\mathrm{tr}(\Gamma_{\hat{a},m}\rho_m^{\otimes n})\mathbb{1}_{\mathcal{J}}\right],\end{aligned}$$

where the restriction of the summation x^n to $T_\delta^n(p_V)$ is valid since $|S(m)| > 1$ forces the choice $A_m \in S(m)$ such that $V^n(A_m,m) \in T_\delta^n(p_V)$. Going further, we have

$$\begin{aligned}\mathbb{E}_{\mathcal{P}}[T_{22}] &= \sum_{\substack{d,\hat{a}\in\mathcal{V}^k\\ \hat{a}\neq d}}\sum_{x^n\in T_\delta^n(p_V)}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathbb{E}\left[\mathrm{tr}(\pi_\rho\pi_{\hat{x}^n}\pi_\rho\rho_{x^n}^{\otimes n})\mathbb{1}_{\mathcal{J}}\right] \\ &= \sum_{d,\hat{a}:\hat{a}\neq d}\sum_{x^n\in T_\delta^n(p_V)}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_\rho\pi_{\hat{x}^n}\pi_\rho\rho_{x^n}^{\otimes n})\mathcal{P}(\mathcal{J}) \\ &\overset{(a)}{\leq} \sum_{d,\hat{a}:\hat{a}\neq d}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_{\hat{x}^n}\pi_\rho)\mathcal{P}(\mathcal{J})2^{-n[S(\rho)-H(p_V)+\delta_1]} \\ &\overset{(b)}{\leq} \sum_{d,\hat{a}:\hat{a}\neq d}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_{\hat{x}^n}\pi_\rho)\mathcal{P}(\mathcal{K})2^{-n[S(\rho)-H(p_V)+\delta_1]} \\ &\overset{(c)}{=} \sum_{d,\hat{a}:\hat{a}\neq d}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_{\hat{x}^n}\pi_\rho)\frac{1}{q^{2n}}2^{-n[S(\rho)-H(p_V)+\delta_1]} \\ &\overset{(d)}{\leq} 2^{-n\left[I(V;Z)_\sigma+\delta_1-2H(p_V)-\frac{2k}{n}\log q+2\log q\right]},\end{aligned} \tag{20}$$

where the restriction of the summation $\hat{x}^n$ to $T_\delta^n(p_V)$ follows from the fact that $\pi_{\hat{x}^n}$ is the zero projector if $\hat{x}^n \notin T_\delta^n(p_V)$, (a) follows from the operator inequality $\sum_{x^n\in T_\delta(p_V)}\pi_\rho\rho_{x^n}\pi_\rho \leq 2^{n(H(p_V)+\delta_1(\delta)}\pi_\rho\rho^{\otimes n}\pi_\rho \leq 2^{n(H(p_V)+\delta_1(\delta)-S(\rho))}\pi_\rho$ found in [17, Eqn. 20.34, 15.20], (b) follows from Eqn. 19, (c) follows from pairwise independence of the distinct codewords, and (d) follows from $\pi_\rho \leq I$ and [17, Eqn. 15.77] and $\delta_1(\delta) \searrow 0$ as $\delta \searrow 0$. We now derive an upper bound on $\mathbb{E}_{\mathcal{P}}[T_{23}]$. We have

$$\begin{aligned}\mathbb{E}_{\mathcal{P}}[T_{23}] &= \sum_{d,\hat{a}\in\mathcal{V}^k}\sum_{\hat{m}\neq m}\sum_{\substack{x^n,\hat{x}^n\in\\ T_\delta^n(p_V)}} \mathbb{E}\left[\mathrm{tr}(\pi_\rho\Pi_{\hat{a},\hat{m}}\pi_\rho\rho_{A_m,m}^{\otimes n})\mathbb{1}_{\mathcal{J}}\right] \\ &= \sum_{d,\hat{a}\in\mathcal{V}^k}\sum_{\hat{m}\neq m}\sum_{x^n,\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_{\hat{x}^n}\pi_\rho\rho_{x^n}^{\otimes n}\pi_\rho)\mathcal{P}(\mathcal{J}) \\ &\leq \sum_{d,\hat{a}\in\mathcal{V}^k}\sum_{\hat{m}\neq m}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_{\hat{x}^n}\pi_\rho)\mathcal{P}(\mathcal{J})2^{-n[S(\rho)-H(p_V)+\delta_1]} \\ &\leq \sum_{d,\hat{a}\in\mathcal{V}^k}\sum_{\hat{m}\neq m}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_{\hat{x}^n}\pi_\rho)\mathcal{P}(\mathcal{K})2^{-n[S(\rho)-H(p_V)+\delta_1]} \\ &= \sum_{d,\hat{a}\in\mathcal{V}^k}\sum_{\hat{m}\neq m}\sum_{\hat{x}^n\in T_\delta^n(p_V)} \mathrm{tr}(\pi_{\hat{x}^n}\pi_\rho)\frac{1}{q^{2n}}2^{-n[S(\rho)-H(p_V)+\delta_1]} \\ &\leq 2^{-n\left[I(V;Z)_\sigma+2\log_2 q-2H(p_V)-\frac{2k+l}{n}\log_2 q+\delta_1\right]},\end{aligned}$$

where the inequalities above use similar reasoning as in bounding the above term corresponding to T_{22}.

B. *Proof of Proposition 6*

We begin by defining the following events:

$$\mathcal{J} \triangleq \Big\{ \big(V_1^n(A_{1.m_1},m_1), X_1^n(m_1), V_2^n(A_{2.m_2},m_2), X_2^n(m_2)\big) = (v_1^n, x_1^n, v_2, x_2) \in T_{8\delta}(p_{V_1X_1V_2X_2}) \Big\},$$

$$\mathcal{V} \triangleq \{V_j^n(a_j,m_j) = v_j^n : j \in [2]\},$$

$$\hat{\mathcal{V}} \triangleq \{V^n(\hat{a}, m_1 \oplus m_2) = \hat{v}^n\},\ \ \mathcal{A} \triangleq \{A_{j,m_j} = a_j : j \in [2]\},$$

This gives,

$$\begin{aligned}\mathbb{E}_{\mathcal{P}}[T_{22}] &= \mathbb{E}_{\mathcal{P}}\Bigg[4\sum_{\underline{m}}\sum_{a_1,a_2}\sum_{\hat{a}\neq\underline{a}^\oplus}\sum_{\substack{(\underline{v}^n,\underline{x})\in\\ T_{8\delta}(p_{\underline{V}\underline{X}})}} p_{\underline{M}}(\underline{m}) \\ &\qquad\qquad \times \mathrm{Tr}\big(\Gamma_{\hat{a},\underline{m}^\oplus}\rho_{m_1m_2}^{\otimes n}\big)\mathbb{1}_{\mathcal{J}}\mathbb{1}_{\mathcal{A}}\Bigg], \\ &\overset{(a)}{=} 4\sum_{\underline{m}}\sum_{a_1,a_2}\sum_{\hat{a}\neq\underline{a}^\oplus}\sum_{\substack{(\underline{v}^n,\underline{x})\in\\ T_{8\delta}(p_{\underline{V}\underline{X}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m})\,\mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho_{x_1^nx_2^n}^{\otimes n}\pi_\rho\Big) \\ &\qquad\qquad \times \mathbb{E}_{\mathcal{P}}\left\{\mathbb{1}_{\mathcal{J}}\mathbb{1}_{\mathcal{A}}\mathbb{1}_{\hat{\mathcal{V}}}\right\}, \\ &\overset{(b)}{\leq} 4\sum_{\underline{m}}\sum_{a_1,a_2}\sum_{\hat{a}\neq\underline{a}^\oplus}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\underline{x}^n\in\underline{\mathcal{X}}^n}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m})\mathcal{P}(\mathcal{V},\mathcal{A},\hat{\mathcal{V}}) \\ &\qquad\qquad \times \left[\prod_{j=1}^{2} p_{X_j|V_j}(x_j^n|v_j^n)\right]\mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho_{x_1^nx_2^n}^{\otimes n}\pi_\rho\Big), \\ &\overset{(c)}{=} 4\sum_{\underline{m}}\sum_{a_1,a_2}\sum_{\hat{a}\neq\underline{a}^\oplus}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m})\mathcal{P}(\mathcal{V},\mathcal{A},\hat{\mathcal{V}}) \\ &\qquad\qquad \times \mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho_{v_1^nv_2^n}^{\otimes n}\pi_\rho\Big),\end{aligned}$$

