An Achievable rate region for the 3—user interference channel based on coset codes

Arun Padakandla, Aria G. Sahebi and S. Sandeep Pradhan, Member, IEEE

Abstract

We consider the problem of communication over a three user discrete memoryless interference channel (3—IC). The current known coding techniques for communicating over an arbitrary 3—IC are based on message splitting, superposition coding and binning using independent and identically distributed (iid) random codebooks. In this work, we propose a new ensemble of codes - partitioned coset codes (PCC) - that possess an appropriate mix of empirical and algebraic closure properties. We develop coding techniques that exploit algebraic closure property of PCC to enable interference alignment over general 3—IC. We analyze the performance of the proposed coding technique to derive an achievable rate region for the general discrete 3—IC. Additive and non-additive examples are identified for which the derived achievable rate region is the capacity, and moreover, strictly larger than current known largest achievable rate regions based on iid random codebooks.

I. INTRODUCTION

An interference channel (IC) is a model for communication between multiple transmitter receiver (Tx-Rx) pairs that share a common communication medium. Each transmitter wishes to communicate specific information to its corresponding receiver. Since the Tx-Rx pairs share a common communication medium, every user’s signal causes interference to every other user. Communication over an IC is therefore facilitated by a coding technique that manages interference efficiently, in addition to combating channel noise.

Carleial proposed the technique of message splitting via superposition coding [1] to manage interference. Carleial's technique is based on each receiver decoding a part of the interferer’s signal and peeling it off to enhance its ability to decode the desired signal. Han and Kobayashi [2] enhanced Carleial’s technique with joint decoding and derived an achievable rate region for the IC with two receivers (2—IC) that is the current known largest. This coding technique and its corresponding achievable rate region will be referred to as CHK-technique and CHK rate region, respectively.

More recently, a newer technique of aligning interference has been proposed for managing interference over additive IC with three or more receivers. The technique of aligning interference is based on carefully choosing codebooks such that the interfering signals align and appear as if they were coming from a single user. This...
technique was proposed for the MIMO X-channel by Maddah Ali et. al. [3], and for the multi-user IC by Jafar and Cadambe [4]. The technique of aligning interference has subsequently been proposed in several settings [5], [6], [7] [8] using algebraic codes.

Our current understanding of interference alignment techniques is limited in several aspects. Firstly, these techniques are applicable only to additive IC’s. Secondly, from an information theoretic point of view, the single-letter distributions induced by the codes are uniform, resulting in achievability of rates corresponding to only uniform distributions. Thirdly, the particular form of (i) encoding, decoding (syndrome or lattice) and (ii) the information theoretic tools constrains us to analyze performance only of additive IC’s.

It is natural to ask whether the technique of interference alignment is applicable to only additive IC’s? More generally, do codes endowed with structure enable alignment and thereby facilitate communication over IC’s that are not additive? This article addresses these questions. In particular, we develop a coding technique based on a new ensemble of codes - partitioned coset codes (PCC) - possessing algebraic and empirical properties to enable alignment over arbitrary discrete memoryless IC’s with three receivers (3−IC). We analyze the performance of the proposed coding technique to derive a new achievable rate region for the 3−IC.

How does the proposed coding technique and the corresponding achievable rate region compare with the current known best? We employ the current known techniques of message splitting, superposition coding and binning based on unstructured codes to derive a characterization of $\mathbb{RSB}$−region, the current known largest achievable rate region for the general 3−IC. An important contribution of this article is the identification of additive as well as non-additive instances of 3−IC for which the proposed coding technique based on PCC yields a strictly larger achievable rate region than the $\mathbb{RSB}$−region. We emphasize that our findings for the non-additive instance validates the utility of the theory developed in this article.

The new elements of our work are the following. Firstly, we employ joint typicality encoding and decoding of coset codes to propose alignment techniques for arbitrary 3−IC’s. Secondly, we employ the technique of binning of coset codes to induce arbitrary distributions over corresponding alphabet sets and thereby prove achievability of rates corresponding to arbitrary distributions. Thirdly, we develop coding techniques over looser algebraic objects such as Abelian groups. These elements enable us to derive a new achievable rate region for the general 3−IC in terms of single-letter information theoretic quantities.

