Communicating over a Classical-Quantum MAC with State Information Distributed at Senders

Arun Padakandla
University of Tennessee, USA
Email: arunpr@utk.edu

Abstract

We consider the problem of communicating over a classical-quantum (CQ) multiple access channel with classical states non-causally available at the transmitter, henceforth referred to as a QMSTx. QMSTx is a classical-quantum multiple access analogue of the channel studied [1] by Gelfand and Pinsker in 1980. We undertake a Shannon-theoretic study and focus on the problem of characterizing inner bounds to the capacity region of a QMSTx. We propose a new coding scheme based on union coset codes - codes possessing algebraic closure properties and derive a new inner bound that subsumes the largest known inner bound based on IID random coding. We identify examples for which the derived inner bound is strictly larger.

I. INTRODUCTION

Consider the scenario of communicating over a classical-quantum (CQ) multiple access channel with classical states (QMSTx) depicted in Fig. 1. S1, S2 model a pair of channel states that are jointly distributed and whose evolution across time is IID. Transmitter (Tx) j is provided the entire realization of the state Sj non-causally and is required to communicate its message Mj to a receiver (Rx) that is uninformed of the states. If the channel is in state s1, s2 and Txs 1, 2 choose input symbols x1, x2 respectively, then the Rx is provided the quantum state \( \rho_{x_1, x_2, s_1, s_2} \). Our focus is on the problem of characterizing an inner bound to the capacity region of a general QMSTx. In the sequel, we describe our motivation and contributions.

Our motivation in addressing this problem is four fold. Firstly, QMSTx is a network for which the conventional long established technique of proving inner bounds via IID random codes, also referred to herein as unstructured codes, is suboptimal. In this article, we design a coding scheme based on union coset codes (UCC) - codes possessing algebraic closure properties - that strictly outperforms the best known coding scheme based on IID codes. Specifically, we analyze performance of the designed coding scheme to derive an inner bound (Thms. 2, 3) to the capacity region of a QMSTx that, not only subsumes the largest inner bound via unstructured codes, but strictly enlarges the same for identified examples (Ex. 1, Prop. 3). These findings build on our earlier work [2], [3] and maybe viewed as another step [4], [5] in our pursuit of designing coding schemes based on coset codes for network CQ communication.

While the utility of coset codes have been established in several networks [3]–[8], their use for a QMSTx is unique and leads us to our second motivation. Coset codes have facilitated higher rates in communication scenarios wherein a compressive bivariate function of the messages or codewords have to be decoded. For instance, on both the 3–user interference [4], [9] and broadcast channels [8], coset codes enable efficient decoding of the bivariate interference. QMSTx is a CQ MAC wherein both messages need to be decoded and decoding a compressive bivariate function of either the codewords or the messages can lead to obfuscation of the messages. Indeed, coset codes have no role in communication over a CQ-MAC without Tx states. It is therefore natural to question the utility of structured codes in communicating over a QMSTx. A second motivation of our work is to demonstrate how algebraic closure properties can be exploited to efficiently sieve relevant information and thereby facilitate enhanced communication over a QMSTx. We illustrate this phenomena in the context of an example (Ex. 1) and a self contained discussion (Secs. III-B, III-C). In particular, Sec. III enables us convey the main ideas of this article.

Thirdly, this study enables us enrich the family of coset codes for CQ communication beyond nested coset codes (NCC) [4], [5] and partitioned coset codes (PCC) [10] studied recently. As elaborated in [3] and recent works [11], [12], coding schemes based on NCC or PCC designed for a classical analogue of a QMSTx, i.e., a classical MAC with states, can be strictly inferior to a coding scheme based on UCC. We have taken this cue and designed UCC based coding schemes and our results in Sec. VI also prove that UCCs achieve capacity of a single sender CQ channel. Lastly, our findings maybe viewed as developing new strategies to handle various network scenarios arising in an eventual quantum communication network.

![Fig. 1.](image_url)
Our presentation is organized in a modular fashion. In Sec. III, we illustrate the main ideas of our work through a discussion in the context of a carefully chosen example (Ex. 1). A general coding scheme for a QMSTx consists of two layers - unstructured codes and UCC. In order to illustrate the new elements in a simplified setting, we present a simplified coding scheme involving only the UCC layer in Sec. IV, wherein we provide a detailed description and proof steps. In Sec. V we present our inner bound that comprises of both unstructured and UCC layers. In Sec. VI, we prove that a coding scheme based on UCCs can achieve the best known single-letter inner bound to the capacity region of a single sender version of a QMSTx, i.e., single Tx, single Rx classical-quantum channel with random classical channel states available only at the Tx, referred to therein as a QSTx. In this article, we focus on conveying the ideas and techniques developed.

The study of channels with Tx state information traces its roots back to Shannon [13] and has had considerable influence on other problems. Indeed, Gelfand and Pinsker’s coding scheme [1] for the classical single Tx channel with states, henceforth referred to as the Gelfand-Pinsker channel, forms the core of Marton’s coding [14] for the broadcast channel. Recently, Boche, Cai and Nötzel [15] studied the CQ analogue of the Gelfand-Pinsker channel and proved achievability of a corresponding inner bound. Their work exploits the method of types and the findings by Nötzel [16] in proving achievability of the inner bound. Moreover, their work [15] highlights the difference between the causal and the non-causal availability of state information at the Tx in regards to the single-letterization of the capacity. Our focus is on designing a new coding scheme and characterizing its performance via a single-letter expression. We have not commented on optimality of the bounds derived herein.

II. PRELIMINARIES AND PROBLEM STATEMENT

For $n \in \mathbb{N}$, $[n] \triangleq \{1, \ldots, n\}$. $\mathcal{F}_q$ denotes the finite field of size $q$ and $\oplus_q$ denotes addition within $\mathcal{F}_q$. For a Hilbert space $\mathcal{H}$, $\mathcal{L}(\mathcal{H})$, $\mathcal{P}(\mathcal{H})$ and $\mathcal{D}(\mathcal{H})$ denote the collection of linear, positive and density operators acting on $\mathcal{H}$ respectively. We let an underline denote an appropriate aggregation of pairs of objects. For example, $\underline{U} \triangleq U_1 \times U_2$ denotes the Cartesian product for sets, $\underline{x} \triangleq (x_1, x_2) \in \mathcal{X}$ and $\underline{x}^n \triangleq (x^n_1, x^n_2)$. The specific aggregation will be clear from context. We abbreviate probability mass function as PMF.

Consider a (generic) QMSTx specified through (i) two finite input sets $\mathcal{X}_1, \mathcal{X}_2$, (ii) two finite sets $\mathcal{S}_1, \mathcal{S}_2$ of states, (iii) a collection $\{\rho_{\underline{x},\underline{s}} \in \mathcal{D}(\mathcal{H}_Y) : (\underline{x}, \underline{s}) \in \mathcal{X} \times \mathcal{S}\}$ of density operators and (iv) cost functions $\kappa_j : \mathcal{X}_j \times \mathcal{S}_j \rightarrow [0, \infty]$ for $j \in [2]$. The cost function is additive, i.e., having observed the state sequence $s^n_j$ the cost incurred by sender $j$ in preparing the state $s^n_j$ is $\tau_j(x^n_j, s^n_j) \triangleq \frac{1}{n} \sum_{t=1}^{n} \kappa_j(x_j, s_j)$. Reliable communication on a QMSTx entails identifying a code.

**Defn. 1.** An $(n, \underline{M}, \underline{e}, \lambda)$ QMSTx code consists of two message index sets $\underline{M}_j : j \in [2]$, two encoder maps $e_j : [\underline{M}_j] \times \mathcal{S}_j^n \rightarrow \mathcal{X}_j^n$ and a decoder POVM $\lambda \triangleq \{\lambda_m = \lambda_{m_1, m_2} \in \mathcal{P}(\mathcal{H}^\otimes n) : m \in \underline{M}\}$. The average error probability of the code is

$$\overline{\xi}(\underline{e}, \lambda) \triangleq 1 - \frac{1}{|\underline{M}|} \sum_{m \in \underline{M}} \sum_{s^n} p^n_S(s^n) \text{tr}(\lambda_m \rho_{m, s^n}),$$

where $\rho_{m, s^n} \triangleq \otimes_{t=1}^{n} \rho_{x^n_t, s^n_t}$ and $(x_1, \ldots, x_n) = e_j(m_j, s_j^n)$. Average cost incurred by sender $j$ in transmitting $m_j$ is $\tau_j(e_j|m_j) \triangleq \sum_{s^n_j} p^n_S(s^n_j) \kappa_j(e_j(m_j, s^n_j), s^n_j)$ and the average cost incurred by sender $j$ is $\tau_j(e_j) \triangleq 1/|\underline{M}_j| \sum_{m_j} \tau_j(e_j|m_j)$.

The object of interest is the capacity region of a QMSTx defined below. In this article, we focus on characterizing inner bounds to the capacity region of a QMSTx.

**Defn. 2.** A rate-cost quadruple $(R, \tau) \in [0, \infty)^4$ is achievable if there exists a sequence of QMSTx codes $(n, \underline{M}^{(n)}, \underline{e}^{(n)}, \lambda^{(n)})$ for which

$$\lim_{n \to \infty} \overline{\xi}(\underline{e}^{(n)}, \lambda^{(n)}) = 0, \\
\lim_{n \to \infty} n^{-1} \log |\underline{M}^{(n)}_j| = R_j, \text{ and } \lim_{n \to \infty} \tau_j(e_j^{(n)}) \leq \tau_j.$$  

The capacity region $\mathcal{C}$ of the QMSTx is the set of all achievable rate-cost vectors and $\mathcal{C}(\tau) \triangleq \{R : (R, \tau) \in \mathcal{C}\}$.

III. ROLE OF ALGEBRAIC STRUCTURE/CLOSURE

In this section, we explain how and why structured codes can facilitate enhanced communication over a QMSTx. We begin by reviewing the best known unstructured coding scheme.

A. Joint Decoding of Unstructured Codes

A QMSTx is a ‘MAC extension’ of a single sender CQ channel with random states [15]. A coding scheme for the QMSTx can therefore be obtained by combining the Gelfand-Pinsker encoding scheme [1] with a simultaneous decoder of a MAC [17] Thm. 2]. Specifically, each sender $j$ builds a $U_j$-code (Tab. I) on an auxiliary set $U_j$. The $U_j$-code comprises of $2^{n(R_j + H_{\mathcal{S}_j})}$ codewords partitioned into $2^{nH_{\mathcal{S}_j}}$ bins. The message $m_j \in [2^{nH_{\mathcal{S}_j}}]$ indexes a bin and the encoder looks for a codeword within this bin that is jointly typical with the state sequence $s^n_j$. The chosen codeword, denoted as $u^n_j(m_j, s^n_j)$, and the state sequence $s^n_j$ are mapped to an input sequence in $\mathcal{X}_j^n$.
The decoder POVM performs simultaneous decoding on the $U_1, U_2-$codebooks. Specifically, one can adopt the decoding POVM proposed in proof of [17] Thm. 2. Leveraging the ‘projector trick’ therein and the ‘overcounting trick’ [18] in the context of Marton decoding, we can analyze the error probability and derive an inner bound. The latter is the largest known inner bound achievable via any unstructured coding scheme and we provide a characterization of the same below.