$$\stackrel{(d)}{\leq} 4\sum_{\underline{m}}\sum_{a_1,a_2}\sum_{\hat{a}\neq \underline{a}^{\oplus}}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m})\mathcal{P}(\mathcal{V},\hat{\mathcal{V}}) \times \mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho^{\otimes n}_{v_1^n v_2^n}\pi_\rho\Big)$$
$$\leq 4\sum_{\underline{m}}\sum_{a_1,a_2}\sum_{\hat{a}\neq \underline{a}^{\oplus}}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho^{\otimes n}_{v_1^n v_2^n}\pi_\rho\Big)$$
$$\stackrel{(e)}{\leq} 4\sum_{\substack{\underline{m},\\ a_1,a_2}}\sum_{\hat{a}}\sum_{\hat{v}^n\in T_{8\delta}(V)} p_{\underline{M}}(\underline{m})\,\mathrm{Tr}(\pi_{\hat{v}^n}\pi_\rho)\frac{1}{q^{3n}} \times 2^{-n(S(\rho)-H(V_1,V_2)-\delta_1)}$$
$$\stackrel{(f)}{\leq} 4\sum_{\substack{\underline{m},\\ a_1,a_2}}\sum_{\hat{a}}\frac{p_{\underline{M}}(\underline{m})}{q^{3n}}2^{-n\left[S(\rho)-H(V_1,V_2)-\delta_1-\sum_v p_V(v)S(\rho_v)-H(V)\right]}$$
$$\stackrel{(g)}{\leq} 4\cdot\exp\left\{\begin{array}{l}-n\Big[3\log q - H(V_1,V_2)-\frac{3k}{n}\log q-\delta_1\\ \quad -\big(\sum_v p_V(v)S(\rho_v)+H(V)-S(\rho)\big)\Big]\end{array}\right\}, \tag{21}$$

and (a) follows from a summing over possible choices for $V^n(\hat{a}, m_1\oplus m_2)$, (b) follows from evaluating the expectation, enlarging the summation range of x_1^n, x_2^n and substituting the distribution of the random code, (c) follows from the definitions of $\rho_{v_1v_2} : \underline{v} \in \underline{\mathcal{V}}$, (d) follows as an upper bound since one of the events has been enlarged, (e) follows from [27, Lemma N.0.21c] and the operator inequality $\sum_{x^n\in T_\delta(p_V)}\pi_\rho\rho_{x^n}\pi_\rho \leq 2^{n(H(p_V)+\delta_1(\delta))}\pi_\rho\rho^{\otimes n}\pi_\rho \leq 2^{n(H(p_V)+\delta_1(\delta)-S(\rho))}\pi_\rho$ found in [17, Eqn. 20.34, 15.20], and from the definition of $\pi_{\hat{v}^n}$ which is the 0 projector if $\hat{v}^n$ is not typical with respect to p_V, (f) follows from $\pi_\rho \leq I$ and [17, Eqn. 15.77], and finally (g) follows by collating all the bounds.

We now analyze T_{23}.

$$\mathbb{E}_{\mathcal{P}}[T_{23}] = \mathbb{E}_{\mathcal{P}}\Bigg[4\sum_{\substack{\underline{m}\in\mathcal{V}^{2l}\\ \hat{m}\neq m_1\oplus m_2}}\sum_{\substack{\underline{a}\in\mathcal{V}^{2k}\\ \hat{a}\in\mathcal{V}^k}}\sum_{\substack{(\underline{v}^n,\underline{x})\in\\ T_{8\delta}(p_{\underline{V}\underline{X}})}} p_{\underline{M}}(\underline{m}) \times \mathrm{Tr}\big(\Gamma_{\hat{a},\underline{m}^{\oplus}}\rho^{\otimes n}_{m_1m_2}\big)\mathbb{1}_{\mathcal{J}}\mathbb{1}_{\mathcal{A}}\Bigg]$$
$$= 4\sum_{\substack{\underline{m}\in\mathcal{V}^{2l}\\ \hat{m}\neq m_1\oplus m_2}}\sum_{\substack{\underline{a}\in\mathcal{V}^{2k}\\ \hat{a}\in\mathcal{V}^k}}\sum_{\substack{(\underline{v}^n,\underline{x})\in\\ T_{8\delta}(p_{\underline{V}\underline{X}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m}) \times \mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho^{\otimes n}_{x_1^nx_2^n}\pi_\rho\Big)\mathbb{E}_{\mathcal{P}}\left[\mathbb{1}_{\mathcal{J}}\mathbb{1}_{\mathcal{A}}\mathbb{1}_{\hat{\mathcal{V}}}\right]$$
$$\leq 4\sum_{\substack{\underline{m}\in\mathcal{V}^{2l}\\ \hat{m}\neq m_1\oplus m_2}}\sum_{\substack{\underline{a}\in\mathcal{V}^{2k}\\ \hat{a}\in\mathcal{V}^k}}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\underline{x}^n\in\underline{\mathcal{X}}^n}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m})\mathcal{P}(\mathcal{V},\mathcal{A},\hat{\mathcal{V}}) \times \left[\prod_{j=1}^{2}p_{X_j|V_j}(x_j^n|v_j^n)\right]\mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho^{\otimes n}_{x_1^nx_2^n}\pi_\rho\Big)$$
$$= 4\sum_{\substack{\underline{m}\in\mathcal{V}^{2l}\\ \hat{m}\neq m_1\oplus m_2}}\sum_{\substack{\underline{a}\in\mathcal{V}^{2k}\\ \hat{a}\in\mathcal{V}^k}}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m})\mathcal{P}(\mathcal{V},\mathcal{A},\hat{\mathcal{V}}) \times \mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho^{\otimes n}_{v_1^nv_2^n}\pi_\rho\Big)$$
$$\leq 4\sum_{\substack{\underline{m}\in\mathcal{V}^{2l}\\ \hat{m}\neq m_1\oplus m_2}}\sum_{\substack{\underline{a}\in\mathcal{V}^{2k}\\ \hat{a}\in\mathcal{V}^k}}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} p_{\underline{M}}(\underline{m})\mathcal{P}(\mathcal{V},\hat{\mathcal{V}}) \times \mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho^{\otimes n}_{v_1^nv_2^n}\pi_\rho\Big)$$
$$\leq 4\sum_{\substack{\underline{m}\in\mathcal{V}^{2l}\\ \hat{m}\neq m_1\oplus m_2}}\sum_{\substack{\underline{a}\in\mathcal{V}^{2k}\\ \hat{a}\in\mathcal{V}^k}}\sum_{\substack{(\underline{v}^n)\in\\ T_{8\delta}(p_{\underline{V}})}}\sum_{\hat{v}^n\in\mathcal{V}^n} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathrm{Tr}\Big(\pi_{\hat{v}^n}\pi_\rho\rho^{\otimes n}_{v_1^nv_2^n}\pi_\rho\Big)$$
$$\leq 4\sum_{\substack{\underline{m}\in\mathcal{V}^{2l}\\ \hat{m}\neq m_1\oplus m_2}}\sum_{\substack{\underline{a}\in\mathcal{V}^{2k}\\ \hat{a}\in\mathcal{V}^k}}\sum_{\hat{v}^n\in\mathcal{V}^n} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathrm{Tr}(\pi_{\hat{v}^n}\pi_\rho) \times 2^{-n(S(\rho)-H(V_1,V_2)-\delta_1)}$$
$$= 4\sum_{\underline{m},\hat{m}}\sum_{\substack{\hat{a},\\ a_1,a_2}}\sum_{\hat{v}^n\in T_\delta(V_1\oplus V_2)} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathrm{Tr}(\pi_{\hat{v}^n}\pi_\rho) \times 2^{-n(S(\rho)-H(V_1,V_2)-\delta_1)}$$
$$\leq 4\sum_{\underline{m},\hat{m}}\sum_{\substack{\hat{a},\\ a_1,a_2}}\frac{p_{\underline{M}}(\underline{m})}{q^{3n}}2^{-n\left[S(\rho)-H(V_1,V_2)-\delta_1-\sum_v p_V(v)S(\rho_v)-H(V)\right]}$$
$$\leq 4\cdot\exp\left\{\begin{array}{l}-n\Big[3\log q - H(V_1,V_2)-\frac{(3k+l)}{n}\log q-\delta_1\\ \quad -\big(\sum_v p_V(v)S(\rho_v)+H(V)-S(\rho)\big)\Big]\end{array}\right\}.$$

The above sequence of steps are analogous to those used in deriving an upper bound on T_{22} and follow from the same set of arguments as provided for the bounds in (21). This completes the proof of the claimed statement.