The technique of employing structured codes to obtain larger achievable rate regions was initiated in the context of a distributed source coding (DSC) problem by Körner and Marton [9]. Recently, this approach has been employed for several problem settings. Philosof and Zamir [10] employ coset codes for efficient communication over doubly dirty MACs and Gaussian version of this problem was studied using lattice codes in [11]. [12] and [13] propose lattice-based schemes for communicating over Gaussian multi-terminal networks. An achievable rate region based on Abelian group codes was provided for the general DSC problem in [14]. Linear codes have been employed for efficient computation over multiple access channels (MAC) in [15]. In the context of the interference channel, Maddah-Ali et. al. [3], [16], and Cadambe and Jafar [4] propose the technique of interference alignment, wherein interference is restricted to a subspace and thereby harness the available of degrees of freedom in an IC with several
Tx-Rx pairs more efficiently. Bresler, Parekh and Tse [5] employ lattice codes to align interference and thereby characterize the capacity of Gaussian ICs within a constant number of bits. The use of lattice codes has also been proposed in [17], [18], [19], [8] for efficient interference management over Gaussian ICs with three or more Tx-Rx pairs. [20] considers saturation technique for general ICs.

This article is organized as follows. In section III we characterize the current known largest achievable rate region based on unstructured codes for the general 3−IC and prove its strict sub-optimality in section IV. We provide new achievable rate regions based on PCC built over fields and groups in sections V and VI, respectively. We begin with preliminaries in section II.

II. PRELIMINARIES: NOTATION AND DEFINITIONS

A. Notation

We let $\mathbb{N}$, $\mathbb{R}$ denote the set of natural numbers and real numbers, respectively. Calligraphic letters such as $\mathcal{X}, \mathcal{Y}$ exclusively denote finite sets. For $K \in \mathbb{N}$, we let $[K] = \{1, 2, \ldots, K\}$. In this article, we will need to define multiple objects, mostly triples, of the same type. In order to reduce clutter, we use an underline to denote aggregates of objects of similar type. For example, (i) if $\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3$ denote (finite) sets, we let $\underline{\mathcal{Y}}$ either denote the Cartesian product $\mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_3$ or abbreviate the collection $(\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3)$ of sets, the particular reference being clear from context, (ii) if $y_j \in \mathcal{Y}_j : j \in [3]$, we let $\underline{y} \in \underline{\mathcal{Y}}$ abbreviate $(y_1, y_2, y_3) \in \mathcal{Y}_j$ (iii) if $d_j : \mathcal{Y}_j^n \to \mathcal{M}_j : j \in [3]$ denote (decoding) maps, then we let $d(\underline{y}^n)$ denote $(d_1(y_1^n), d_2(y_2^n), d_3(y_3^n))$. If $j \in \{1, 2\}$, then $j' \in \{1, 2\} \setminus \{j\}$ is the other index. Unless otherwise mentioned, we let $\theta$ denote an integral power of a prime. Throughout, $\mathcal{F}_\theta$ will denote the finite field of cardinality $\theta$. $\oplus$ denotes the addition operation in the corresponding finite field. We employ the notion of typicality as in [21]. In particular, if $U, V$ are random variables distributed with respect to $p_{UV}$, then $T_\eta(U, V) \in \mathcal{U}_n \times \mathcal{V}_n$ denotes the typical set with respect to $p_{UV}$ and deviation parameter $\eta$. For any $v^n \in \mathcal{V}^n$, $T_\eta(U|v^n) = \{u^n : (u^n, v^n) \in T_\eta(U, V)\}$ denotes the conditional typical set. $\ast$ denotes binary convolution, i.e., $\alpha \ast \beta = (1 - \beta) + (1 - \alpha) \beta$. $|a|^+ \ast \alpha$ is defined as $\max\{0, a\}$.

B. Definitions: 3−IC, 3−to−1IC, achievability, capacity region

A 3−IC consists of three finite input alphabet sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3$ and three finite output alphabet sets $\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3$. The discrete time channel is (i) time invariant, (ii) memoryless, and (iii) used without feedback. Let $W_{Y_j|X_j}(y_j|x_j)$ denote probability of observing symbol $y_j \in \mathcal{Y}_j$ at output $j$, given $x_j \in \mathcal{X}_j$ is input by encoder $j$. Inputs are constrained with respect to bounded cost functions $\kappa_j : \mathcal{X}_j \to [0, \infty)$ : $j \in [3]$. The cost function is assumed to be additive, i.e., cost of transmitting vector $x_j^n \in \mathcal{X}_j^n$ is $\kappa_j^n(x_j^n) = \frac{1}{n} \sum_{t=1}^n \kappa_j(x_{jt})$. We refer to this 3−IC as $(\mathcal{X}, \mathcal{Y}, W_{Y_j|X_j}, \kappa)$.