**Theorem 1.** A rate-cost quadruple $(R, \tau)$ is achievable if there exists finite sets $U_1, U_2$, conditional distributions $p_{X_j, U_j | S_j}$ on $X_j \times U_j$ for $j \in [2]$ such that $p_{S_j X_j} (s, u, x) = p_Z (s) \prod_{j = 1}^2 p_{X_j, U_j | S_j} (x_j, u_j | s_j)$ with respect to which

\[
R_j < I(U_j; Y, U_2) - I(U_j; S_j) \nu, \quad \EE\{s_j | X_j, S_j\} \leq \tau_j, \\
R_1 + R_2 < I(U; Y) + I(U_1, S_1; U_2, S_2) \sigma,
\]

for $j \in [2]$, where all informations are computed wrt the state

\[
\sigma^{YXSU} \triangleq \sum_{x, u, z} p_{S_j X_j} (s, u, x) \rho_{zz} \otimes \|x \oplus u\rangle \langle z \oplus s|.
\]

**B. Binary Double Dirty MAC**

Our discussion for the following example portrays the deficiency of unstructured codes and the role of structure.

**Ex. 1.** Let $X_1 = X_2 = S_1 = S_2 = \{0, 1\}$, $p_Z (s) = \frac{1}{2}$ for every $s \in S$, $|v_0\rangle = [\cos \theta \quad \sin \theta]^T$ and $|v_1\rangle = [\sin \theta \quad -\cos \theta]^T$. For $(x, s) \in \{0, 1\}^4$, let $\rho_{j, x_2, s_1, s_2} = \gamma (x_1 \oplus x_2, s_1 \oplus s_2)$, where $\gamma (\cdot, \cdot)$ is provided in Table II $\oplus$ denotes addition in the binary field $\mathbb{F}_2$ and the cost function $\kappa_j (x_j, s_j) = 1_{\{x_j = 1\}}$ is the Hamming weight function. For $\tau \in (0, \frac{1}{2})$, what is $\mathcal{E}(\tau, \tau)$?

Our discussion below for the $\theta = 0$ case leads us pedagogically to the non-commuting case $\theta \in (0, \frac{\pi}{2})$ which follows. The classical channel corresponding to $\theta = 0$ was first studied by Philosof and Zamir [19] and the following discussion describes their findings.

**Case $\theta = 0$:** Since the collection $\{\rho_{zz} : (x, s) \in \{0, 1\}^4\}$ is commuting, we identify this as a classical MAC with distributed states whose output $Y \in \{0, 1\}$, inputs $X_1, X_2 \in \{0, 1\}$ and states $S_1, S_2 \in \{0, 1\}$ are related as $Y = X_1 \oplus S_1 \oplus X_2 \oplus S_2$. $S_1, S_2$ are uniformly distributed and the average Hamming weight of the inputs is constrained to $\tau < \frac{1}{2}$. The latter constraint precludes the senders from negating the effect of the state. What rate pairs are then achievable?

We first study the best unstructured coding scheme and characterize the corresponding largest known inner bound. Towards that end, observe that the effective classical channel of Ex. 1 is a ‘MAC extension’ of a single sender channel with random parameters whose output $Y \in \{0, 1\}$, Hamming cost-constrained input $X \in \{0, 1\}$ and uniformly distributed state $S \in \{0, 1\}$ are related as $Y = X \oplus S$. Philosof and Zamir [19] proved that the best unstructured coding strategy for Ex. 1 is obtained by replicating, at both the senders, the capacity achieving strategy for the single sender channel. Specifically, they prove the optimal choice of parameters in Thm. 1 for Ex. 1 to be binary auxiliary sets $U_1 = U_2 = \{0, 1\}$, $p_{U_j | S_j} (1 | 0) = p_{U_j | S_j} (0 | 1) = \tau = 1 - p_{U_j | S_j} (0 | 0) = 1 - p_{U_j | S_j} (1 | 1)$ and $X_j = U_j \oplus S_j$ for $j \in [2]$.

We now detail the coding scheme corresponding to the above choice to shed light on its deficiency. To communicate at rate $R_j < h_b (\tau)$, sender $j$ randomly partitions the entire set of $2^n$ sequences into $2^{n R_j}$ bins. The message $m_j$ indexes the bin within which the sender looks for a codeword that is within an average Hamming distance of $\tau$ from the observed state sequence. Since each bin contains $2^n (1 - R_j) > 2^{n (1 - h_b (\tau))}$ sequences chosen randomly, the sender finds such a codeword whp. Let $U_j^n$ denote the chosen codeword and $S_j^n$ the observed state sequence. Sender $j$ inputs $X_j^n = U_j^n \oplus S_j^n$ on the channel. The choice of the $U_j-$codeword guarantees that the Hamming weight constraint is met.
Observe that the channel relationship \( Y = X_1 \oplus S_1 \oplus X_2 \oplus S_2 \) implies that the received vector is \( Y^n = U^n_1 \oplus U^n_2 \). Recall that each message \( m_j \) of sender \( j \) is assigned a bin of \( U_j \)—codewords. The space of received sequences occupied by a single message pair \( (m_1, m_2) \) is therefore got by adding all possible codeword pairs in the two bins indexed by \( m_1, m_2 \). Since the codewords in each bin is picked uniformly and independently without any joint structure, every pair yields \( \text{whp} \) a distinct sum, resulting in the range of this addition to be of size \( 2^{n(2-R_1-R_2)} > 2^{hn(1-h_b(\tau))} \). Since the ‘fan-out’ of every message pair is of size atleast \( 2^{hn(1-h_b(\tau))} \), we cannot hope to pack more than \( \frac{2^n}{2^{hn(1-h_b(\tau))}} \) fan-outs in the binary output space resulting in the following fact.

**Fact. 1.** Consider Ex. 1 with average Hamming cost constraint \( \tau < \frac{1}{2} \). Any rate pair \((R_1, R_2)\) achievable by unstructured coding schemes satisfies \( R_1 + R_2 < uce\{\max\{0, 2h_b(\tau) - 1\}\} \) where \( uce\{f(\tau)\} \) denotes the upper convex envelope of the function \( f(\tau) \). See [19] for a proof.

We now present a linear coding scheme that can achieve any rate pair \((R_1, R_2)\) satisfying \( R_1 + R_2 < h_b(\tau) \). For simplicity, we describe achievability of the rate pair \((h_b(\tau), 0)\). Our coding scheme is identical to the unstructured coding scheme with two key differences. The first key difference is that the bins of each sender’s codebook are chosen to be cosets of a common linear code. Let \( \lambda_2 \) denote a linear code of rate \( 1 - h_b(\tau) \) whose cosets can quantize a uniform source to with an average Hamming distortion of \( \tau \). In other words, a uniformly and randomly chosen coset of \( \lambda_2 \) contains a codeword within an average Hamming distance of \( \tau \) of the observed state sequence \( \text{whp} \). See [20] or [3] for proof of existence. Since sender \( 2 \) has no message to transmit, it is provided with just \( \lambda_2 \) that serves as its only bin. Sender \( 1 \) is provided with all of the \( 2^{hn(1-h_b(\tau))} \) cosets of \( \lambda_2 \), each of which serves as its bins. The encoding is identical to that for unstructured coding.

The codebook of sender 2 when added to any bin of user 1’s code results in a coset of \( \lambda_2 \), and therefore contains at most \( 2^{hn(1-h_b(\tau))} \) codewords. Moreover, since \( U^n_2 \) lies in \( \lambda_2 \), user 1’s codeword \( U^n_1 \) and the received vector \( Y^n = U^n_1 \oplus U^n_2 \) lie in the same coset. The receiver can identify the coset from which sender 1 chose his \( U_1 \)—codeword and hence gather sender 1’s message. Since the channel is noiseless, sender 1 may employ all cosets of \( \lambda_2 \) and therefore communicate at rate \( h_b(\tau) \) which is larger than \( 2h_b(\tau) - 1 \) for all \( \tau \in (0, \frac{1}{2}) \).

**Case \( \theta \in (0, \frac{\pi}{4}) \):** The arguments in [19] can be used to prove that the optimal choice of parameters in Thm. 3 for this case too is \( U_1 = U_2 = \{0, 1\} \), \( p_{U_1, s_1}(0|0) = p_{U_2, s_2}(0|1) = \tau = 1 - p_{U_1, s_1}(0|0) = 1 - p_{U_2, s_2}(1|0) \) and \( X_1 = U_1 \oplus S_1 \) where \( \oplus \) denotes addition mod 2. This implies the quantum state corresponding to which we compute our information quantities is

\[
\sigma^{YS_1s_2x_1x_2u_1u_2} = \sum_{s_1, s_2} \frac{1}{4} \left( \frac{(1-\tau)^2}{4} \right) \left( |1, 1\rangle \langle 1, 1| + |0, 0\rangle \langle 0, 0| \right) \otimes |s_1, s_2\rangle \langle s_1, s_2| + \left( \frac{1-\tau^2}{4} \right) \left( |0, 0\rangle \langle 0, 0| \right) \otimes |s_1, s_2\rangle \langle s_1, s_2|.
\]

The bound on the sum rate achievable using IID random codes as stated in Thm. 3 is \( I(U_1 U_2; Y)_{\sigma} - I(U_1; S_1) - I(U_2; S_2)_{\sigma} \). In Appendix A we have provided characterization of the component quantum states with respect to which the above information quantities have to be computed. Referring to the same, it can be verified that \( I(U_1 U_2; Y)_{\sigma} - I(U_1; S_1) - I(U_2; S_2)_{\sigma} = \alpha - 2 + 2h_b(\tau) \) where

\[
\alpha = h_b(1 - 2\tau^2 \sin^2 \theta) - h_b(\sqrt{1 - 4\epsilon(1 - \epsilon)\sin^2 \theta}), \quad h_b(x) \triangleq h_b\left(\frac{1}{2} + \frac{x}{2}\right) \quad \text{and} \quad \epsilon = 2\tau(1 - \tau).
\]

It maybe verified that \( \alpha = 1 \) if \( \theta = 0 \) indicating the maximum sum rate achievable is a continuous function of \( \theta \) as one expects. In Prop. 3 we verify that the linear coding scheme achieves any rate pair satisfying \( R_1 + R_2 < uce\{\max\{0, \alpha - 1 + h_b(\tau)\}\} \) which strictly subsumes that achievable above.