C. Proof of Proposition 8

For $\underline{m}$, a_{m_1} and a_{m_2}, define the following events:

$$\mathcal{V} \triangleq \{V_j^n(a_{m_j}, m_j) = v_j^n \;:\; j\in[2]\},$$
$$\mathcal{U} \triangleq \{U_j^n(m_{j+2}) = u_j^n \;:\; j\in[2]\},$$
$$\mathcal{W} \triangleq \{\underline{W}^n(\underline{m}) = \underline{w}^n\},\quad \mathcal{A} \triangleq \{A_{m_j} = a_j \;:\; j\in[2]\}.$$

Additionally, for $m^{\oplus}$ and $a^{\oplus}$, define the following events:

$$\hat{\mathcal{V}} \triangleq \{V^n(a^{\oplus}, m^{\oplus}) = v^n\},\ \hat{\mathcal{W}} \triangleq \{W_V^n(m^{\oplus}) = w_V^n\}.$$

$$\mathbb{E}_{\mathcal{P}}[T_{20}] = \mathbb{E}_{\mathcal{P}}\Bigg[\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\underline{v}^n\underline{u}^n v^n\\ \underline{w}^n w_V^n}} p_{\underline{M}}(\underline{m})\mathbb{1}_{\mathcal{V}}\mathbb{1}_{\hat{\mathcal{V}}}\mathbb{1}_{\mathcal{U}}\mathbb{1}_{\mathcal{W}}\mathbb{1}_{\hat{\mathcal{W}}}\mathbb{1}_{\mathcal{A}}\mathbb{1}_{\mathcal{E}} \times \mathrm{Tr}\left\{\left(I-\Gamma_{v^n\underline{u}^nw_V^n\underline{w}_U^n}\right)\rho'_{\underline{u}^n\underline{v}^n\underline{w}^n}\right\}\Bigg],$$
$$\stackrel{(a)}{\leq} 2\tau + \sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{(\underline{v}^n\underline{u}^n)\in T_{8\delta}^{(n)}\\ v^n\underline{w}^nw_V^n}} p_{\underline{M}}(\underline{m})\mathcal{P}(\mathcal{V},\hat{\mathcal{V}},\mathcal{A})\mathcal{P}\left(\mathcal{U}\right)\mathcal{P}(\mathcal{W},\hat{\mathcal{W}}) \times \mathrm{Tr}\left\{\left(I-\Gamma_{v^n\underline{u}^nw_V^n\underline{w}_U^n}\right)\tilde{\rho}_{\underline{u}^n\underline{v}^n}\right\},$$
$$\stackrel{(b)}{\leq} 2\tau + 4\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{(\underline{v}^n\underline{u}^n)\in T_{8\delta}^{(n)}\\ v^n\underline{w}^nw_V^n}} p_{\underline{M}}(\underline{m})\left[\mathrm{Tr}\left\{(I-\widetilde{\Pi}')\tilde{\rho}_{\underline{u}^n\underline{v}^n}\right\} + \mathrm{Tr}\left\{\widehat{\Pi}'_{v^n\underline{u}^nw_V^n\underline{w}_U^n}\tilde{\rho}_{\underline{u}^n\underline{v}^n}\right\}\right]\mathcal{P}(\mathcal{V},\hat{\mathcal{V}},\mathcal{A})\mathcal{P}\left(\mathcal{U}\right)\mathcal{P}(\mathcal{W},\hat{\mathcal{W}}),$$

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3192876

$$\overset{(c)}{\leq} 2\tau + 4\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{(\underline{v}^n\underline{u}^n)\in T_{8\delta}^{(n)}\\ v^n\underline{w}^n w_V^n}} p_{\underline{M}}(\underline{m})\mathbb{1}_{\{v^n=v_1^n\oplus v_2^n\}}$$

$$\times \operatorname{Tr}\left\{\widehat{\Pi}'_{v^n\underline{u}^n w_V^n \underline{w}_U^n}\tilde{\rho}_{\underline{u}^n\underline{v}^n}\right\}\mathcal{P}(\mathcal{V},\hat{\mathcal{V}},\mathcal{A})\mathcal{P}(\mathcal{U})\mathcal{P}(\mathcal{W},\hat{\mathcal{W}}),$$

$$\overset{(d)}{\leq} 2\tau + 4\cdot\frac{18}{\tau^2}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{(\underline{v}^n\underline{u}^n,v^n)\in T_{8\delta}^{(n)}} p_{\underline{M}}(\underline{m})$$

$$\times\left(\sum_{\Phi\in\mathscr{U}}\left(1-\operatorname{Tr}\left\{\Pi^{\Phi}_{v^n\underline{u}^n}\rho_{\underline{v}^n\underline{u}^n}\right\}\right)\right)\mathcal{P}(\mathcal{V},\hat{\mathcal{V}},\mathcal{A})\mathcal{P}(\mathcal{U}),$$

$$\overset{(e)}{\leq} 2\tau + \frac{28\cdot 18}{\tau^2}\delta_2,$$

where $\mathscr{U}\triangleq\{\mathrm{V},\mathrm{U_j},\mathrm{VU_j},\underline{\mathrm{U}},\mathrm{V}\underline{\mathrm{U}}\}$, and $\delta_2(\delta)\searrow 0$ as $\delta\searrow 0$, and (a) follows from the argument $\left\|\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n}-\tilde{\rho}_{\underline{v}^n\underline{u}^n}\right\|_1\leq 4\tau$ (similar to the [13, Equation 5]) and the trace inequality $\operatorname{Tr}\{\Delta\rho\}\leq\operatorname{Tr}\{\Delta\sigma\}+\frac{1}{2}\|\rho-\sigma\|_1$, where $0\leq\Delta,\rho,\sigma\leq I$, (b) follows from Non-Commutative union bound [28], (c) follows from the fact that $\widetilde{\Pi}'$ is a projection operator $\mathcal{H}'^{\otimes n}_Z$ projecting onto $\bar{\mathcal{H}}_Z^{\otimes n}$, and $\tilde{\rho}_{\underline{v}^n\underline{u}^n}\in\mathcal{D}(\bar{\mathcal{H}}_Z^{\otimes n})$. Thus, $\operatorname{Tr}\{(I-\widetilde{\Pi}')\tilde{\rho}_{\underline{v}^n\underline{u}^n}\}=0$, (d) follows from [13, Corollary 1], and (e) follows from Proposition 7. Letting $\tau=\delta_2^{1/4}$, we obtain $\mathbb{E}_{\mathcal{P}}[T_{20}]\leq 504\sqrt{\delta_2}+2\delta_2^{1/4}$.

This concludes the proof of the Proposition 8.

D. Proof of Proposition 9

For $\underline{m}$, a_{m_1} and a_{m_2}, define the following events:

$$\mathcal{V}\triangleq\{V_j^n(a_{m_j},m_j)=v_j^n\ :\ j\in[2]\},$$

$$\mathcal{U}\triangleq\{U_j^n(m_{j+2})=u_j^n\ :\ j\in[2]\},$$

$$\mathcal{W}\triangleq\{\underline{W}^n(\underline{m})=\underline{w}^n\},\quad \mathcal{A}\triangleq\{A_{m_j}=a_j\ :\ j\in[2]\}.$$

1) Analysis of $T_{2V\underline{U}}$: We begin by analyzing error event

$$T_{2V\underline{U}}\triangleq\sum_{\underline{m}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} p_{\underline{M}}(\underline{m})\operatorname{Tr}\left(\Gamma_{(\hat{a},\hat{m}),\hat{m}_3,\hat{m}_4}\rho'^{\otimes n}_{\underline{m}}\right)\mathbb{1}_{\mathscr{E}}.$$

Define the following additional events for $\hat{m},\hat{m}_3,\hat{m}_4$ and $\hat{a}$:

$$\hat{\mathcal{V}}\triangleq\{\hat{V}^n(\hat{a},\hat{m})=\hat{v}^n\},$$

$$\hat{\mathcal{U}}\triangleq\{U_j^n(\hat{m}_{j+2})=\hat{u}_j^n\ :\ j\in[2]\},$$

$$\hat{\mathcal{W}}\triangleq\{W_V^n(\hat{m})=\hat{w}_V^n,\ \underline{W}_U^n(\hat{m}_3,\hat{m}_4)=\underline{\hat{w}}_U^n\}.$$