**Definition 1:** A 3−IC code $(n, \mathcal{M}, e, d)$ consist of (i) index sets $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$ of messages, (ii) encoder maps $e_j : \mathcal{M}_j \to \mathcal{X}_j^n : j \in [3]$, and (iii) decoder maps $d_j : \mathcal{Y}_j^n \to \mathcal{M}_j : j \in [3]$. 
Definition 2: The error probability of a $3$–IC code $(n, \mathcal{M}, \varepsilon, d)$ conditioned on message triple $(m_1, m_2, m_3) \in \mathcal{M}$ is

$$\xi(\varepsilon, d|m) := 1 - \sum_{y^n \in \mathcal{Y}^n} W_{Y^n|X^n}^n(y^n|m_1, m_2, m_3).$$

The average error probability of a $3$–IC code $(n, \mathcal{M}, \varepsilon, d)$ is $\bar{\xi}(\varepsilon, d) := \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \xi(\varepsilon, d|m)$. Average cost per symbol of transmitting message $m \in \mathcal{M}$ is $\tau(\varepsilon|m) := \left(\hat{r}_j^n(\varepsilon(m_j)) : j \in [3]\right)$ and average cost per symbol of $3$–IC code $(n, \mathcal{M}, \varepsilon, d)$ is $\tau(\varepsilon) := \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \tau(\varepsilon|m)$.

Definition 3: A rate-cost sextuple $(R_1, R_2, R_3, t_1, t_2, t_3) \in [0, \infty]^6$ is said to be achievable if for every $\eta > 0$, there exists $N(\eta) \in \mathbb{N}$ such that for all $n > N(\eta)$, there exists a $3$–IC code $(n, \mathcal{M}^{(n)}, \varepsilon^{(n)}, d^{(n)})$ such that (i) $\frac{\log |\mathcal{M}^{(n)}|}{n} \geq R_3 - \eta$; (ii) $\bar{\xi}(\varepsilon^{(n)}, d^{(n)}) \leq \eta$, and (iii) average cost $\tau(\varepsilon^{(n)})_j \leq t_j + \eta$. The capacity region is $\mathcal{C}(\varepsilon) := \{R \in \mathbb{R}^3 : (R, \tau) \text{ is achievable}\}$.

We now consider $3$–to–$1$ IC, a class of $3$–IC’s that was studied in [22]. $3$–to–$1$ IC enables us to prove strict sub-optimality of coding techniques based on unstructured codes. A $3$–to–$1$ IC is a $3$–IC wherein two of the users enjoy interference free point-to-point links. Formally, a $3$–IC $(\mathcal{X}, \mathcal{Y}, W_{Y|X})$ is a $3$–to–$1$ IC if (i) $W_{Y_1|X}(y_2|x) := \sum_{(y_1, y_3) \in \mathcal{Y}_1 \times \mathcal{Y}_3} W_{Y_1|X}(y_2|x) W_{Y_1|X}(y_1|x) W_{Y_3|X}(y_3|x)$ is independent of $(x_1, x_3) \in \mathcal{X}_1 \times \mathcal{X}_3$, and (ii) $W_{Y_2|X}(y_2|x) := \sum_{(y_1, y_3) \in \mathcal{Y}_1 \times \mathcal{Y}_3} W_{Y_2|X}(y_2|x) W_{Y_1|X}(y_1|x) W_{Y_3|X}(y_3|x)$ is independent of $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$ for every collection of input and output symbols $(x, y) \in \mathcal{X} \times \mathcal{Y}$. For a $3$–to–$1$ IC, the channel transition probabilities factorize as

$$W_{Y|X}(y|x) = W_{Y_1|X}(y_1|x) W_{Y_2|X_2}(y_2|x_2) W_{Y_3|X_3}(y_3|x_3)$$

for some conditional probability mass functions (pmfs) $W_{Y_1|X}$, $W_{Y_2|X_2}$ and $W_{Y_3|X_3}$. We also note that $X_1X_3 - X_2 - Y_2$ and $X_1X_2 - X_3 - Y_3$ are Markov chains for any distribution $p_{X_1}p_{X_2}p_{X_3}$.