Two important observations are in order. Firstly, since exponentially many pairs of codewords from \( \lambda_2 \) and the coset chosen by sender 1 have the same sum, the receiver cannot disambiguate the pair of codewords chosen by the two senders. It can only disambiguate the sum \( U^n_1 \oplus U^n_2 \). The second key difference in this coding scheme is that the receiver must not attempt to decode the pair, but instead decipher the message by decoding the sum of the two codewords.

**C. Sieving Relevant Information via Algebraic Closure**

The key difference between the structured and unstructured coding scheme is the decoding rule. While the former pins down the pair, the latter only decodes the sum, leaving uncertainty in the pair. Note that, the codeword \( u^n_j(m_j, s^n_j) \) chosen by sender \( j \) contains, in addition to the message, information about \( s^n_j \). By requiring the receiver to pin down the pair \( (u^n_j(m_j, s^n_j) : j \in [2]) \) of chosen codewords, the unstructured coding scheme is forcing the receiver to gather information of the state sequences that is not of value to it. Is there a function of \( (u^n_j(m_j, s^n_j) : j \in [2]) \) that, while containing information of the pair \( m_1, m_2 \) of messages can also suppress the amount of information of the pair \( s^n_1, s^n_2 \) and can the coding scheme enable the Rx decode this function efficiently? The structured coding scheme is enabling the Rx do this via the mod 2 function.
IV. INNER BOUND BASED ON UNION COSET CODES

Theorem 2. A rate-cost quadruple \((R_1, R_2)\) is achievable if there exists a finite field \(\mathcal{V}_1 = \mathcal{V}_2 = \mathcal{W} = \mathcal{F}_q\) and conditional PMFs \(p_{X_j, V_j | S_j}\) on \(X_j \times V_j\) for \(j \in [2]\) with respect to which

\[
R_1 + R_2 < \min \{ H(V_1 | S_1) : j \in [2] \} - H(V_1 \oplus q V_2 | Y) \tag{3}
\]

where all mutual informations are computed wrt the state

\[
\sigma^{X_1X_2} = \sum_{s_1, v_1, w_1, x_1} p_{S_1V_1W_1X_1}(s_1, v_1, w_1, x_1) \rho_{X_1} \otimes \rho_{V_1} \otimes \rho_{W_1} \otimes \rho_{X_1 \oplus q V_2} \text{ with }
\]

\[
p_{S_1V_1W_1X_1}(s_1, v_1, w_1, x_1) = p_S(s) \prod_{j=1}^{2} p_{X_j, V_j | S_j}(x_j, v_j | s_j) \mathbb{I}\{v_1 \oplus q v_2\},
\]

for all \((s, v, w, x) \in S \times V \times W \times X\).

Proof. We begin by outlining our techniques and identifying the new elements. The main novelty is in the code structure we design and the decoding POVM we propose. In Sec. IV-A we characterize a UCC and describe our codes. The Gelfand-Pinsker encoding (Sec. IV-B) is employed by both senders. We decode only the sum codeword and hence employ a single user decoding POVM (Sec. IV-C). Since we decode into a UCC obtained by adding two statistically correlated UCCs, our analysis is not a standard one and detailed in Sec. IV-D.

A. Code Structure

The gain in rates for Ex. 1 crucially relied on the bins of both codes being coset shifts of a common linear code, thereby ensuring that the size of the sum of any pair of bins was contained. We observe that the shifts can be arbitrary and there are no structural requirements on the union of these cosets. We are thus led to a UCC.

Defn. 3. A UCC built over \(\mathcal{F}_q\) is specified through a generator matrix \(g \in \mathcal{F}_q^{k \times n}\) and a map \(\iota : \mathcal{F}_q^{l} \rightarrow \mathcal{F}_q^{n}\) of coset shifts. The collection \(c(m) \triangleq \{v^n(a, m) = ag \oplus_q \iota(m)\}\) forms the bin corresponding to message \(m \in \mathcal{F}_q^{l}\) and the union \(\cup_m c(m)\) of bins forms the code. We refer to this as an \((n, k, l, g, \iota)\) UCC or an \((n, k, l, g, c)\) UCC.

We employ UCCs as the codebook for both senders. The symmetry in Ex. 1 permitted us to design codes of the same rate for both senders. In general, to enable codes of different rates, we propose a ‘nesting’ of the two UCCs. Without loss of generality, assume the size of sender 1’s bins is the smaller of the two. We equip user \(j\) with UCC \((n, k_j, l, g_j, \iota_j)\) and enforce \(g_2 = \begin{bmatrix} g_1^T & g_2^T \end{bmatrix}^T\). This ensures that the bins of user 1’s code are sub-cosets of the bins of user 2’s code, thus guaranteeing the desirable property mentioned prior to Defn. 3. Let \(\lambda_j \triangleq (v^n_j(a_j, m_j), a_j \oplus_q \iota_j(m_j) : (a_j, m_j) \in \mathcal{V}_j^k \times \mathcal{V}_j^l)\) denote the codebook of sender \(j\).

B. Encoding

Our encoding is identical to that described for unstructured codes in Sec. III-A. On observing message \(m_j \in \mathcal{Q}_j\) and state sequence \(s^n_j\), sender \(j\) looks for a codeword in \(c_j(m_j)\) that is jointly typical with \(s^n_j\). It finds at least one, one among these is chosen and denoted \(v^n_j(m_j, s^n_j)\). If it finds none, \(v^n_j(m_j, s^n_j)\) is set to a default codeword in \(c_j(m_j)\). The pair \((s^n_j, v^n_j(m_j, s^n_j))\) is mapped to an input sequence via a ‘fusion map’ \(f_j : \mathcal{S}_j^n \times \mathcal{V}_j^n \rightarrow \mathcal{X}_j^n\). For the sake of the ensuing analysis, we formalize this encoding with some notation.

Let \(\alpha_j(m_j, s^n_j) \triangleq \sum_{a_j} \mathbb{I}\{(v_j^n(a_j, m_j), s^n_j) \in T(a_j, s_j)\}\) be the number of available jointly typical codewords and let

\[
\mathcal{L}_j(m_j, s^n_j) \triangleq \begin{cases} \{a_j(v^n_j(a_j, m_j), s^n_j) \in T(a_j, s_j)\} & \text{if } \alpha_j(m_j, s^n_j) > 0 \\ \{0^n_j\} & \text{otherwise} \end{cases}
\]

For every pair \((m_j, s^n_j)\), \(a_j(m_j, s^n_j)\) is an element chosen from \(\mathcal{L}_j(m_j, s^n_j)\). We define \(v^n_j(m_j, s^n_j) \triangleq v^n_j(a_j(m_j, s^n_j), s^n_j)\). A predefined ‘fusion map’ \(f_j : \mathcal{S}_j^n \times \mathcal{V}_j^n \rightarrow \mathcal{X}_j^n\) is used to map the pair \(s^n_j, v^n_j(m_j, s^n_j)\) to an input sequence in \(\mathcal{X}_j^n\) henceforth denoted \(x^n_j(m_j, s^n_j)\).
C. Decoding POVM

Consider the UCC \((n, k_2, l_2, g_2, \tau_{\theta})\) where \(\tau_{\theta}(m) = \tau_1(m) \oplus_{q^l}(m_2)\) and let \(w^n(a, m) \triangleq a g_2 \oplus_{q^l} \tau_1(m) \oplus_{q^l} \tau_2(m_2)\) denote its codewords. Let \(\pi_{a,m}\) be the conditional typical projector of \(\otimes_{i=1}^n \rho_w(a,m)\) wrt the state \(\rho_w = \sum_{a,m} p_{X_1|X_0}^{n}(x)(\mathbb{E}_{x|w}(x), \mathbb{E}(w))\rho_{x,w}\) : \(w \in W\) where \(p_{X_1|X_0}^{n}\) is as defined in the Thm. statement. We define \(\gamma_{a,m} \triangleq \pi_m \pi_{a,m} \pi^Y\) where \(\pi^Y\) is the unconditional typical projector of the state \(\sum_{a,m} \rho_{x,y}^{n}(x,y)\). The decoding POVM is

\[
\lambda_{m} \triangleq \left( \sum_{a,m} \gamma_{a,m,n,m_2} \right)^{-\frac{1}{2}} \left( \sum_{a} \gamma_{a,m,n,m_2} \left( \sum_{\tilde{a},m_1,m_2} \gamma_{\tilde{a},m_1,m_2} \right)^{-\frac{1}{2}} \right)
\]

(4)

and \(\lambda_{-1} \triangleq I^{\otimes n} - \sum_{m} \lambda_{m}\).

D. Probability of Error Analysis

We begin our analysis by stating the distribution of the random code. Specifying \(g_1, g_{2/1}, \tau_j(m_j), a_j(m_j, s_j^{n}), x_j^n(m_j, s_j^{n}) : (m_j, s_j^{n}) \in [q^j] \times S_j^{n}\) completely specifies the code. A distribution for the random code is therefore specified through a distribution of these objects. We let upper case letters denote the corresponding random objects. \((G_2, G_{2/1}, \tau_j(m_j) : m_j \in [q^j] : j \in [2])\) are mutually independent and uniformly distributed on their respective range spaces. \(A_j(m_j, s_j^{n})\) is conditionally independent of the earlier mentioned objects given \(a_j(m_j, s_j^{n})\) and uniformly distributed in \(L(m_j, s_j^{n})\). Finally, given all of the earlier mentioned objects, \(X_j^n(m_j, s_j^{n}) \sim p_{X_j|V_j}^{n}(\cdot |V_j(m_j, s_j^{n}), s_j^{n})\).

The average probability of error is

\[
\zeta(\xi, \lambda) = \sum_{m} \zeta(m) \left| \mathcal{M} \right| \text{ where } \zeta(m) \triangleq \sum_{s_j^{n}} p_{s_j^{n}}^{n}(s_j^{n}) \zeta(m|s_j^{n})
\]

(5)

\[
\zeta(m|s_j^{n}) \triangleq \text{tr}((I - \lambda_m)\rho_{m,s_j^{n}})\rho_{m,s_j^{n}}^{\perp} \triangleq \bigotimes_{t=1}^{n} \rho_{x_t(m,s_j^{t}),x_2(m_2,s_2^{t})}^{\perp},
\]

where \(I = I^{\otimes n}\), \(\mathcal{M}_j = [q^j]\) and hence \(\left| \mathcal{M} \right| = q^{j_1+j_2}\). Henceforth, we focus on a generic term \(\zeta(m)\). Let \(a_{\theta} \triangleq a_1(m_1, s_1^{n}) 0^{j_2-k_1} \oplus a_2(m_2, s_2^{n})\) and \(E_j \triangleq \{a_j(m_j, s_j^{n}) \geq 1\}\). \(E \triangleq E_1 \cap E_2\). With these, we have,

\[
\zeta(m|s_j^{n}) \leq \tau_0 + \tau_1 + \tau_2 \text{ where } \tau_0 \triangleq \mathbb{I}_E^{\perp} + \mathbb{I}_{\xi_2}^{\perp}, \tau_1 = \text{tr}((I - \gamma_{a_{\theta},m})\rho_{m,s_j^{n}})\mathbb{I}_E, \tau_2 \triangleq \sum_{\tilde{a}_{\theta} \neq a_{\theta}} \sum_{\tilde{m}_{\theta} \neq m} \text{tr}(\gamma_{\tilde{a}_{\theta},\tilde{m}}\rho_{\tilde{m},s_j^{n}})\mathbb{I}_E
\]

(6)

where, we recall \(\gamma_{a_{\theta},m} = \pi^Y \pi_{a_{\theta},m} \pi^Y\) and \(\pi_{a_{\theta},m}\) is the conditional typical projector of \(\otimes_{i=1}^n \rho_w(a,m)\). The rest of our proof derives upper bounds on \(T_i \triangleq \sum_{s_j^{n}} p_{s_j^{n}}^{n}(s_j^{n}) \mathbb{E}(\xi_i)\) for \(i \in [3]\).