Next consider the set of inequalities which provide an upper bound on $\mathbb{E}_{\mathcal{P}}\left[T_{2V\underline{U}}\right]$ as given in the following page. We provide the following explanations for the steps involved: (a) follows by bounding $\mathbb{1}_{\mathcal{A}}\leq 1$, (b) follows by using $\mathcal{P}(\mathcal{V},\hat{\mathcal{V}})=\frac{1}{q^{3n}}$ and rearranging the terms, (c) follows by using the fact that w_V used by the decoder is identical to w_{V_1} and expanding $\mathcal{P}(\mathcal{W}|\hat{\mathcal{W}})$ (for $\hat{m}\neq m^{\oplus},\hat{m}_3\neq m_3,\hat{m}_4\neq m_4$) as follows:

$$\sum_{\underline{w}^n}\mathcal{P}(\mathcal{W}|\hat{\mathcal{W}})$$

$$=\sum_{\underline{w}^n}\mathcal{P}(\underline{W}^n(\underline{m})=\underline{w}^n|W_V^n(\hat{m})=\hat{w}_V^n,\underline{W}_U^n(\hat{m}_3,\hat{m}_4)=\hat{w}_U^n),$$

$$=\begin{cases}\sum_{\underline{w}^n}1/|\mathcal{W}|^{4n} & :\hat{m}\neq m_1\\ \sum_{\underline{w}^n}\mathbb{1}_{\{w_{V_1}^n=\hat{w}_V^n\}}1/|\mathcal{W}|^{3n} & :\hat{m}=m_1,\end{cases}$$

(d) follows from the observations [13, Section 4]:

$$\sum_{\underline{w}^n}\frac{1}{|\mathcal{W}|^{4n}}\mathcal{T}^{\mathrm{V}\underline{\mathrm{U}}}_{\underline{w}^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})$$

$$=\frac{1}{1+4\tau^2}\tilde{\rho}_{\underline{v}^n\underline{u}^n}+N_\tau(\tilde{\rho}_{\underline{v}^n\underline{u}^n}),$$

$$\sum_{\underline{w}^n}\mathbb{1}_{\{w_{V_1}^n=\hat{w}_V^n\}}\frac{1}{|\mathcal{W}|^{3n}}\mathcal{T}^{\mathrm{V}\underline{\mathrm{U}}}_{\underline{w}^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})$$

$$=\frac{1+\tau^2}{1+4\tau^2}\mathcal{T}^{\mathrm{V_1}}_{\hat{w}_V^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})+N^{\mathrm{V_1}}_{\hat{w}_V^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n}),$$

(e) follows from the typicality property that for $\underline{v}^n\in T_{8\delta}^{(n)}(p_{V_1V_2})$ and sufficiently large n, we have $\sum_{v^n}p_V^n(v^n)p^n_{\underline{V}|V}(\underline{v}^n|v^n)\leq 2^{-n(H(V_1,V_2)+\delta_1)}$, and the following observations found in [13, Section 4]:

$$(i)\ \left\|N_\tau(\tilde{\rho}_{v^n\underline{u}^n})\right\|_\infty\leq 4\sqrt{2}\tau/\sqrt{|\mathcal{W}|^n},$$
$$(ii)\ ||N^{\mathrm{V_1}}_{\hat{w}_V^n;\tau}(\tilde{\rho}_{v^n\underline{u}^n})||_\infty\leq 4\sqrt{2}\tau/\sqrt{|\mathcal{W}|^n},$$
$$(iii)\ ||\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}_V^n\underline{\hat{w}}_U^n}||_1\leq 2|\mathcal{H}_Z|^n,$$

(f) follows by using the definition $\tilde{\rho}_{v^n\underline{u}^n}=\sum_{\underline{v}^n}p^n_{\underline{V}|V}(\underline{v}^n|v^n)\mathbb{1}_{\{v^n=v_1^n\oplus v_2^n\}}\rho_{\underline{v}^n\underline{u}^n}\otimes|0\rangle\langle 0|^{\mathbb{C}^{2n}}$, (g) follows from [13, Equation 8], and the fact that $\operatorname{Tr}\{\bar{\Pi}^{\mathrm{V}\underline{\mathrm{U}}}_{\hat{v}^n\underline{\hat{u}}^n}\tilde{\rho}\}=\operatorname{Tr}\{\Pi^{\mathrm{V}\underline{\mathrm{U}}}_{\hat{v}^n\underline{\hat{u}}^n}\rho\}$, (h) follows from Proposition 7, and finally (i) follows by choosing $|\mathcal{W}|\leq 2^{I(V,U_1,U_2;Z)_\sigma}$.

2) Analysis of $T_{2\underline{U}}$: We now analyze the error event $T_{2\underline{U}}$ using similar techniques as used for analyzing $T_{2V\underline{U}}$. Define the following events for $m^{\oplus}$, $\hat{m}_3,\hat{m}_4$ and $a^{\oplus}$:

$$\hat{\mathcal{V}}\triangleq\{V^n(a^{\oplus},m^{\oplus})=v^n\},$$

$$\hat{\mathcal{U}}\triangleq\{U_j^n(\hat{m}_{j+2})=\hat{u}_j^n\ :\ j\in[2]\},$$

$$\hat{\mathcal{W}}\triangleq\{W_V^n(m^{\oplus})=w_V^n,\ \underline{W}_U^n(\hat{m}_3,\hat{m}_4)=\underline{\hat{w}}_U^n\}.$$

Now consider the set of inequalities which provide an upper bound on $\mathbb{E}_{\mathcal{P}}[T_{2\underline{U}}]$ as given in the following page. The sequence of steps involved are analogous to those used in deriving an upper bound on $\mathbb{E}_{\mathcal{P}}[T_{2V\underline{U}}]$.

Similarly, for $i,j\in[2]$ and $i\neq j$, we get:

$$\mathbb{E}_{\mathcal{P}}[T_{2VU_j}]$$
$$\leq 2^{\left\{n\left[\left(\frac{3k+l+l_j}{n}\right)\log q-3\log q+H(V_1,V_2)+H(V)+3\delta_1-I(V,U_j;Z|U_i)_\sigma\right]\right\}},$$
$$\mathbb{E}_{\mathcal{P}}[T_{2V}]$$
$$\leq 2^{\left\{n\left[\left(\frac{3k+l}{n}\right)\log q-3\log q+H(V_1,V_2)+H(V)+3\delta_1-I(V;Z|U_1,U_2)_\sigma\right]\right\}},$$
$$\mathbb{E}_{\mathcal{P}}[T_{2U_j}]$$
$$\leq 2^{\left\{n\left[\left(\frac{2k+l_j}{n}\right)\log q-2\log q+H(V_1,V_2)+3\delta_1-I(U_j;Z|V,U_i)_\sigma\right]\right\}}.$$