In the following section, we describe the coding technique of message splitting and superposition using unstructured codes and employ this to derive the $\mathcal{R}$SB–region for $3$–to–$1$ IC.

III. MESSAGE SPLITTING AND SUPERPOSITION USING UNSTRUCTURED CODES

Before we consider the case of a $3$–to–$1$ IC, it is appropriate to state how does one optimally stitch together current known coding techniques - message splitting, superposition coding and precoding via binning - for communicating over $3$–IC? Each encoder must make available parts of its signal to each user it interferes with. Specifically, encoder $j$ splits its signal into four parts - one public, two semi-private and one private. The corresponding decoder $j$ decodes all of these parts. The other two decoders, say $i$ and $k$, for which encoder $j$’s signal is interference, decode the public part of user $j$’s signal. The public part is decoded by all receivers, and is therefore encoded using a cloud center codebook at the base layer. Moreover, each semi-private part of encoder $j$’s signal is decoded by exactly one among the decoders $i$ and $k$. The semi-private parts are encoded at the intermediate level using one codebook each. These codebooks, referred to as semi-satellite codebooks, are conditionally coded over the cloud.

$^1$Any interference channel wherein only one of the users is subjected to interference is a $3$–to–$1$ IC by a suitable permutation of the user indices.
center codebook. The semi-satellite codebooks are precoded for each other via binning. The private part is encoded at the top layer using a satellite codebook. The satellite codebook is conditionally coded over the cloud center and semi-satellite codebooks. Each decoder decodes the eight parts using a joint typicality decoder. Finally, the encoders and decoders share a time sharing sequence to enable them to synchronize the choice of codebooks at each symbol interval. We henceforth refer to the above coding technique as the $\mathcal{SB}$-technique.

One can characterize $\mathcal{SB}$-region - an achievable rate region corresponding to the above coding technique - via random coding. Indeed, such a characterization is quite involved. Since our objective is to illustrate sub-optimality of $\mathcal{SB}$-technique, it suffices to obtain a characterization of $\mathcal{SB}$-region for 3-to-1 ICs.

For the case of 3-to-1 IC, user 1’s signal does not cause interference to users 2 and 3, and therefore will not need it to split its message. This can be proved using the Markov chains $X_1X_3 \rightarrow X_2 \rightarrow Y_2$ and $X_1X_2 \rightarrow X_3 \rightarrow Y_3$. Moreover, signal of user 2 does not interfere with user 3’s reception and vice versa. Therefore, users 2 and 3 will only need to split their messages into two parts - a private part and a semi-private part that is decoded by user 1. Using this approach we obtain the following achievable rate region.

**Definition 4:** Let $\mathbb{D}_u(\tau)$ denote the collection of pmfs $p_{QU_3,XY}$ defined on $Q \times U_2 \times U_3 \times X \times Y$, where $Q, U_2, U_3$ are finite sets, such that (i) $p_{Y|U_2U_3Q} = W_{Y|X}$, (ii) the triplet $X_1, (U_2, X_2)$ and $(U_3, X_3)$ are conditionally mutually independent given $Q$, (iii) $E \{\kappa_j(X_j)\} \leq \tau_j : j \in [3]$. For $p_{QU_3XY} \in \mathbb{D}_u(\tau)$, let $\alpha_u(p_{QU_3XY})$ denote the set of rate triples $(R_1, R_2, R_3) \in [0, \infty)^3$ that satisfy

$$0 \leq R_1 < I(X_1; Y_1| Y_2, U_2, U_3), \quad 0 \leq R_j < I(U_j; Y_j| Q): j = 2, 3$$

$$R_1 + R_2 < I(U_2X_1; Y_1| QU_3) + I(X_2; Y_2| QU_2), \quad R_1 + R_3 < I(U_3X_1; Y_1| QU_2) + I(X_3; Y_3| QU_3)$$

$$R_1 + R_2 + R_3 < I(U_2U_3X_1; Y_1| Q) + I(X_2; Y_2| QU_2) + I(X_3; Y_3| QU_3),$$

and

$$\alpha_u(\tau) = \text{cl} \left( \bigcup_{p_{QU_3XY} \in \mathbb{D}_u(\tau)} \alpha_u(p_{QU_3XY}) \right).$$

**Theorem 1:** For 3-to-1 IC $(X, Y, W_{Y|X})$, $\alpha_u(\tau)$ is achievable, i.e., $\alpha_u(\tau) \subseteq C(\tau)$.