Upper bound on \(T_0\) : \(E_1, E_2\) are events involving only classical probabilities and we refer to [2] Lemma 7 in Appendix B for a proof of the following.

**Prop. 1.** For any \(\eta > 0\), \(\exists N_\eta \in \mathbb{N}\) such that \(\forall n \geq N(\eta)\), \(\mathbb{E}(T_0) \leq \exp\{-n\eta\} \text{ if } \frac{k_2 \log q}{n} > \log q - H(V_j|S_j)\) for \(j \in [2]\).

To comprehend the above bound, note that codewords of a random UCC are uniformly distributed. The expected number of codewords jointly typical with a typical state sequence \(s_j^{n}\) is \(|N(V_j|s_j^{n})|q^{j-n}\) whose exponent is \(k \log q - n \log q + nH(V_j|S_j)\). Prop. [1] guarantees the latter exponent is positive.

Upper bound on \(T_1\) : Since \(\tau_1\) involves the event \(E = E_1 \cap E_2\), an upper bound on \(T_1\) can be derived using pinching and gentle operator lemma. Since this is fairly straightforward we refer the reader to a subsequent version of this manuscript for details.

**Prop. 2.** For any \(\eta > 0\), there exists \(N_\eta \in \mathbb{N}\) such that for all \(n \geq N(\eta)\), \(T_2 \leq \exp\{-n\eta\}\) if

\[
\max_{j=1,2} \frac{k_j}{n} + \sum_{i=1}^{2} \frac{k_i + l_i}{n} < 3 \frac{H(W|Y)_{\sigma} - \sum_{i=1}^{2} H(V_i|S_i)_{\sigma}}{\log q}
\]

**Proof.** Proof is provided in Appendix B

By eliminating \(\frac{k_j}{n}, \frac{k_2 \log q}{n}\) from the bounds in Prop. [1] and [2] and equating \(R_j = \frac{l_j}{n} \log q\), we obtain the condition stated in the theorem statement.
Prop. 3. Consider Ex. 1 for \( \tau \in (0, \frac{1}{2}) \) and \( \theta = \frac{7}{8} \). The inner bound achievable via UCCs is strictly larger than that achievable via unstructured codes.

Proof. By choosing \( \mathcal{V}_1 = \mathcal{V}_2 = \mathcal{F}_2 \) the binary field and \( p_{X_j,V_j|S_j}(1,1+s_j|s_j) = \tau = 1 - p_{X_j,V_j|S_j}(0,s_j|s_j) \) for \( s_j \in \{0,1\} \) and \( j \in [2] \) and evaluating the inner bound in Thm. 2 it can be verified that any rate pair \((R_1,R_2)\) satisfying
\[
R_1 + R_2 < uce\{\max\{0,\alpha - 1 + h_b(\tau)\}\}
\]

is achievable where \( \alpha \) is as defined in (2). See Fig. 2 for plots of the rate regions \( R_1 + R_2 < uce\{\max\{0,\alpha - 1 + h_b(\tau)\}\} \) and \( R_1 + R_2 < uce\{\max\{0,\alpha - 2 + 2h_b(\tau)\}\} \) strictly larger than that achievable via IID and structured codes respectively to verify the latter is strictly larger.

V. Enhancing IID Coding Schemes via UCCs

The UCC based coding scheme can enable efficient decoding of \( \mathcal{V}_1 \oplus \mathcal{V}_2 \). On a QMSTx wherein the latter function contains the information of the pair of messages, the UCC coding scheme can outperform the use of unstructured codes. In general, the information corresponding to the message pair can be encoded in both univariate and bivariate functions of auxiliary RVs. A general coding scheme for QMSTx must therefore incorporate both unstructured codes and UCCs. We present the following inner bound that subsumes the inner bounds stated in Thms. 1, 2.

**Theorem 3.** A rate-cost \((\overline{R},\overline{\tau})\) quadruple is achievable if there exists finite sets \( U_1, U_2 \), a finite field \( \mathcal{V}_1 = \mathcal{V}_2 = \mathcal{W} = \mathcal{F}_q \) of size \( q \) and conditional PMFs \( p_{U_j,V_j|X_j,S_j} : j \in [2] \) wrt which
\[
R_j \leq I(U_j;U_2Y)_\sigma - I(U_j;S_j)_\sigma - H(W|Y|Y)_\sigma
\]
\[
\quad + \min\{H(V_1|U_1S_1)_\sigma, H(V_2|U_2S_2)_\sigma\}, \text{ for } j = 1, 2,
\]
\[
R_1 + R_2 \leq I(U;U_2Y)_\sigma - I(U;S)_\sigma - H(W|Y|Y)_\sigma
\]
\[
\quad + \min\{H(V_1|U_1S_1)_\sigma, H(V_2|U_2S_2)_\sigma\},
\]

where the above entropies are evaluated wrt the state
\[
\sigma_{UXUVWS}^{YXUVWS} \triangleq \sum_{X=S=W} p_{SUXUVWS}(x,s,u,v,w,z)\rho_{xx} \otimes |x_u \uplus v \uplus w s|, \quad p_{SUXUVWS}(x,s,u,v,w,z) = p_S(s)\prod_{j=1}^2 p_{X_jV_jU_j|S_j}(x_j,v_j,u_j|s_j)\mathbb{1}_{\{v_1 \uplus v_2 = v\}}.
\]

for all \((x,s,u,v,w,z) \in S \times V \times W \times X\).

By choosing \( \mathcal{V}_1 = \mathcal{V}_2 = \phi \), we can recover the inner bound achievable via IID codes in 1. By choosing \( U_1 = U_2 = \phi \), we can recover the inner bound in Thm. 2 thus proving that above inner bound subsumes all known inner bounds for a general QMSTx. We now outline the main elements of our proof and furnish details in a subsequent version of this manuscript. The code structure and the encoding is identical to the classical MAC with distributed states and is provided in 2. Decoding is based on a combination of joint and successive decoding. A joint decoding POVM is employed to decode into \( U_1,U_2 \). Following this, decoding of \( \mathcal{V}_1 \oplus \mathcal{V}_2 \) is performed on the collapsed state. We leverage an alternate form of the ‘overcounting trick’ that we have used in 10 to obtain the same pre-Fourier Motzkin bounds as those in 2 Proof of Thm. 5.
VI. COMMUNICATING OVER CLASSICAL-QUANTUM CHANNEL WITH RANDOM STATES USING UCCs

We begin with a formal description of a point-to-point classical quantum channel with classical random states available non-causally at the transmitter. We henceforth refer to this channel as a QSTx.

Consider a (generic) QSTx specified through (i) a finite input set $X$, (ii) a finite set $S$ of states, (iii) a PMF $p_S(\cdot)$ on $S$, (iii) a collection $(\rho_{xs} \in \mathcal{D}(\mathcal{H}_Y)) : (x, s) \in X \times S$ of density operators and (iv) cost function $\kappa : X \times S \rightarrow [0, \infty)$. The cost function is additive, i.e., having observed the state sequence $s^n$ the cost incurred by the sender in preparing the state $\otimes_{t=1}^n \rho_{x_t,s_t}$ is $\kappa(x, s^n) \triangleq \frac{1}{n} \sum_{t=1}^n \kappa(x_t, s_t)$. Reliable communication on a QSTx entails identifying a code.

**Defn. 4.** An $(n, M, e, \lambda)$ QSTx code consists of a message index set $M$, an encoder map $e : M \times S^n \rightarrow X^n$ with codewords denoted $(x^n(m, s^n) : 1 \leq t \leq n) : (m, s^n) \in M \times S^n$ and a decoder POVM $\lambda \triangleq \{ \lambda_m \in \mathcal{P}(\mathcal{H}_Y^n) : m \in M \}$. The average error probability of the code is

$$\xi(e, \lambda) \triangleq 1 - \frac{1}{|M|} \sum_{m \in M} \sum_{s^n \in S^n} p_S^n(s^n) \text{tr} \left( \lambda_m \rho_{x^n(m, s^n), s^n} \right) \text{ where } \rho_{x^n(m, s^n), s^n} = \bigotimes_{t=1}^n \rho_{x(m, s^n), s_t}.$$  

Average cost incurred by the sender in transmitting message $m$ is $\tau(e|m) \triangleq \sum_{s^n} p_S^n(s^n) \kappa(e(m, s^n), s^n)$ and the average cost incurred by the sender is $\tau(e) \triangleq \frac{1}{|M|} \sum_m \tau(e|m)$.

The object of interest is the capacity region of a QSTx defined below. In this section, we prove achievability of the current known largest single-letter inner bounds to the capacity region of a QSTx.

**Defn. 5.** A rate-cost quadruple $(R, \tau) \in [0, \infty)^2$ is achievable if there exists a sequence of QSTx codes $(n, M^{(n)}, e^{(n)}, \lambda^{(n)})$ for which

$$\lim_{n \rightarrow \infty} \frac{\tau(e^{(n)})}{n} = 0, \text{ and } \lim_{n \rightarrow \infty} n^{-1} \log M^{(n)} = R, \text{ and } \lim_{n \rightarrow \infty} \tau(e^{(n)}) \leq \tau.$$

The capacity region $\mathcal{C}$ of the QSTx is the set of all achievable rate-cost vectors and $\mathcal{C}(\tau) \triangleq \{ R : (R, \tau) \in \mathcal{C} \}$.