This completes the proof of the Proposition 9

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3192876

$$
\begin{aligned}
&\mathbb{E}_{\mathcal{P}}\Big[T_{2V\underline{U}}\Big] = \mathbb{E}\Bigg[\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\underline{u}^n\underline{\hat{u}}^n\underline{v}^n\hat{v}^n\\ \underline{w}^n\hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} p_{\underline{M}}(\underline{m})\mathrm{Tr}\Big\{\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}^n_V\underline{\hat{w}}^n_U}\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n}\Big\}\mathbb{1}_{\mathcal{V}}\mathbb{1}_{\hat{\mathcal{V}}}\mathbb{1}_{\mathcal{U}}\mathbb{1}_{\hat{\mathcal{U}}}\mathbb{1}_{\mathcal{W}}\mathbb{1}_{\hat{\mathcal{W}}}\mathbb{1}_{\mathcal{A}}\mathbb{1}_{\mathcal{E}}\Bigg],\\
&\overset{(a)}{\leq}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{(\underline{u}^n,\underline{v}^n)\in T^{(n)}_{8\delta}\\ \underline{\hat{v}}^n\hat{u}^n\\ \underline{w}^n\hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} p_{\underline{M}}(\underline{m})\mathrm{Tr}\Big\{\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}^n_V\underline{\hat{w}}^n_U}\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n}\Big\}\mathcal{P}(\mathcal{V},\hat{\mathcal{V}})\mathcal{P}(\mathcal{U})\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\mathcal{W},\hat{\mathcal{W}}),\\
&\overset{(b)}{=}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\hat{v}^n\underline{\hat{u}}^n\\ \hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})\mathrm{Tr}\Big\{\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}^n_V\underline{\hat{w}}^n_U}\sum_{\substack{(\underline{u}^n,\underline{v}^n)\in T^{(n)}_{8\delta}\\ \underline{w}^n}}\mathcal{P}(\mathcal{U})\mathcal{P}(\mathcal{W}|\hat{\mathcal{W}})\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n}\Big\},\\
&\overset{(c)}{=}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\hat{v}^n\underline{\hat{u}}^n\\ \hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})\mathrm{Tr}\Big\{\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}^n_V\underline{\hat{w}}^n_U}\sum_{(\underline{u}^n,\underline{v}^n)\in T^{(n)}_{8\delta}}\mathcal{P}(\mathcal{U})\\
&\qquad\times\Big[\mathbb{1}_{\{\hat{m}\neq m_1\}}\sum_{\underline{w}^n}\frac{1}{|\mathcal{W}|^{4n}}\mathcal{T}^{\mathrm{VU}}_{\underline{w}^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})+\mathbb{1}_{\{\hat{m}=m_1\}}\sum_{\underline{w}^n}\mathbb{1}_{\{w^n_{V_1}=\hat{w}^n_V\}}\frac{1}{|\mathcal{W}|^{3n}}\mathcal{T}^{\mathrm{VU}}_{\underline{w}^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})\Big]\Big\},\\
&\overset{(d)}{\leq}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\hat{v}^n\underline{\hat{u}}^n\\ \hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})\mathrm{Tr}\Big\{\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}^n_V\underline{\hat{w}}^n_U}\sum_{(\underline{u}^n,\underline{v}^n)\in T^{(n)}_{8\delta}}\mathcal{P}(\mathcal{U})\\
&\qquad\times\Big[\mathbb{1}_{\{\hat{m}\neq m_1\}}\Big(\frac{1}{1+4\tau^2}\tilde{\rho}_{\underline{v}^n\underline{u}^n}+N_\tau(\tilde{\rho}_{\underline{v}^n\underline{u}^n})\Big)+\mathbb{1}_{\{\hat{m}=m_1\}}\Big(\frac{1+\tau^2}{1+4\tau^2}\mathcal{T}^{\mathrm{V}_1}_{\hat{w}^n_V;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})+N^{\mathrm{V}_1}_{\hat{w}^n_V;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})\Big)\Big]\Big\},\\
&\overset{(e)}{\leq}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\hat{v}^n\underline{\hat{u}}^n\\ \hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\sum_{v^n}p^n_V(v^n)\Big[\mathrm{Tr}\Big\{\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}^n_V\underline{\hat{w}}^n_U}\\
&\qquad\times\sum_{\underline{u}^n}\mathcal{P}(\mathcal{U})\Big[\mathbb{1}_{\{\hat{m}\neq m_1\}}\sum_{\underline{v}^n:(\underline{u}^n,\underline{v}^n)\in T^{(n)}_{8\delta}}p^n_{\underline{V}|V}(\underline{v}^n|v^n)\mathbb{1}_{\{v^n=v^n_1\oplus v^n_2\}}\tilde{\rho}_{\underline{v}^n\underline{u}^n}+\\
&\qquad\qquad+\mathbb{1}_{\{\hat{m}=m_1\}}\mathcal{T}^{\mathrm{V}_1}_{\hat{w}^n_V;\tau}\Big(\sum_{\underline{v}^n:(\underline{u}^n,\underline{v}^n)\in T^{(n)}_{8\delta}}p^n_{\underline{V}|V}(\underline{v}^n|v^n)\mathbb{1}_{\{v^n=v^n_1\oplus v^n_2\}}\tilde{\rho}_{\underline{v}^n\underline{u}^n}\Big)\Big]\Big\}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\Big],\\
&\overset{(f)}{=}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\hat{v}^n\underline{\hat{u}}^n\\ \hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\Big[\mathrm{Tr}\Big\{\Gamma_{\hat{v}^n\underline{\hat{u}}^n\hat{w}^n_V\underline{\hat{w}}^n_U}\\
&\qquad\times\sum_{v^n\underline{u}^n}p^n_V(v^n)\mathcal{P}(\mathcal{U})\Big[\mathbb{1}_{\{\hat{m}\neq m_1\}}\tilde{\rho}_{v^n\underline{u}^n}+\mathbb{1}_{\{\hat{m}=m_1\}}\mathcal{T}^{\mathrm{V}_1}_{\hat{w}^n_V;\tau}(\tilde{\rho}_{v^n\underline{u}^n})\Big]\Big\}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\Big],\\
&\overset{(g)}{\leq}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\hat{v}^n\underline{\hat{u}}^n\\ \hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\Big[\mathrm{Tr}\Big\{\Pi^{\mathrm{V}\underline{\mathrm{U}}}_{\hat{v}^n\underline{\hat{u}}^n}\rho\Big\}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\Big],\\
&\overset{(h)}{\leq}\sum_{\substack{\underline{m}\\ \underline{a}}}\sum_{\substack{\hat{v}^n\underline{\hat{u}}^n\\ \hat{w}^n_V\underline{\hat{w}}^n_U}}\sum_{\hat{a}}\sum_{\substack{\hat{m}\neq m^{\oplus}\\ \hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{3n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\Big[2^{-n(I(VU_1U_2;Z)-\delta_1)}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\Big],\\
&\overset{(i)}{\leq}2^{\Big\{n\Big[\Big(\frac{3k+l+l_1+l_2}{n}\Big)\log q-3\log q+H(V)+H(V_1,V_2)+3\delta_1-I(V,U_1,U_2;Z)_\sigma\Big]\Big\}},
\end{aligned}
$$