**IV. STRICT SUB-OPTIMALITY OF $\mathcal{SB}$-REGION FOR 3-TO-1 IC**

This section contains our first main finding of this article - strict sub-optimality of $\mathcal{SB}$-technique. In particular, we identify a binary additive 3-to-1 IC for which we prove strict sub-optimality of $\mathcal{SB}$-technique. We begin with the description of the 3-to-1 IC. It maybe noted that a similar example was studied in [5], wherein CHK technique restricted to Gaussian test channels were shown to be strictly sub-optimal. While our finding is in a similar spirit, our proof takes into account all possible test channels under the CHK technique. In [9], it was proven that linear codes are strictly more efficient than unstructured codes for the DSC problem.

**Example 1:** Consider a binary additive 3-to-1 IC illustrated in figure 1 with $X_j = Y_j = \{0, 1\} : j \in [3]$ with channel transition probabilities $W_{Y_j|X_j}(y|x) = BSC_{\delta_j}(y_1|x_1 \oplus x_2 \oplus x_3)BSC_{\delta_j}(y_2|x_2)BSC_{\delta_j}(y_3|x_3)$, where $BSC_{\eta}(0|1) = BSC_{\eta}(1|0) = 1 - BSC_{\eta}(0|0) = 1 - BSC_{\eta}(1|1) = \eta$ denotes the transition probabilities of a BSC.
with cross over probability $\eta \in [0, \frac{1}{2}]$. Inputs of users 2 and 3 are not constrained, i.e., $\kappa_j(0) = \kappa_j(1) = 0$ for $j = 2, 3$. User 1’s input is constrained with respect to a Hamming cost function, i.e., $\kappa_1(x) = x$ for $x \in \{0, 1\}$ to an average cost of $\tau \in (0, \frac{1}{2})$ per symbol. Let $C(\tau)$ denote the capacity region of this 3–to–1 IC.

Clearly, $C(\tau) \subseteq \beta(\tau, \frac{1}{2}, \frac{1}{2}, \delta)$, where

$$\beta(\tau, \delta) := \{(R_1, R_2, R_3) \in [0, \infty)^3 : R_j \leq h_b(\delta_j \ast \tau_j) - h_b(\delta_j) : j = 1, 2, 3\}.$$  

Let us focus on achievability. We begin with a few simple observations for the above channel. Let us begin with the assumption $\delta := \delta_2 = \delta_3$. As illustrated in figure 1 users 2 and 3 enjoy interference free unconstrained binary symmetric channels (BSC) with cross over probability $\delta = \delta_2 = \delta_3$. They can therefore communicate at their respective capacities $1 - h_b(\delta)$. Constrained to average Hamming weight of $\tau$, user 1 cannot hope to achieve a rate larger than $h_b(\tau \ast \delta_1) - h_b(\delta_1)$\footnote{If receiver 1 is provided with the codewords transmitted by users 2 and 3, the effective channel it sees is a BSC with cross over probability $\delta_1$.} What is the maximum rate achievable by user 1 while users 2 and 3 communicate at their respective capacities?

User 1 cannot achieve rate $h_b(\tau \ast \delta_1) - h_b(\delta_1)$ and decode the pair of codewords transmitted by user 2 and 3 if $h_b(\tau \ast \delta_1) - h_b(\delta_1) + 2(1 - h_b(\delta)) > 1 - h_b(\delta_1)$ or equivalently $1 + h_b(\tau \ast \delta_1) > 2h_b(\delta)$. Under this condition, $\#SB$–technique forces decoder 1 to be contented to decoding univariate components - represented through semi-private random variables $U_2, U_3$ - of user 2 and 3’s signals. We state that as long as the univariate components leave residual uncertainty in the interfering signal, i.e., $H(X_2 \oplus X_3 | U_2, U_3) > 0$, the rate achievable by user 1 is strictly smaller than its maximum $h_b(\tau \ast \delta_1) - h_b(\delta_1)$\footnote{The reader will be able to reason this by relating this situation to a point-to-point (PTP) channel with partial state observed at the receiver.}