**Theorem 4.** Consider a QSTx characterized through a finite set $S$ of states, a PMF $p_S$ on $S$, modeling the distribution of the random state, an input set $X$ and a collection of density operators $(\rho_{xs} \in \mathcal{D}(\mathcal{H}_Y)) : (x, s) \in X \times S$. For $\tau > 0$, $R \in \mathcal{C}(\tau)$ if there exists a PMF $p_{S|X,Y|S}$ on $S \times Y \times X$ for which $\sum_{x,s} p_S(s)p_{X|S}(x|s)\kappa(x,s) \leq \tau$ and $R < I(V;Y) - I(V;S)$ where all information quantities are computed with respect to the quantum state

$$\sigma_{YSXV} \triangleq \sum_{x,s,v} p_S(s)p_{X|S}(v|x|s)\rho_{xs} \otimes |s x v\rangle\langle s x v|.$$  

(7)

**Proof.** The two new elements in our proof are the code structure (Sec. VI-A). Specifically, we build a union coset code to communicate over the QSTx. Since the codewords of a random union coset code are not mutually independent and are uniformly distributed, a standard information theoretic proof is not applicable. We therefore provide detailed steps in Sec. VI-B.

A. Code Structure

Let $\mathcal{V} = \mathcal{F}_q$ be a finite field of size $q$. Consider a $(n, k, l, g, t)$ UCC whose codewords are $(v^n(a, m) \triangleq ag\oplus_q t(m) : (a, m) \in \mathcal{V}_k \times \mathcal{V}_l)$ and the bin corresponding to message $m$ is the collection $c(m) \triangleq \{ ag\oplus_q t(m) : a \in \mathcal{V}_k \}$. As we describe in the sequel, the encoder observes the state sequence $s^n \in S^n$ and chooses a codeword in $c(m)$ where $m \in \mathcal{M}$ is the message that needs to communicated to the Rx.

B. Encoding

For every possible pair $(m, s^n)$ of message and state sequence, let

$$\alpha(m, s^n) \triangleq \sum_{a \in \mathcal{V}_k} 1_{\{ (v^n(a, m), s^n) \in T^n_{\tau}(p_{V|S}) \}}$$  

(8)

be the number of codewords in the bin indexed by the message that is jointly typical with the observed state sequence $s^n \in S^n$.

Let

$$\mathcal{L}(m, s^n) \triangleq \begin{cases} \{ a : (v^n(a, m), s^n) \in T^n_{\tau}(p_{V|S}) \} & \text{if } \alpha(m, s^n) \geq 1 \\ \{ 0^k \} & \text{otherwise, i.e., } \alpha(m, s^n) = 0. \end{cases}$$  

(9)

be a list of candidate code words that is available to the encoder for the message, state sequence pair $(m, s^n)$. Let $a_{m,s}^n$, be chosen from $\mathcal{L}(m, s^n)$ and $v^*(m, s^n) \triangleq v^n(a_{m,s}^n, m)$. A predefined ‘fusion map’ $f : S^n \times S \rightarrow \mathcal{X}^n$ is used to map the pair $s^n, v^*(m, s^n)$ to an input sequence in $\mathcal{X}^n$ henceforth denoted $x^n(m, s^n)$. On observing state sequence $s^n$ and message $m$, the encoder chooses state sequence $x^n(m, s^n) = (x(m, s^n)_t : 1 \leq t \leq n)$, and we define $\rho_{m,s^n} \triangleq \bigotimes_{t=1}^n \rho_{x(m, s^n)_t,s_t}$.
C. Decoding POVMs

Consider a PMF $p_{SYX} = p_{S|Y,X}$ on $S \times Y \times X$. Let

$$\rho \triangleq \sum_{x,s} p_{SX}(s,x)p_{xz} \quad \rho_v \triangleq \sum_{x,s} p_{XS|V}(x,s|v)p_{xz}$$

have spectral decompositions $\rho = \sum_{y \in Y} q(y)|f_y\rangle\langle f_y|$ and $\rho_v = \sum_{y \in Y} r_{v|Y}(y|v)|e_{y|v}\rangle\langle e_{y|v}|$

respectively. Let

$$\pi Y \triangleq \sum_{y^n \in Y^n} \bigotimes_{i=1}^n |f_{y_i}\rangle\langle f_{y_i}| \mathcal{I}\{y^n \in T^n_y(p_Y)\}$$

and $\pi_{v^n} \triangleq \sum_{y^n \in Y^n} \bigotimes_{i=1}^n |e_{y_i|v}\rangle\langle e_{y_i|v}| \mathcal{I}\{(v^n,y^n) \in T^n_{v,p_{v|Y}}(p_Y, r_{v|Y}(Y|v))\}$

be the unconditional and conditional typical projectors. For $(a, m) \in V^k \times Y^l$, let

$$\gamma_{a,m} \triangleq \pi Y \pi_{v^n(a,m)\pi Y} \text{ and } \lambda_m \triangleq \left( \sum_{a,\hat{m} \in Y^l} \gamma_{a,\hat{m}} \right)^{-\frac{1}{2}} \sum_{a \in Y^l} \sum_{\hat{m} \in Y^l} \gamma_{a,\hat{m}} \left( \sum_{\hat{a},\hat{m} \in Y^l} \gamma_{\hat{a},\hat{m}} \right)^{-\frac{1}{2}}$$

for $m \in [q^l]$ and $\lambda_{-1} = 1_{HY} - \sum_{m \in M} \gamma_m$.

and $\{\lambda_m : m \in M = \{q^l\}, \lambda_{-1}\}$ be the decoding POVM.

D. Error Probability

As is standard in information theory, we derive an upper bound on the error probability of the best code by averaging the error probability over an ensemble of codes. We begin by specifying the distribution of a random code in our ensemble. Note that a code is completely specified via (i) the generator matrix $g \in \mathbb{V}^k \times \mathbb{S}^n$, the map $\iota : \mathbb{V}^l \rightarrow \mathbb{S}^n$ and the collection $(a^*_{m,n} \in \mathbb{V}^k : (m, s^n) \in M \times S^n)$. The generator matrix $G$, the map $\iota$ and the collection $(A^*_{m,n} \in \mathbb{V}^k : (m, s^n) \in M \times S^n)$ of a random code are distributed with PMF

$$P \left( G = g, \iota(m) = d^n(m) \mid a^*_{m,n} = a(m, s^n) : (m, s^n) \in M \times S^n \right) = \frac{1}{q^n} \prod_{n \in \mathbb{V}^l} \prod_{\iota \in \mathbb{S}^n} \mathcal{I}\{(a(m, s^n) \in L(m, s^n))\} . \quad (12)$$

From (12), it can be verified that the generator matrix $G$ and the range of $(\iota(m) : m \in \mathbb{V}^l)$ are mutually independent and uniformly distributed in the respective range spaces. Moreover, for $(m, s^n) \in M \times S^n$ and any $a \in L(m, s^n)$, we note that

$$P \left( a^*_{m,n} = a(m, s^n) \right) = \frac{1}{q^n} \prod_{\iota \in \mathbb{S}^n} \mathcal{I}\{(m, s^n) \in L(m, s^n))\}, \quad (13)$$

a relation we shall opportune to use in our analysis. For a specific code, the average error probability of the code is

$$\overline{\xi}(e, \lambda) \triangleq \frac{1}{q} \sum_{m, s^n} \sum_{a \in \mathbb{S}^n} p^a_s(s^n) \text{ tr} \{ (I - \lambda_m) \rho_{m,s^n} \} \leq \gamma_0 \frac{1}{q} \sum_{m, s^n} \sum_{a \in \mathbb{S}^n} p^a_s(s^n) \text{ tr} \{ (I - \lambda_m) \rho_{m,s^n} \} \mathcal{I}\{ (m, s^n) \in L(m, s^n))\},$$

where

$$\gamma_0 \triangleq \frac{1}{q} \sum_{m, s^n} \sum_{a \in \mathbb{S}^n} p^a_s(s^n) \mathcal{I}\{ (m, s^n) \in L(m, s^n))\},$$

and $\lambda_m \geq (S + T)^{-\frac{1}{2}} S(S + T)^{-\frac{1}{2}}$ and the operator inequalities $0 \leq S \leq I, 0 \leq T$ hold. In breaking down the error event, we have considered the event $E_{L-\eta}$ and the choice of $L$ will be specified in due course. From the Hayashi Nagaoka inequality [21] [22] Lemma 16.4.1, we have

$$I_{HY} - \lambda_m \leq I_{HY} - (S + T)^{-\frac{1}{2}} S(S + T)^{-\frac{1}{2}} - 2(I - S) + 4(I - T) \quad \text{and hence } \overline{\xi}(e, \lambda) \leq \frac{\gamma_0}{q} - \frac{\gamma_1}{q} + \frac{\gamma_2}{q}$$

Let $T_i : 0 \leq i \leq 3$ denote these terms corresponding to a random code whose distribution is specified in [12]. In the sequel, we derive upper bounds for each of the four terms $T_0, T_1, T_2, T_2$ corresponding to the best code by evaluating upper bounds on $E \{ T_i \} : 0 \leq i \leq 3$.

Bound on $E \{ T_0 \}$: We note that $T_0$ concerns only the event that the encoder cannot find at least $2^{n(L-\eta)}$ codewords in the bin indexed by the message that is jointly typical with the observed state sequence. The analysis of this event involves only classical probabilities. Using a standard second moment method similar to that in [2] Lemma 7 in Appendix B] or [4] Lemma 8 in Appendix A. Employing these techniques, the following lemma can be proved.
Lemma 1. For every $\eta > 0$, there exists $N_\eta \in \mathbb{N}$ such that for all $n \geq N_\eta$, we have

$$E\{T_0\} \leq \exp \left\{ -n \left( \frac{k \log q}{n} - \log q - H(V|S) + L - \eta \right) \right\}. \quad (14)$$

Bound on $E\{T_1\}$: For a specific code, we have $t_1 = t_{11} + t_{12}$, where

$$t_{11} \triangleq \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \text{tr} \left( [I - \gamma_{a,m,s^n}] \rho_{m,s^n} \right) \mathbb{I} \left\{ \alpha(m,s^n) \geq 2^{n(l-n)} \right\} T_n^r(p_{SV}),$$

$$t_{12} \triangleq \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \text{tr} \left( [I - \gamma_{a,m,s^n}] \rho_{m,s^n} \right) \mathbb{I} \left\{ \alpha(m,s^n) \geq 2^{n(l-n)} \right\} T_n^r(p_{X|VS} s^n, v^*(m,s^n)) \bigcup \bigcup_{k \in \mathbb{N}} T_n^r(p_{X|SV} s^n, v^*(m,s^n)).$$

A bound on $E\{T_{11}\}$ can be derived using standard bounds on typical sequences. Indeed, since $X^n(m,s^n)$ is conditionally picked with $\prod p_{X|Y:V} (v^*(m,s^n), s^n)$, the probability that it is not conditionally typically falls exponentially. In the following, we indicate how we break up $t_{12}$ and indicate how each term in corresponding breakup can be bounded.