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3192876

$$
\begin{aligned}
\mathbb{E}_{\mathcal{P}}\left[T_{2\underline{U}}\right] &= \mathbb{E}\left[\sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{\substack{v^n,\underline{\hat{u}}^n,\underline{v}^n,\underline{u}^n\\ w_V^n,\underline{w}^n,\underline{\hat{w}}_U^n}}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} p_{\underline{M}}(\underline{m})\mathrm{Tr}\left\{\Gamma_{v^n\underline{\hat{u}}^n w_V^n \underline{\hat{w}}_U^n}\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n}\right\}\mathbb{1}_{\mathcal{V}}\mathbb{1}_{\hat{\mathcal{V}}}\mathbb{1}_{\mathcal{U}}\mathbb{1}_{\hat{\mathcal{U}}}\mathbb{1}_{\mathcal{W}}\mathbb{1}_{\hat{\mathcal{W}}}\mathbb{1}_{\mathcal{A}}\mathbb{1}_{\mathcal{E}}\right],\\
&\overset{(a)}{\leq} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{\substack{v^n(\underline{u}^n,\underline{v}^n)\in T_{8\delta}^{(n)}\\ \underline{\hat{u}}^n\underline{w}^n w_V^n\underline{\hat{w}}_U^n}}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} p_{\underline{M}}(\underline{m})\mathrm{Tr}\left\{\Gamma_{v^n\underline{\hat{u}}^n w_V^n \underline{\hat{w}}_U^n}\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n}\right\}\mathcal{P}(\mathcal{V},\hat{\mathcal{V}})\mathcal{P}(\mathcal{U})\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\mathcal{W},\hat{\mathcal{W}}),\\
&\overset{(b)}{=} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{\substack{v^n\underline{v}^n\underline{\hat{u}}^n\\ w_V^n\underline{\hat{w}}_U^n}}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{2n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})\mathrm{Tr}\Big\{\Gamma_{v^n\underline{\hat{u}}^n w_V^n \underline{\hat{w}}_U^n}\sum_{\substack{\underline{u}^n:(\underline{u}^n,\underline{v}^n)\in T_{8\delta}^{(n)}\\ \underline{w}^n}}\mathcal{P}(\mathcal{U})\mathcal{P}(\mathcal{W}|\hat{\mathcal{W}})\rho'_{\underline{v}^n\underline{u}^n\underline{w}^n}\Big\},\\
&\overset{(c)}{=} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{\substack{v^n\underline{v}^n\underline{\hat{u}}^n\\ w_V^n\underline{\hat{w}}_U^n}}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{2n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})\mathrm{Tr}\Big\{\Gamma_{v^n\underline{\hat{u}}^n w_V^n \underline{\hat{w}}_U^n}\sum_{\underline{u}^n:(\underline{u}^n,\underline{v}^n)\in T_{8\delta}^{(n)}}\mathcal{P}(\mathcal{U})\\
&\qquad\times\left[\mathbb{1}_{\{m^{\oplus}\neq m_1\}}\sum_{\underline{w}^n}\frac{1}{|\mathcal{W}|^{4n}}\mathcal{T}^{\mathrm{VU}}_{\underline{w}^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})+\mathbb{1}_{\{m^{\oplus}=m_1\}}\sum_{\underline{w}^n}\mathbb{1}_{\{w_{V_1}^n=w_V^n\}}\frac{1}{|\mathcal{W}|^{3n}}\mathcal{T}^{\mathrm{VU}}_{\underline{w}^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})\right]\Big\},\\
&\overset{(d)}{\leq} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{\substack{v^n\underline{v}^n\underline{\hat{u}}^n\\ w_V^n\underline{\hat{w}}_U^n}}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{2n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})\mathrm{Tr}\Big\{\Gamma_{v^n\underline{\hat{u}}^n w_V^n \underline{\hat{w}}_U^n}\sum_{\underline{u}^n:(\underline{u}^n,\underline{v}^n)\in T_{8\delta}^{(n)}}\mathcal{P}(\mathcal{U})\\
&\qquad\times\left[\mathbb{1}_{\{m^{\oplus}\neq m_1\}}\Big(\tilde{\rho}_{\underline{v}^n\underline{u}^n}+N_\tau(\tilde{\rho}_{\underline{v}^n\underline{u}^n})\Big)+\mathbb{1}_{\{m^{\oplus}=m_1\}}\Big(\frac{1+\tau^2}{1+4\tau^2}\mathcal{T}^{\mathrm{V}_1}_{w_V^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})+N^{\mathrm{V}_1}_{w_V^n;\tau}(\tilde{\rho}_{\underline{v}^n\underline{u}^n})\Big)\right]\Big\},\\
&\overset{(e)}{\leq} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{\substack{\underline{\hat{u}}^n\\ w_V^n\underline{\hat{w}}_U^n}}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{2n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\sum_{v^n}p_V^n(v^n)\Bigg[\mathrm{Tr}\Big\{\Gamma_{v^n\underline{\hat{u}}^n w_V^n \underline{\hat{w}}_U^n}\sum_{\underline{u}^n}\mathcal{P}(\mathcal{U})\\
&\qquad\times\Big[\mathbb{1}_{\{m^{\oplus}\neq m_1\}}p^n_{\underline{V}|V}(\underline{v}^n|v^n)\mathbb{1}_{\{v^n=v_1^n\oplus v_2^n\}}\tilde{\rho}_{\underline{v}^n\underline{u}^n}\\
&\qquad\quad+\mathbb{1}_{\{m^{\oplus}=m_1\}}\mathcal{T}^{\mathrm{V}_1}_{w_V^n;\tau}\Big(\sum_{\underline{v}^n:(\underline{u}^n,\underline{v}^n)\in T_{8\delta}^{(n)}}p^n_{\underline{V}|V}(\underline{v}^n|v^n)\mathbb{1}_{\{v^n=v_1^n\oplus v_2^n\}}\tilde{\rho}_{\underline{v}^n\underline{u}^n}\Big)\Big]\Big\}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\Bigg],\\
&\overset{(f)}{=} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{\substack{\underline{\hat{u}}^n\\ w_V^n\underline{\hat{w}}_U^n}}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{2n}}\mathcal{P}(\hat{\mathcal{U}})\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\sum_{v^n}p_V^n(v^n)\Bigg[\mathrm{Tr}\Big\{\Gamma_{v^n\underline{\hat{u}}^n w_V^n \underline{\hat{w}}_U^n}\\
&\qquad\times\Big[\mathbb{1}_{\{m^{\oplus}\neq m_1\}}\sum_{\underline{u}^n}\mathcal{P}(\mathcal{U})\tilde{\rho}_{v^n\underline{u}^n}+\mathbb{1}_{\{m^{\oplus}=m_1\}}\mathcal{T}^{\mathrm{V}_1}_{\hat{w}_V^n;\tau}\Big(\sum_{\underline{u}^n}\mathcal{P}(\mathcal{U})\tilde{\rho}_{v^n\underline{u}^n}\Big)\Big]\Big\}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\Bigg],\\
&\overset{(g)}{\leq} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{w_V^n\underline{\hat{w}}_U^n}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{2n}}\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\sum_{v^n}p_V^n(v^n)\\
&\qquad\times\left[\sum_{\underline{\hat{u}}^n}\mathcal{P}(\hat{\mathcal{U}})\mathrm{Tr}\Big\{\Pi^{\mathrm{V}}_{v^n\underline{\hat{u}}^n}\rho_{v^n}\Big\}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\right],\\
&\overset{(h)}{\leq} \sum_{\substack{\underline{m}\\ \underline{a}}}\ \sum_{w_V^n\underline{\hat{w}}_U^n}\ \sum_{\substack{\hat{m}_3\neq m_3\\ \hat{m}_4\neq m_4}} \frac{p_{\underline{M}}(\underline{m})}{q^{2n}}\mathcal{P}(\hat{\mathcal{W}})2^{n(H(V_1,V_2)+\delta_1)}\left[2^{-n(I(U_1U_2;Z|V)-\delta_1)}+\frac{16\sqrt{2}\tau|\mathcal{H}_Z|^n}{\sqrt{|\mathcal{W}|^n}}\right],\\
&\overset{(i)}{\leq} 2^{\left\{n\left[\left(\frac{2k+l_1+l_2}{n}\right)\log q-2\log q+H(V_1,V_2)+3\delta_1-I(U_1,U_2;Z|V)_\sigma\right]\right\}}.
\end{aligned}
$$

APPENDIX B
CHARACTERIZATION OF CERTAIN HIGH PROBABLE SUBSPACES

In this appendix, we characterize certain high probability subspaces of tensor product quantum states. The statements we prove here are colloquially referred to as 'pinching' [17] in the literature. We prove statements in a form that can be used for use in the proof of aforementioned Theorems and Lemma 1. We begin with definitions of typical and conditional typical projectors. We adopt strong (frequency) typicality. All statements hold for most of the variants of notion of typicality. For concreteness, the reader may refer to [7, App. A].

Lemma 1. *Suppose (i) $\mathcal{A},\mathcal{B}$ are finite sets, (ii) p_{AB} is a PMF on $\mathcal{A}\times\mathcal{B}$, (iii) $(\rho_b \in \mathcal{D}(\mathcal{H}) : b \in \mathcal{B})$ is a collection of density operators, $\rho_a \triangleq \sum_{b\in\mathcal{B}} p_{B|A}(b|a)\rho_b$ for $a\in\mathcal{A}$ and $\rho = \sum_{a\in\mathcal{A}} p_A(a)\rho_a = \sum_{b\in\mathcal{B}} p_B(b)\rho_b$. There exists a strictly positive $\mu>0$, whose value depends only on p_{AB}, such that for every $\delta>0$, there exists a $N(\delta)\in\mathbb{N}$ such that for all $n\geq N(\delta)$, we have*

$$\mathrm{Tr}\big(\Pi^\delta_\rho \Pi^\delta_{a^n}\Pi^\delta_\rho \rho_{b^n}\big) \geq 1-\exp\{-n\lambda\delta^2\},$$

whenever $(a^n,b^n)\in T^{(n)}_\delta(p_{AB})$ where $\Pi^\delta_{a^n}$ is the conditional typical projector of $\rho_{a^n} = \otimes_{t=1}^n \rho_{a_t}$ [17, Defn. 15.2.4] and Π^δ_ρ is the unconditional typical projector [17, Defn. 15.1.3] of $\rho^{\otimes n}$.

Proof. We rename $\mathcal{A}=\mathcal{V}$, $\mathcal{B}=\mathcal{X}$, $p_{AB}=p_{VX}$, a as v and b as x. We have

$$\mathrm{Tr}\big(\Pi^\delta_\rho \Pi^\delta_{v^n}\Pi^\delta_\rho \rho_{x^n}\big) \geq \mathrm{Tr}\big(\Pi^\delta_{v^n}\rho_{x^n}\big) - \frac{1}{2}\left\|\rho_{x^n} - \Pi^\delta_\rho\rho_{x^n}\Pi^\delta_\rho\right\|. \tag{22}$$

In the following we derive a lower bound on $\mathrm{Tr}\big(\Pi^\delta_{v^n}\rho_{x^n}\big)$ and derive an upper bound on $\left\|\rho_{x^n} - \Pi^\delta_\rho\rho_{x^n}\Pi^\delta_\rho\right\|$. Toward the deriving the former, we recall that we have $(v^n,x^n)\in T^{(n)}_\delta(p_{VX})$. Let us define:

$$p_{Y|XV}(y|x,v) \triangleq \left\langle e_{y|v}|\rho_x|e_{y|v}\middle|e_{y|v}|\rho_x|e_{y|v}\right\rangle,$$

for all $(x,v,y)\in\mathcal{X}\times\mathcal{V}\times\mathcal{Y}$. Clearly, we have $p_{Y|XV}(y|x,v)\geq 0$, and $\sum_{y\in\mathcal{Y}} p_{Y|XV}(y|x,v) = \sum_{y\in\mathcal{Y}}\left\langle e_{y|v}|\rho_x|e_{y|v}\middle|e_{y|v}|\rho_x|e_{y|v}\right\rangle = \mathrm{Tr}(\rho_x)=1$. Hence, we see that $p_{Y|XV}$ is a stochastic matrix. Next we note that

$$\begin{aligned}
&\sum_{x\in\mathcal{X}} p_{Y|XV}(y|x,v)p_{XV}(x,v)\\
&=\sum_{x\in\mathcal{X}} p_{XV}(x,v)\left\langle e_{y|v}|\rho_x|e_{y|v}\middle|e_{y|v}|\rho_x|e_{y|v}\right\rangle\\
&=p_V(v)\\
&\times\left\langle e_{y|v}|\sum_{x\in\mathcal{X}} p_{X|V}(x|v)\rho_x|e_{y|v}\middle|e_{y|v}|\sum_{x\in\mathcal{X}} p_{X|V}(x|v)\rho_x|e_{y|v}\right\rangle\\
&=p_V(v)\left\langle e_{y|v}|\rho_v|e_{y|v}\middle|e_{y|v}|\rho_v|e_{y|v}\right\rangle = p_V(v)q_{Y|V}(y|v),
\end{aligned} \tag{23}$$

where we have used the spectral decomposition of ρ_v.