We now describe a simple linear coding technique, based on the works of [22], [6], [17], that enables user 1 to achieve its maximum rate $h_b(\tau \ast \delta_1) - h_b(\delta_1)$ even under the condition $1 + h_b(\tau \ast \delta_1) > 2h_b(\delta)$! Let us assume $\tau \ast \delta_1 \leq \delta$. We choose a linear code, or a coset thereof, that achieves the capacity of a BSC with cross over probability $\delta$. We equip users 2 and 3 with the same code, thereby constraining the sum of their transmitted
codewords to this linear code, or a coset thereof, of rate $1 - h_b(\delta)$. Since $\tau \ast \delta_1 \leq \delta$, decoder 1 can first decode the interfering signal - sum of codewords transmitted by encoders 2 and 3 - treating the rest as noise, peel it off, and then decode the desired signal. User 1 can therefore achieve its maximum rate $h_b(\tau \ast \delta_1) - h_b(\delta_1)$ if $\tau \ast \delta_1 \leq \delta$.

In proposition $[1]$ we prove that if $1 + h_b(\delta_1 \ast \tau) > h_b(\delta_2) + h_b(\delta_3)$, then $(h_b(\tau \ast \delta_1) - h_b(\delta_1), 1 - h_b(\delta_2), 1 - h_b(\delta_3)) \notin \alpha_u((\tau, 0, 0))$. We therefore conclude that if $\tau, \delta_1, \delta_2, \delta_3$ are such that $1 + h_b(\delta_1 \ast \tau) > h_b(\delta_2) + h_b(\delta_3)$ and $\min \{\delta_2, \delta_3\} \geq \delta_1 \ast \tau$, then $\mathcal{SB}$-technique is strictly suboptimal for the 3-to-1 IC presented in example $[1]$.

**Proposition 1:** For the 3-to-1 IC of example $[1]$ if $\tau \ast \delta_1 \leq \min \{\delta_2, \delta_3\}$, then $\mathcal{C}(\tau) = \beta(\tau, \frac{1}{2}, \frac{1}{2}, \delta)$, where $\beta(\tau, \delta)$ is given by $[3]$. If $h_b(\delta_2) + h_b(\delta_3) < 1 + h_b(\tau \ast \delta_1)$, then $(h_b(\tau \ast \delta_1) - h_b(\delta_1), 1 - h_b(\delta_2), 1 - h_b(\delta_3)) \notin \alpha_u(\tau, 0, 0)$. Please refer to appendix $A$ for a proof. In particular, if $\delta_1 = 0.01$ and $\delta_2 \in (0.1325, 0.21)$, then $\alpha_u(\frac{1}{8}, 0, 0) \notin \mathcal{C}(\frac{1}{8})$.

V. Achievable rate region using PCC built over finite fields

In this section we present our second main finding - a new achievable rate region for 3-IC in the context of finite fields. In other words, we propose a coding technique based on PCC built over finite fields. Characterizing its information-theoretic performance enables us to derive an achievable rate region, henceforth referred to as PCC-rate region.$^4$ We derive PCC rate region in three pedagogical steps. In the first step, presented in section V-A, we employ PCC to manage interference seen by only one of the receivers. This simplified setting aids the reader recognize and absorb all the key elements of the framework proposed herein. For this step, we provide a complete proof of achievability. In this section, we also identify a non-additive 3-to-1 IC (Example 2) for which we analytically prove (i) strict sub-optimality of $\mathcal{SB}$-technique and (ii) optimality of PCC rate region. We provide several examples that illustrate the central theme of this article - codes endowed with algebraic closure properties enable interference alignment over arbitrary 3-ICs, not just additive, symmetric instances - and thereby justify the framework developed herein.

In the second step, presented in section V-B, we employ PCC to manage interference seen by every receiver and thereby provide a characterization of PCC rate region. In the third step we provide a unification of PCC rate region and $\mathcal{SB}$- rate region along the lines of [23, Section VI].

A. Step 1: Managing interference seen by one receiver using PCC built over fields

**Definition 5:** Let $\mathbb{D}_f(\tau)$ denote the collection of distributions $p_{QU_2U_3XY} \in \mathbb{D}_u(\tau)$ defined over $Q \times U_2 \times U_3 \times X \times Y$, such that $U_2 = U_3$ is a finite field. For $p_{QU_2U_3XY} \in \mathbb{D}_f(\tau)$, let $\alpha_j^{-1}(p_{QU_2U_3XY})$ be defined as the set of rate triples $(R_1, R_2, R_3) \in [0, \infty)^3$ that satisfy

$R_1 < \min \{0, H(U_j|Q) - H(U_2 \oplus U_3|QY_1) : j = 2, 3\} + I(X_1; U_2 \oplus U_3, Y_1|Q),$