**Bound on $E\{T_{12}\}$**: We have

$$t_{12} \leq \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \text{tr} \left( [I - \pi^Y \pi_{x^n} \pi^Y] \rho_{x^n,s^n} \right) \mathbb{I} \left\{ a_{m,s} = a, v^n(m,a) = v^n, x^n(m,s^n) = x^n \right\} \leq \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \text{tr} \left( [I - \pi^Y \pi_{x^n} \pi^Y] \rho_{x^n,s^n} \right) \mathbb{I} \left\{ v^n(m,a) = v^n, x^n(m,s^n) = x^n \right\} = t_{121} - t_{122}$$

$$t_{121} \triangleq \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \mathbb{I} \left\{ v^n(m,a) = v^n, x^n(m,s^n) = x^n \right\}$$

$$t_{122} \triangleq \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \mathbb{I} \left\{ v^n(m,a) = v^n, x^n(m,s^n) = x^n \right\}.$$

A lower bound on $E\{T_{122}\}$ can be derived using gentle operator lemma and pinching. Specifically, we have

$$E\{T_{122}\} = \frac{2}{q^{l+1}} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \text{tr} \left( [\pi^Y \pi_{x^n} \pi^Y] \rho_{x^n,s^n} \right) P \left( v^n(m,a) = v^n, x^n(m,s^n) = x^n \right)$$

$$= \frac{2}{q^{l+1}} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \text{tr} \left( [\pi^Y \pi_{x^n} \pi^Y] \rho_{x^n,s^n} \pi^Y \right) p_{X|VS} (x^n|v^n, s^n)$$

$$\geq \frac{2}{q^{l+1}} \sum_{m=1}^M \sum_{s^n} \sum_{a,m,s^n} p_n^m(s^n) \left[ \text{tr} (\pi_{x^n} \rho_{x^n,s^n} \pi^Y) - \| \pi^Y \rho_{x^n,s^n} \pi^Y - \rho_{x^n,s^n} \|_1 \right] p_{X|VS} (x^n|v^n, s^n). \quad (15)$$

The first term on the RHS of (15) can be lower bounded by the pinching lemma [22, Property 15.2.7] and the second term can be upper bounded via gentle operator lemma [22, Lemma 9.4.2]. We now proceed to $E\{T_{11}\}$

**Bound on $t_{11}$**:

$$t_{11} \leq \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} p_n^m(s^n) \mathbb{I} \left\{ (s^n, v^*(m,s^n)) \in T_n^r(p_{SV}), x^n(m,s^n) \notin T_n^r(p_{X|SV}|s^n, v^*(m,s^n)) \right\} \quad \text{and}$$

$$t_{11} = \frac{2}{q^l} \sum_{m=1}^M \sum_{s^n} p_n^m(s^n) \mathbb{I} \left\{ (s^n, v^*(m,s^n)) \notin T_n^r(p_{SV}), x^n(m,s^n) \in T_n^r(p_{X|SV}|s^n, v^*(m,s^n)) \right\} \quad \text{and}$$
In the sequel, we compute upper bound on \( \mathbb{E}\{T_{12}\} \) and lower bound on \( \mathbb{E}\{\overline{T}_{12}\} \). We begin with the latter. We have

\[
\mathbb{E}\{\overline{T}_{12}\} = \frac{2}{q^2} \sum_{m} \sum_{s^n} \sum_{(x^n,s^n)} \overline{P}_{S}(s^n) \text{tr}\left( \pi_Y \pi_{v^n} \pi_Y \rho_{x^n,s^n} \right) P(X^n(m, s^n) = x^n, V^* (m, s^n) = v^n)
\]

\[
= \frac{2}{q^2} \sum_{m} \sum_{s^n} \sum_{(x^n,s^n)} \overline{P}_{S}(s^n) \text{tr}\left( \pi_Y \pi_{v^n} \pi_Y \rho_{x^n,s^n} \right) p_{X|V}(x^n | v^n, s^n) P(V^* (m, s^n) = v^n)
\]

\[
\geq \frac{2}{q^2} \sum_{m} \sum_{s^n} \sum_{(x^n,s^n)} \overline{P}_{S}(s^n) \text{tr}\left( \pi_Y \pi_{v^n} \pi_Y \rho_{x^n,s^n} \right) p_{X|V}(x^n | v^n, s^n) P(V^* (m, s^n) = v^n)
\]

(17)

**Bound on \( \mathbb{E}\{T_{21}\} \):** Before we study \( \mathbb{E}\{T_{21}\} \), we begin by noting that

\[
\tau_{21} = \frac{4}{q^2} \sum_{m} \sum_{s^n} \sum_{a \neq a_{m,s}^*} \overline{P}_{S}(s^n) \text{tr}(\gamma_{a,m} \rho_{m,s^n}) \mathbb{1}_{\mathcal{E}_{L-n}} = \frac{4}{q^2} \sum_{m} \sum_{s^n} \sum_{a \neq a_{m,s}^*} \overline{P}_{S}(s^n) \text{tr}(\pi_Y \pi_{v^n} \pi_Y \rho_{x^n,s^n}) \mathbb{1}_{\mathcal{E}_{L-n}}
\]

(18)

\[
= \frac{4}{q^2} \sum_{m} \sum_{s^n} \sum_{a \neq a_{m,s}^*} \overline{P}_{S}(s^n) \text{tr}(\pi_Y \pi_{v^n} \pi_Y \rho_{x^n,s^n}) \mathbb{1}_{\{ \alpha(m, s^n) \geq 2^{n(L-\eta)}, a_{m,s}^* = a, v^n(a, m) = v^n \}}
\]

(19)

\[
\geq \frac{4}{q^2} \sum_{m} \sum_{s^n} \sum_{a \neq a_{m,s}^*} \overline{P}_{S}(s^n) \text{tr}(\pi_Y \pi_{v^n} \pi_Y \rho_{x^n,s^n}) \mathbb{1}_{\{ \alpha(m, s^n) \geq 2^{n(L-\eta)}, a_{m,s}^* = a, v^n(a, m) = v^n, \hat{v}^n \in T_\eta(p_{V^n}) \}}
\]

(20)

where (i) \( \rho_{m,s^n} = \bigotimes_{n=1}^{n} \rho_{x(m,s^n),s} \) is as defined earlier, (ii) (19) follows by summing over all possible choices for the corresponding codewords, (iii) (20) holds for \( L \geq \eta \) since the encoding rule guarantees \( a_{m,s}^* \in \mathcal{L}(m, s^n) \) and the latter set defined in (9) contains indices corresponding to codewords that are jointly typical with the observed state sequence whenever \( \alpha(m, s^n) \geq 1 \) and (iv) (20) is true since, as defined in (11), \( \pi_{v^n} \) is the zero projector if \( \hat{v}^n \notin T_\eta(p_{V^n}) \). This implies

\[
\mathbb{E}\{T_{21}\} = \frac{4}{q^2} \sum_{m} \sum_{s^n} \sum_{a \neq a_{m,s}^*} \overline{P}_{S}(s^n) \text{tr}(\pi_Y \pi_{v^n} \pi_Y \rho_{x^n,s^n}) P\left( \alpha(m, s^n) \geq 2^{n(L-\eta)}, a_{m,s}^* = a, v^n(a, m) = v^n, \hat{v}^n \in T_\eta(p_{V^n}) \right)
\]

(21)

For \( (v^n, s^n) \in T_\eta(p_{V^n}) \) and \( a \neq a \), we have

\[
P\left( \alpha(m, s^n) \geq 2^{n(L-\eta)}, a_{m,s}^* = a, V^n(\hat{a}, m) = \hat{v}^n, X^n(m, s^n) = x^n, \right) = P\left( V^n(a, m) = v^n, \hat{v}^n, X^n(\hat{a}, m) = \hat{v}^n, \right) P\left( \alpha(m, s^n) \geq 2^{n(L-\eta)} \right)
\]

(22)

\[
x P\left( a_{m,s}^* = a, V^n(\hat{a}, m) = \hat{v}^n, X^n(m, s^n) = x^n, \right) \leq \frac{1}{q^{2n}} \cdot \frac{1}{\alpha(m, s^n)} P_{X|SV}(x^n | s^n, v^n) \mathbb{1}_{\{ \alpha(m, s^n) \geq 2^{n(L-\eta)} \}} \leq \frac{1}{q^{2n}} \cdot \frac{1}{\alpha(m, s^n)} P_{X|SV}(x^n | s^n, v^n) \mathbb{1}_{\{ \alpha(m, s^n) \geq 2^{n(L-\eta)} \}} \leq \frac{2^{n(H(V)+3n)} P_{X|SV}(x^n | s^n, v^n) \mathbb{1}_{\{ \alpha(m, s^n) \geq 2^{n(L-\eta)} \}}}{q^{2n} 2^{n(L-\eta)}}
\]

(23)

where the first inequality in (23) follows the fact that codewords of a UCC are pairwise independent and uniformly distributed \( [3] \) and the second inequality in (23) follows from standard bounds on conditional probability of jointly typical sequences.
Substituting the bound in the RHS of (23) in (21), we have
\[
E(T_{21}) \leq \frac{4 \cdot 2^{n(H(V|S) + 3q)}}{q^{l+2n} \cdot 2^{n(L - \eta)}} \sum_{m} \sum_{\ell} \sum_{a, \hat{a} \in V_k} \sum_{\alpha \in T^n_{\eta}(pv)} \sum_{x^n \in X^n} \text{tr}(\pi^n \pi_x^n \pi^Y p_{XV} S(x^n, v^n, s^n) \rho_{x^n, s^n})
\]
\[
\leq \frac{4 \cdot 2^{n(H(V|S) + 3q)}}{q^{l+2n} \cdot 2^{n(L - \eta)}} \sum_{m} \sum_{\ell} \sum_{a, \hat{a} \in V_k} \sum_{\alpha \in T^n_{\eta}(pv)} \sum_{x^n \in X^n} \text{tr}(\pi^n \pi_x^n \pi^Y \rho_{x^n, s^n}^Y)
\]
\[
\leq \frac{4 \cdot 2^{n(H(V|S) + 3q)}}{q^{l+2n} \cdot 2^{n(L - \eta)}} \sum_{m} \sum_{\ell} \sum_{a, \hat{a} \in V_k} \sum_{\alpha \in T^n_{\eta}(pv)} \sum_{x^n \in X^n} \text{tr}(\pi^n \pi_x^n \pi^Y \rho_{x^n, s^n}^Y)
\]
\[
\leq \frac{4 \cdot 2^{n(H(V|S) - H(Y) + 6q)}}{q^{l+2n} \cdot 2^{n(L - \eta)}} \sum_{m} \sum_{\ell} \sum_{a, \hat{a} \in V_k} \sum_{\alpha \in T^n_{\eta}(pv)} \sum_{x^n \in X^n} \text{tr}(\pi^n \pi_x^n \pi^Y)
\]
\[
\leq \frac{4 \cdot 2^{n(H(V|S) - H(Y) + 6q)}}{q^{l+2n} \cdot 2^{n(L - \eta)}} \sum_{m} \sum_{\ell} \sum_{a, \hat{a} \in V_k} \sum_{\alpha \in T^n_{\eta}(pv)} \sum_{x^n \in X^n} 1
\]
\[
\leq \exp\left\{ -n \left( L - \frac{k \log q}{n} - \log q + H(V|S) + \log q - H(V|Y) - \frac{k \log q}{n} \right) \right\}
\]
where (24) follows from the operator inequality
\[
\sum_{\ell} \sum_{a, \hat{a} \in V_k} \sum_{x^n \in X^n} p_{XV} S(x^n, v^n, s^n) \rho_{x^n, s^n} \leq \sum_{x^n \in X^n, x^n \in X^n, v^n \in V^n} p_{XV} S(x^n, v^n, s^n) \rho_{x^n, s^n} = \rho_{x^n, s^n}^Y
\]
which follows from the positivity of the density operators. (25) follows from the operator inequalities \(\pi^n \rho_{x^n, s^n}^Y \leq 2^{-n(H(Y) - 3q)} \pi^n\) [22, Property 15.1.3] and \(\pi^n \leq I\). (26) follows from \(\text{tr}(\pi^n v^n) \leq 2^{n(H(V|Y) + 3q)}\) for \(v^n \in T^n_{\eta}(pv)\) [22, Property 15.1.2] and \(|T^n_{\eta}(pv)| \leq 2^{n(H(V|Y) + 3q)}\) and the last bound (27) follows by collating all exponents.