Observe that if $(x^n,v^n)\in T^n_{\delta/4}(p_{XV})$, and $y^n\in T^n_\delta(p_{XV}p_{Y|XV}|x^n,v^n)$, then we have $(x^n,v^n,y^n)\in T^n_\delta(p_{XV}p_{Y|XV})$. This implies that we have $(v^n,y^n)\in T^n_{4\delta}(p_{VY})$, where p_{VY} is the marginal of $p_{XV}p_{Y|XV}$. Using this and (23), we see that $(v^n,y^n)\in T^n_{4\delta}(p_Vq_{Y|V})$. In summary, we see that if $(x^n,v^n)\in T_\delta(p_{XV})$, then we have

$$T^n_{4\delta}(p_{XV}p_{Y|XV}|x^n,v^n)\subseteq\left\{y^n : (v^n,y^n)\in T^n_{4\delta}(p_Vq_{Y|V})\right\}.$$

We are now set to provide the promised lower bound. Consider

$$\begin{aligned}
&\mathrm{Tr}(\Pi_{v^n}\rho_{x^n})\\
&=\mathrm{Tr}\left(\left[\sum_{\substack{y^n:\\(v^n,y^n)\in T^{(n)}_{4\delta}(p_Vq_{Y|V})}}\bigotimes_{t=1}^n\left|e_{y_t|v_t}\right\rangle\left\langle e_{y_t|v_t}\right|\right]\left[\bigotimes_{j=1}^n\rho_{x_j}\right]\right)\\
&=\mathrm{Tr}\left(\left[\sum_{y^n:(v^n,y^n)\in T^{(n)}_{4\delta}(p_Vq_{Y|V})}\bigotimes_{t=1}^n\left|e_{y_t|v_t}\right\rangle\left\langle e_{y_t|v_t}\right|\rho_{x_t}\right]\right)\\
&=\sum_{\substack{y^n:\\(v^n,y^n)\in T^{(n)}_{4\delta}(p_Vq_{Y|V})}}\prod_{t=1}^n\left\langle e_{y_t|v_t}|\rho_{x_t}|e_{y_t|v_t}\middle|e_{y_t|v_t}|\rho_{x_t}|e_{y_t|v_t}\right\rangle\\
&\geq\sum_{y^n\in T^{(n)}_{4\delta}(p_{XV}p_{Y|XV}|x^n,v^n))}\prod_{t=1}^n p_{Y|XV}(y_t|x_t,v_t)\\
&\geq 1-2|\mathcal{X}||\mathcal{Y}||\mathcal{V}|\exp\left\{-\frac{2n\delta^2 p_{XVY}(x^*,v^*,y^*)}{4(\log(|\mathcal{X}||\mathcal{Y}||\mathcal{V}|))^2}\right\},
\end{aligned} \tag{24}$$

where we used (23) in the last equality, and (x^*,v^*,y^*) is the triple which attains the minimum non-zero probability.

We next provide the upper bound. Note from the Gentle measurements lemma [17, Lemma 9.4.2], we have $\|\rho_{x^n} - \Pi^\delta_\rho\rho_{x^n}\Pi^\delta_\rho\|\leq 3\sqrt{\epsilon}$ if $\mathrm{Tr}\big(\Pi^\delta_\rho\rho_{x^n}\big)\geq 1-\epsilon$. In the following we provide a lower bound on $\mathrm{Tr}\big(\Pi^\delta_\rho\rho_{x^n}\big)$. Recall that $\Pi^\delta_\rho = \sum_{y^n\in T^n_\delta(s_Y)}\bigotimes_{t=1}^n\left|g_{y_t}\right\rangle\left\langle g_{y_t}\right|$, where

$$\rho=\sum_{y\in\mathcal{Y}} s_Y(y)\left|g_y\right\rangle\left\langle g_y\right|,$$

is the spectral decomposition of ρ, and $\rho=\sum_{x\in\mathcal{X}} p_X(x)\rho_x$. Let $\hat{p}_{Y|X}(y|x)\triangleq\langle g_y|\rho_x|g_y|g_y|\rho_x|g_y\rangle$, for all $(x,y)\in\mathcal{X}\times\mathcal{Y}$. Note that $\hat{p}_{Y|X}$ is not related to $p_{Y|X}$ defined previously. We note that $\hat{p}_{Y|X}(y|x)\geq 0$, and $\sum_{y\in\mathcal{Y}}\hat{p}_{Y|X}(y|x) = \sum_{y\in\mathcal{Y}}\langle g_y|\rho_x|g_y|g_y|\rho_x|g_y\rangle = \mathrm{Tr}(\rho_x)=1$ for all $x\in\mathcal{X}$. Thus we see that $\hat{p}_{Y|X}$ is a stochastic matrix. It can also be noted that

$$\begin{aligned}
&\sum_{x\in\mathcal{X}}\hat{p}_{Y|X}(y|x)p_X(x)\\
&\qquad=\left\langle g_y|\sum_{x\in\mathcal{X}} p_X(x)\rho_x|g_y\middle|g_y|\sum_{x\in\mathcal{X}} p_X(x)\rho_x|g_y\right\rangle\\
&\qquad=\langle g_y|\rho|g_y|g_y|\rho|g_y\rangle = s_Y(y),
\end{aligned}$$

for all $y\in\mathcal{Y}$. This implies that the condition $y^n\in T^n_\delta(s_Y)$ is equivalent to the condition $y^n\in T^n_\delta(\hat{p}_Y)$, where $\hat{p}_Y(y) = \sum_{x\in\mathcal{X}}\hat{p}_{Y|X}(y|x)p_X(x)$. Moreover, if $x^n\in T^n_{\delta/2}(p_X)$, and $y^n\in T^n_\delta(p_X\hat{p}_{Y|X}|x^n)$, then we have $(x^n,y^n)\in T^n_\delta(p_X\hat{p}_{Y|X})$. Consequently, we have $y^n\in T^n_\delta(\hat{p}_Y)$, which in turn implies that $y^n\in T^n_\delta(s_Y)$. In essence, we have that if $x^n\in T^n_{\delta/2}(p_X)$ then $T^n_\delta(p_X\hat{p}_{Y|X}|x^n)\subseteq T^n_\delta(s_Y)$. Now we are set to provide the lower bound on $\mathrm{Tr}\big(\Pi^\delta_\rho\rho_{x^n}\big)$ as follows:

$$\begin{aligned}
\mathrm{Tr}\big(\Pi^\delta_\rho\rho_{x^n}\big) &= \mathrm{Tr}\left(\sum_{y^n\in T_\delta(s_Y)}\bigotimes_{t=1}^n\left|g_{y_t}\right\rangle\left\langle g_{y_t}\right|\rho_{x_t}\right)\\
&=\sum_{y^n\in T_\delta(s_Y)}\prod_{t=1}^n\langle g_{y_t}|\rho_{x_t}|g_{y_t}|g_{y_t}|\rho_{x_t}|g_{y_t}\rangle
\end{aligned}$$

$$= \sum_{y^n \in T_\delta(s_Y)} \prod_{t=1}^{n} \hat{p}_{Y|X}(y_t|x_t)$$
$$\geq \sum_{y^n \in T_\delta(\hat{p}_{Y|X} p_X|x^n)} \prod_{t=1}^{n} \hat{p}_{Y|X}(y_t|x_t)$$
$$\geq 1 - 2|\mathcal{X}||\mathcal{Y}| \exp\left\{ -\frac{2n\delta^2 p_X^2(x^*) \hat{p}_{Y|X}^2(y|x)}{4(\log(|\mathcal{X}||\mathcal{Y}|))^2} \right\}. \tag{25}$$

where x^* is the value which attains the minimum non-zero probability. We therefore have

$$\|\rho_{x^n} - \Pi_\rho^\delta \rho_{x^n} \Pi_\rho^\delta\| \leq 6|\mathcal{X}||\mathcal{Y}| \exp\left\{ -\frac{2n\delta^2 p_X^2(x^*) \hat{p}_{Y|X}^2(y|x)}{4(\log(|\mathcal{X}||\mathcal{Y}|))^2} \right\},$$

and

$$\mathrm{Tr}(\Pi_{v^n} \rho_{x^n}) \geq 1 - 2|\mathcal{X}||\mathcal{Y}||\mathcal{V}| \frac{2n\delta^2 p_X^2(x^*) \hat{p}_{Y|X}^2(y|x)}{4(\log(|\mathcal{X}||\mathcal{Y}|))^2},$$

thereby permitting us to conclude that

$$\mathrm{Tr}\left(\Pi_\rho^\delta \Pi_{v^n}^\delta \Pi_\rho^\delta \rho_{x^n}\right) \geq \mathrm{Tr}\left(\Pi_{v^n}^\delta \rho_{x^n}\right) - \frac{1}{2}\|\rho_{x^n} - \Pi_\rho^\delta \rho_{x^n} \Pi_\rho^\delta\|$$
$$\geq 1 - \frac{2n\delta^2 p_X^2(x^*) \hat{p}_{Y|X}^2(y|x)}{4(\log(|\mathcal{X}||\mathcal{Y}|))^2},$$

if $(x^n, v^n) \in T_{\delta/2}^n(p_{XV})$. $\square$

References

[1] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," Phys. Rev. A, vol. 56, pp. 131–138, Jul 1997. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.56.131

[2] A. S. Holevo, "The capacity of the quantum channel with general signal states," IEEE Transactions on Information Theory, vol. 44, no. 1, pp. 269–273, 1998.

[3] A. Winter, "The capacity of the quantum multiple-access channel," IEEE Transactions on Information Theory, vol. 47, no. 7, pp. 3059–3065, 2001.

[4] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources (corresp.)," IEEE Transactions on Information Theory, vol. 25, no. 2, pp. 219–221, 1979.

[5] B. Nazer and M. Gastpar, "Computation over multiple-access channels," IEEE Trans. on Info. Th., vol. 53, no. 10, pp. 3498 –3516, oct. 2007.

[6] M. Hayashi and Á. Vázquez-Castro, "Computation-aided classical-quantum multiple access to boost network communication speeds," Physical Review Applied, vol. 16, no. 5, p. 054021, 2021.

[7] S. S. Pradhan, A. Padakandla, and F. Shirani, "An algebraic and probabilistic framework for network information theory," Foundations and Trends® in Communications and Information Theory, vol. 18, no. 2, pp. 173–379, 2020. [Online]. Available: http://dx.doi.org/10.1561/0100000083

[8] A. Padakandla and S. Sandeep Pradhan, "Computing sum of sources over an arbitrary multiple access channel," in 2013 IEEE International Symposium on Information Theory, 2013, pp. 2144–2148.

[9] R. Ahlswede and T. Han, "On source coding with side information via a multiple-access channel and related problems in multi-user information theory," IEEE Transactions on Information Theory, vol. 29, no. 3, pp. 396–412, 1983.

[10] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," IEEE Transactions on information Theory, vol. 19, no. 4, pp. 471–480, 1973.

[11] T. A. Atif, A. Padakandla, and S. S. Pradhan, "Computing sum of sources over a classical-quantum mac," in 2021 IEEE International Symposium on Information Theory (ISIT), 2021, pp. 414–419.

[12] P. Sen, "A one-shot quantum joint typicality lemma. arxiv e-prints, page," arXiv preprint arXiv:1806.07278, 2018.

[13] ——, "Unions, intersections and a one-shot quantum joint typicality lemma," Sādhanā, vol. 46, no. 1, pp. 1–44, 2021.

[14] O. Fawzi, P. Hayden, I. Savov, P. Sen, and M. M. Wilde, "Classical communication over a quantum interference channel," IEEE Transactions on Information Theory, vol. 58, no. 6, pp. 3670–3691, 2012.

[15] I. Savov, "Network information theory for classical-quantum channels," arXiv preprint arXiv:1208.4188, 2012.

[16] T. A. Atif, A. Padakandla, and S. S. Pradhan, "Achievable rate-region for 3—user classical-quantum interference channel using structured codes," in 2021 IEEE International Symposium on Information Theory (ISIT), 2021, pp. 760–765.

[17] M. M. Wilde, Quantum Information Theory, 1st ed. USA: Cambridge University Press, 2013.

[18] A. S. Holevo, Quantum systems, channels, information: a mathematical introduction. Walter de Gruyter, 2012, vol. 16.

[19] M. Gastpar and B. Nazer, "Algebraic structure in network information theory," IEEE ISIT Tutorial, 2011.

[20] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," IEEE Transactions on Information Theory, vol. 57, no. 10, pp. 6463–6486, 2011.

[21] M. V. Pedersen, F. H. Fitzek, and T. Larsen, "Implementation and performance evaluation of network coding for cooperative mobile devices," in ICC Workshops-2008 IEEE International Conference on Communications Workshops. IEEE, 2008, pp. 91–96.

[22] A. Giridhar and P. R. Kumar, "Computing and communicating functions over sensor networks," IEEE Journal on selected areas in communications, vol. 23, no. 4, pp. 755–764, 2005.

[23] B. Nazer, A. Sanderovich, M. Gastpar, and S. Shamai, "Structured superposition for backhaul constrained cellular uplink," in 2009 IEEE International Symposium on Information Theory, 2009, pp. 1530–1534.

[24] B. Nazer and M. Gastpar, "Computing over multiple-access channels with connections to wireless network coding," in 2006 IEEE International Symposium on Information Theory, 2006, pp. 1354–1358.

[25] T. Berger, "Multiterminal source coding," The Inform. Theory Approach to Communications, G. Longo, Ed., New York: Springer-Verlag, 1977.

[26] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," IEEE Transactions on Information Theory, vol. 49, no. 7, pp. 1753–1768, 2003.

[27] A. Padakandla, "An Algebraic Framework for Multi-terminal Communication," Ph.D. dissertation, Univ. of Michigan, Ann Arbor, USA, May. 2014, available at http://deepblue.lib.umich.edu/handle/2027.42/107264.

[28] P. Sen, "Achieving the han-kobayashi inner bound for the quantum interference channel," in 2012 IEEE International Symposium on Information Theory Proceedings. IEEE, 2012, pp. 736–740.

Mohammad Aamir Sohail is pursuing a Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Michigan, Ann Arbor. His research interests include quantum error correction, quantum algorithms, and quantum information theory. He graduated from the Indian Institute of Technology (IIT) Hyderabad with a Bachelor of Technology degree in Electrical Engineering and was awarded the President of India Gold Medal.

Touheed Anwar Atif received a B.Tech. degree from the Department of Electrical Engineering, Indian Institute of Technology Hyderabad in 2017 and an M.Sc. degree in Electrical Engineering from the University of Michigan, Ann Arbor in 2019. He is currently pursuing a Ph.D. degree in Electrical Engineering and Computer Science with the University of Michigan, Ann Arbor. His research interests include quantum information theory and quantum algorithms.

Arun Padakandla received an MSc degree in Electrical Communication Engg. from the Indian Institute of Science, Bangalore. He went on to receive an MSc degree in Mathematics and a Doctorate in Electrical Engg., both from the University of Michigan at Ann Arbor. Following a brief stint as a research engineer at Ericsson Research, San Jose, he joined the NSF Center for Science of Information as a postdoctoral research fellow in 2015. Since 2018, he has been on the faculty of the Dept. of EECS, Univ. of Tennessee at Knoxville. His research interests lie in quantum and classical information science.

S. Sandeep Pradhan (Fellow, IEEE) received an M.E. degree from the Indian Institute of Science in 1996 and a Ph.D. degree from the University of California at Berkeley in 2001. From 2002 to 2008, he was an Assistant Professor, and from 2008 to 2015, he was an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, where he is currently a Professor. His research interests include network information theory, coding theory, and quantum information theory. He was an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY in the area of Shannon theory from 2014 to 2016.