**Bound on \(E(T_{22})\)**: Our analysis of \(E(T_{22})\) is very similar to \(E(T_{21})\). The only difference between these analyses stems from the fact that the legitimate codeword \(V^n(a_{m,n}^*, s^n, m)\) and an incorrect codeword in the same bin \(V^n(\tilde{a}, m)\) are not statistically independent, however the legitimate codeword \(V^n(a_{m,n}^*, s^n, m)\) and any codeword in a different bin \(V^n(\tilde{a}, \tilde{m})\) for \(\tilde{m} \neq m\) are statistically independent. This suggests that we can derive the bounds without having to condition on the realization of \(a_{m,n}^*\) as in (22) - (23). Except for this minor difference, the rest of the analysis provided below is identical. We have
\[
t_{22} = \frac{4}{q^l} \sum_{m, \tilde{m}, m \neq \tilde{m}} \sum_{s^n} \sum_{a, \tilde{a} \in V_k} p^n_{S}(s^n) \text{tr}(\gamma_{\tilde{a}, \tilde{m}} \rho_{m,s^n}) \mathbb{I}_{E_{L - \eta}} = \frac{4}{q^l} \sum_{m, \tilde{m}, m \neq \tilde{m}} \sum_{s^n} \sum_{a, \tilde{a} \in V_k} p^n_{S}(s^n) \text{tr}(\pi^n \pi_v^n(\tilde{a}, \tilde{m}, a, m) \pi^Y \rho_{m,s^n}) \mathbb{I}_{E_{L - \eta}}
\]
\[
= \frac{4}{q^l} \sum_{m, \tilde{m}, m \neq \tilde{m}} \sum_{s^n} \sum_{a, \tilde{a} \in V_k} p^n_{S}(s^n) \text{tr}(\pi^n \pi_v^n(\tilde{a}, \tilde{m}, a, m) \pi^Y \rho_{m,s^n}) \mathbb{I}_{\{\alpha(m, s^n) \geq 2^{n(L - \eta)}, V^*(m, s^n) = v^n, v^n(\tilde{a}, \tilde{m}) = \hat{v}^n, x^n(m, s^n) = x^n\}}
\]
\[
= \frac{4}{q^l} \sum_{m, \tilde{m}, m \neq \tilde{m}} \sum_{s^n} \sum_{a, \tilde{a} \in V_k} p^n_{S}(s^n) \text{tr}(\pi^n \pi_v^n(\tilde{a}, \tilde{m}, a, m) \pi^Y \rho_{x^n, s^n}) \mathbb{I}_{\{\alpha(m, s^n) \geq 2^{n(L - \eta)}, V^*(m, s^n) = v^n, v^n(\tilde{a}, \tilde{m}) = \hat{v}^n, x^n(m, s^n) = x^n\}}
\]
where as earlier, (i) \(\rho_{m,s^n} = \bigotimes_{t=1}^{n} \rho_{x^n, s^n}, s^n\), (ii) (29) follows by summing over all possible choices for the corresponding codewords, (iii) (30) holds for \(L \geq \eta\) since the encoding rule guarantees \(a_{m,n}^* \in \mathcal{L}(m, s^n)\) and the latter set defined in \(9\) contains indices corresponding to codewords that are jointly typical with the observed state sequence whenever \(\alpha(m, s^n) \geq 1\) and (iv) (30) is true since, as defined in (11), \(\pi_{v^n}\) is the zero projector if \(\hat{v}^n \notin T^n_{\eta}(pv)\). This implies
\[
E(T_{22}) = \frac{4}{q^l} \sum_{m, \tilde{m}, m \neq \tilde{m}} \sum_{s^n} \sum_{a, \tilde{a} \in V_k} p^n_{S}(s^n) \text{tr}(\pi^n \pi_v^n(\tilde{a}, \tilde{m}, a, m) \pi^Y \rho_{x^n, s^n}) \mathbb{I}_{\{\alpha(m, s^n) \geq 2^{n(L - \eta)}, V^*(m, s^n) = v^n, v^n(\tilde{a}, \tilde{m}) = \hat{v}^n, x^n(m, s^n) = x^n\}}
\]
\[
= \sum_{s^n} \sum_{a, \tilde{a} \in V_k} p^n_{S}(s^n) \text{tr}(\pi^n \pi_v^n(\tilde{a}, \tilde{m}, a, m) \pi^Y \rho_{x^n, s^n}) \mathbb{I}_{\{\alpha(m, s^n) \geq 2^{n(L - \eta)}, V^*(m, s^n) = v^n, v^n(\tilde{a}, \tilde{m}) = \hat{v}^n, x^n(m, s^n) = x^n\}} \leq \frac{2^n(H(V|S) + 3q)}{q^{k+2n}2^{n(L - \eta)}}.
\]
where follows from the same set of arguments that got us from (22) to (23). Substituting the above upper bound in (31), we have

$$
\mathbb{E}[T_{22}] \leq \frac{4 \cdot 2^{n(H(V|S)+3\eta)}}{q^{-k+l+2n}} \sum_{m, m \neq m, m, \neq m} \sum_{\phi^0 \in T^n_\eta(p_V)} \sum_{a} \sum_{\phi^0 \in T^n_\eta(p_V)} \sum_{x^n \in X^n} \text{tr}(\pi^{Y_0} \rho^{\otimes n}) 
\leq \frac{4 \cdot 2^{n(H(V|S)+3\eta)}}{q^{-k+l+2n}} \sum_{m, m \neq m, m, \neq m} \sum_{\phi^0 \in T^n_\eta(p_V)} \sum_{a} \sum_{\phi^0 \in T^n_\eta(p_V)} \sum_{x^n \in X^n} \text{tr}(\pi^{Y_0} \rho^{\otimes n}) \quad (33)
$$

which follows from the positivity of the density operators, (34) follows from the operator inequalities $\pi^{Y_0} \rho^{\otimes n} \rho^{\otimes n} \leq 2^{n[H(Y|S)+3\eta]} \pi^{Y_0}$ [22], Property 15.1.3 and $\pi^{Y_0} \leq I$, (35) follows from $\text{tr}(\pi^{Y_0}) \leq 2^n[H(Y|V)+3\eta]$ for $\phi^{n} \in T^n_\eta(p_V)$ [22], Property 15.1.2 and $|T^n_\eta(p_V)| \leq 2^n[H(V|S)]$ and the last bound (36) follows by collating all exponents.

**E. Collating Bounds and Characterization of a Single-letter achievable Rate Region**

Through the above analysis, we have proved that for every choice of a finite field $\mathcal{V} = \mathbb{F}_q$ and a PMF $p_{SVX}$ on $\mathcal{S} \times \mathcal{V} \times \mathcal{X}$, there exists a code of block length $n$ specified through an encoder $e$, a decoding POVM $\lambda$ consisting of $q^l$ codewords with error probability

$$
\bar{\xi}(e, \lambda) \leq \exp \left\{ -n \left( \frac{k \log q}{n} - \log q + H(V|S) + L - \eta \right) \right\}
$$

if $L \geq \eta > 0$. By choosing $L \triangleq \frac{k \log q}{n} - \log q + H(V|S) - 4\eta$ we can guarantee $\bar{\xi}(e, \lambda) \leq 3 \exp \{-n\eta\}$ if

$$
\frac{k \log q}{n} - \log q + H(V|S) > 5\eta > 0 \quad \text{and} \quad \frac{(k+l) \log q}{n} < \log q - H(V|Y) \quad (37)
$$

where are information quantities computed with respect to the state defined in (7). We therefore choose

$$
\frac{k \log q}{n} = \log q - H(V|S) + 5\eta \quad \text{and} \quad \frac{l \log q}{n} > H(V|S) - H(V|Y) - 5\eta = I(V;Y) - I(V;S) - 5\eta \quad (38)
$$

and guarantee $\bar{\xi}(e, \lambda) \leq 3 \exp \{-n\eta\}$. This completes the proof.

**APPENDIX A**

**Characterization of the Quantum States in Evaluation of Information Quantities for Ex. 1**

Consider Ex. 1 for $\theta \in (0, \frac{\pi}{2})$. In this appendix, we provide characterization of the quantum state in (1) for the choice $U_1 = U_2 = \{|0, 1\}, p_{U_1|S_1}(|0) = p_{U_2|S_1}(|0) = 1 - p_{U_1|S_1}(|1) = 1 - p_{U_2|S_1}(|1)$ and $X_j = U_j \oplus S_j$ for $j \in [2]$, where $\oplus$ denotes addition mod$-2$. The characterizations below enable us to compute the information quantities and thereby quantify
where

$$\sigma_{YS, X, Z, U_1, U_2} = \sum_{s_1, s_2} \frac{\tau(1 - \tau)}{4} \left[ |s_1 s_2 1 \oplus s_2 s_1 1 \oplus s_2| \right] |1| + \left[ |s_1 s_2 1 s_2| \right] \otimes [0 1 s_2 | 1 s_1 1 \oplus s_2] + \left[ |1 0 1 s_1 1 | 1 0 1 \oplus s_2| \right].$$

Partial tracing over the appropriate component systems, we have

$$\sigma_{S, U_1, U_2} = \sum_{s_1, s_2} \frac{\tau(1 - \tau)}{4} \left[ \right] |s_1 s_2 1 \oplus s_2 s_1 1 \oplus s_2| \left[ \right] \otimes [s_1 s_2 1 s_2|1|1]|1 \oplus s_2| \left[ \right] \otimes [1 1 1 \oplus s_2|1 1 1 \oplus s_2|1 1 1 \oplus s_2|1 1 1 \oplus s_2|1 1 1 \oplus s_2].$$

where $\epsilon = 2\tau(1 - \tau)$. 

**APPENDIX B**

**PROOF OF PROP. 2: BOUND ON T2**

We begin by defining events

$$\mathcal{F}_1 \triangleq \left\{ V_n^{i, j} = v_n^{i, j} \in [2], w_n^{i, j} = v_n^{i, j} \right\}, \mathcal{F}_2 \triangleq \left\{ A_j = v_n^{i, j} \right\}, \mathcal{F}_3 \triangleq \left\{ X_n^{i, j} \in T_n(p), \sigma_n^{i, j} \in T_n(p) \right\}, \omega \triangleq \left\{ \frac{w_n^{i, j}}{w_n^{i, j}} \right\}. $$

From the definition of $a_\oplus$ and the distribution of the random code, we have

$$P(F_1 \cap F_2 \cap F_3) \leq P(F_1) P(F_2 | F_1) P(F_3 | F_1 \cap F_2) \mathbb{I}_{\beta} \mathbb{I}_{\omega} \leq \frac{1}{q^{3n_2}} P_S(\mathbb{S}_n) \sum_{j=1}^{2} P_{X_j} | V_j S_j (x_n^{i, j}, v_n^{i, j}) \mathbb{I}_{\beta} \mathbb{I}_{\omega} \leq \frac{2n(H(V_1 | S_1) + 2\eta)}{q^{3n_2 - n(H(V_2 | S_2))}} \sum_{j=1}^{2} P_{X_j} | V_j S_j (x_j^{i, j}, v_j^{i, j}) \mathbb{I}_{\beta} \mathbb{I}_{\omega} \leq \Theta P_{S(VX)}(\mathbb{S}_n, \mathbb{S}_n) \mathbb{I}_{\beta} \mathbb{I}_{\omega} \leq \frac{2n(H(V_1 | S_1) + 2\eta)}{q^{3n_2 - n(H(V_2 | S_2))}} \sum_{j=1}^{2} P_{X_j} | V_j S_j (x_j^{i, j}, v_j^{i, j}) \mathbb{I}_{\beta} \mathbb{I}_{\omega}$$

where $\Theta \triangleq \frac{2n(H(V_1 | S_1) + 2\eta)}{q^{3n_2 - n(H(V_2 | S_2))}}$. 

For the choice of parameters stated earlier, the quantum state in (1) is
where \(\Theta\) follows from the property of a uniformly distributed UCC proven in [2], Lemma 9 in Appendix E. \(\Theta\) follows from the presence of \(\mathbb{I}_\beta\) in the factors. The term corresponding to \(T_2\) from \(\Theta\) in \(\mathbb{E}(\xi(x, \lambda))\) is

\[
\sum_{\mathbf{z}^n} p_\mathbf{z}(\mathbf{z}^n) \mathbb{E}(\{T_2\}) = \sum_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{w}^n, \mathbf{w}^n} \left( \sum_{\mathbf{z}^n} p^n_{\mathbf{Y}^n}(\mathbf{z}^n, \mathbf{w}^n) \rho_{\mathbf{z}^n, \mathbf{w}^n} \rho_{\mathbf{w}^n} \right) \mathbb{I}_\beta \mathbb{I}_\omega
\]

\[
\leq \Theta \sum_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{w}^n, \mathbf{w}^n} \left( \sum_{\mathbf{z}^n} p^n_{\mathbf{Y}^n}(\mathbf{z}^n, \mathbf{w}^n) \rho_{\mathbf{z}^n, \mathbf{w}^n} \right) \mathbb{I}_\omega \left( \pi_Y \pi_{\mathbf{w}^n} \mathbf{Y} \rho_{\mathbf{w}^n} \right)
\]

\[
\leq \Theta \sum_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{w}^n, \mathbf{w}^n} \left( \sum_{\mathbf{z}^n} p^n_{\mathbf{Y}^n}(\mathbf{z}^n, \mathbf{w}^n) \rho_{\mathbf{w}^n} \right) \mathbb{I}_\omega \left( \pi_Y \pi_{\mathbf{w}^n} \mathbf{Y} \rho_{\mathbf{w}^n} \right)
\]

\[
\leq \Theta \sum_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{w}^n, \mathbf{w}^n} \left( \sum_{\mathbf{z}^n} p^n_{\mathbf{Y}^n}(\mathbf{z}^n, \mathbf{w}^n) \mathbb{I}_\omega \left( \pi_Y \pi_{\mathbf{w}^n} \mathbf{Y} \rho_{\mathbf{w}^n} \right) \right)
\]

\[
\leq \Theta \sum_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{w}^n, \mathbf{w}^n} \left( \sum_{\mathbf{z}^n} p^n_{\mathbf{Y}^n}(\mathbf{z}^n, \mathbf{w}^n) \mathbb{I}_\omega \left( \pi_Y \pi_{\mathbf{w}^n} \mathbf{Y} \rho_{\mathbf{w}^n} \right) \right)
\]

\[
\leq \Theta \frac{2nH(Y)_o}{n} \sum_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{w}^n} \left( \mathbb{I}_\omega \left( \pi_Y \pi_{\mathbf{w}^n} \mathbf{Y} \rho_{\mathbf{w}^n} \right) \right)
\]

\[
\leq \exp \left\{ -n \left( 3 \log q - H(W|Y)_o + \sum_{i=1}^2 H(U_i|S_i)_o - \frac{k_1 + 2k_2 + l_1 + l_2}{n} \log q - 8\eta \right) \right\}
\]

where \(\Theta\) follows from substituting the upper bound \(\Theta\). \(\Theta\) follows from averaging the density operators and the fact that density operators are positive. \(\Theta\) follows again by averaging and cyclicality of the trace. \(\Theta\) follows from the operator inequality \(\pi_Y \rho_{\mathbf{w}^n} \mathbf{Y} \leq 2^{-n(H(Y|W)_o+6\eta)}\) and the fact that for typical \(\mathbf{w}^n\), we have \(\mathbb{I}_\omega \left( \pi_Y \pi_{\mathbf{w}^n} \mathbf{Y} \right) \leq 2^{nH(Y|W)_o+2n\eta}\) and the last inequality follows by substituting the value of \(\Theta\) from \(\Theta\). We obtained the above bound on \(\frac{k_1 + 2k_2 + l_1 + l_2}{n} \log q\) since we have assumed \(k_2 \geq k_1\). In general, we obtain the bound

\[
\sum_{\mathbf{z}^n} p_\mathbf{z}(\mathbf{z}^n) \mathbb{E}(\{T_2\}) \leq \exp \left\{ -n \left( 3 \log q - H(W|Y)_o + \sum_{i=1}^2 H(U_i|S_i)_o - \frac{k_1 + k_2 + \max\{k_1, k_2\} + l_1 + l_2}{n} \log q - 8\eta \right) \right\}
\]

**REFERENCES**

[1] S. I. Gel’fand and M. S. Pinsker, “Capacity of a broadcast channel with one deterministic component,” Probl. Pered. Inform., vol. 16, no. 1, pp. 24–34, Jan.–Mar. 1980.; translated in Probl. Inform. Transm., vol. 16, no. 1, pp. 17-25, Jan.–Mar. 1980.

[2] A. Padakandla and S. S. Pradhan, “An Achievable Rate Region Based on Coded Access Channels With States,” IEEE Transactions on Information Theory, vol. 63, no. 10, pp. 6393–6415, Oct. 2017.

[3] 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

[4] A. Padakandla, A. G. Sahebi, 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.

[5] ———, “Computing Sum of Sources over a Classical-Quantum MAC,” in 2021 IEEE International Symposium on Information Theory (ISIT), 2021, pp. 414–419.

[6] 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.

[7] B. Nazer and M. Gastpar, “Computation over multiple-access channels,” IEEE Transactions on Information Theory, vol. 53, no. 10, pp. 3498–3516, 2007.

[8] A. Padakandla and S. S. Pradhan, “Achievable Rate Region for Three User Discrete Broadcast Channel Based on Coded Codes,” IEEE Transactions on Information Theory, vol. 64, no. 4, pp. 2267–2279, April 2018.

[9] A. Padakandla, A. G. Sahebi, and S. S. Pradhan, “An Achievable Rate Region for the Three-User Interference Channel Based on Coded Codes,” IEEE Transactions on Information Theory, vol. 62, no. 3, pp. 1250–1279, March 2016.

[10] A. Padakandla, “An achievable rate region for 3—user classical-quantum broadcast channels,” 2022. [Online]. Available: https://arxiv.org/abs/2203.00110

[11] M. Heidari, F. Shirani, and S. S. Pradhan, “A new achievable rate region for multiple-access channel with states,” in 2017 IEEE International Symposium on Information Theory (ISIT), 2017, pp. 36–40.

[12] ———, “Quasi structured codes for multi-terminal communications,” IEEE Transactions on Information Theory, vol. 65, no. 10, pp. 6263–6289, 2019.

[13] C. E. Shannon, “Channels with side information at the transmitter,” IBM Journal of Research and Development, vol. 2, no. 4, pp. 280–293, 1958.

[14] K. Marton, “A coding theorem for the discrete memoryless broadcast channel,” IEEE Transactions on Information Theory, vol. 25, no. 3, pp. 306–311, May 1979.

[15] H. Boche, N. Cai, and J. Nötzel, “The classical-quantum channel with random state parameters known to the sender,” Journal of Physics A: Mathematical and Theoretical, vol. 49, no. 19, p. 195302, apr 2016. [Online]. Available: https://doi.org/10.1088/1751-8113/49/19/195302

[16] J. Nötzel, “Hypothesis testing on invariant subspaces of the symmetric group, part i - quantum sanov’s theorem and arbitrarily varying sources,” Journal of Physics A: Mathematical and Theoretical, vol. 47, 10 2013.

[17] 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.

[18] I. Savov and M. M. Wilde, “Classical codes for quantum broadcast channels,” IEEE Transactions on Information Theory, vol. 61, no. 12, pp. 7017–7028, 2015.
[19] T. Philosof and R. Zamir, “On the loss of single-letter characterization: The dirty multiple access channel,” IEEE Trans. on Info. Th., vol. 55, pp. 2442–2454, June 2009.
[20] A. Wyner, “Recent results in the shannon theory,” Information Theory, IEEE Transactions on, vol. 20, no. 1, pp. 2 – 10, Jan 1974.
[21] 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.
[22] M. M. Wilde, Quantum Information Theory, 2nd ed. Cambridge University Press, 2017.