$R_j < I(U_j, X_j; Y_j|Q) : j = 2, 3,$

$R_1 + R_j < I(X_2; Y_2|QU_3) + I(X_1; U_2 \oplus U_3, Y_1|Q) + H(U_j|Q) - H(U_2 \oplus U_3|QY_1) : j = 2, 3,$

$^4$We employ the same terminology for the rate region achievable using PCC built over Abelian groups in section VI.
and
\[ a_f^{3^{-1}}(\tau) = \text{cocl} \left( \bigcup_{p_{QU_3XY} \in D_f(\tau)} a_f^{3^{-1}}(p_{QU_3XY}) \right). \]

**Theorem 2:** For 3-IC $\mathcal{X}, \mathcal{Y}, W_{Y|X}, \mathbb{E}$, $a_f^{3^{-1}}(\tau)$ is a continuous function of the 3-IC $\mathcal{X}, \mathcal{Y}, W_{Y|X}, \kappa$. A proof is provided in appendix B. Here we provide a simplified description of the coding technique. Towards that end, consider a pmf $p_{QU_3XY} \in \mathcal{D}_f(\tau)$ with $Q = \{x\}$ and $U_2 = U_3 = F_0$. Encoder 1 builds a single codebook $C_1 = (x_1^n(m_1) : m_1 \in \mathcal{M}_1)$ of rate $R_1$ over $\mathcal{X}_1$ and the codeword indexed by the message is transmitted on the channel.

The structure and encoding rules for users 2 and 3 are identical and we describe it using a generic index $j \in \{2, 3\}$. As in section III, we employ a two layer - cloud center and satellite - code for user $j$ and split its message $M_j \in \mathcal{M}_j$ into two parts. Let (i) $M_{j1} \in \mathcal{M}_{j1} := \{\theta^j\}$ denote its semi-private part, and (ii) $M_{jX} \in \mathcal{M}_{jX} := \{\exp\{nL_j\}\}$ denote its private part. While in section III, user 1 decoded the pair of cloud center codewords, the first key difference we propose is that user 1 decodes the sum of user 2 and 3 cloud center codewords. Let a coset $\lambda_j \subseteq U_j^n$ of a linear code $\mathcal{X}_j \subseteq U_j^n$ denote user $j$’s cloud center codebook. In particular, let $g_j \in U_j^{s_j \times n}$ denote generator matrix of $\mathcal{X}_j$ and coset $\lambda_j$ correspond to shift $b_j^n \in U_j^n$. We let the cloud center codebooks of users’ 2 and 3 overlap, i.e., the larger of $\overline{\lambda}_2, \overline{\lambda}_3$ contains the other. For example, if $s_{j2} \leq s_{j3}$, then $\overline{\lambda}_{j2} \subseteq \overline{\lambda}_{j3}$. We therefore let $g_{j3}^T = \begin{bmatrix} g_{j2}^T & g_{j3/j2}^T \end{bmatrix}$.

Since codewords of a uniformly distributed coset code are uniformly distributed, we need to partition the coset code $\lambda_j$ into $\theta^j$ bins to induce a non-uniform distribution over the auxiliary alphabet $U_j$. In particular, for each codeword $u_j^n(a^{s_j}) := a^{s_j} \oplus b_j^n$, where $a^{s_j} \in U_j^{s_j}$, a binning function $i_j(a^{s_j}) \in \theta^j$ is defined that indexes the bin containing $u_j^n(a^{s_j})$. We let $c_{j1}(m_{j1}) = \{a^{s_j} \in U_j^{s_j} : i_j(a^{s_j}) = m_{j1}\}$ denote the set containing indices corresponding to message $m_{j1}$. The structure of the cloud center codebook plays an important role and we formalize the same through the following definition.

**Definition 6:** A coset code $\lambda$ is completely specified by the generator matrix $g \in F_0^{k \times n}$ and a bias vector $b^n \in F_0^n$. Consider a partition of $\lambda$ into $\theta^l$ bins. Each codeword $a^{k} \oplus b^n$ is assigned an index $i(a^{k}) \in \theta^l$. This coset code $\lambda$ with its partitions is referred to as an $(n, k, l, g, b^n, i)$ partitioned coset code (PCC) or succinctly as an $(n, k, l)$ PCC. For each $m \in \theta^l$, let $c(m) := \{a^{k} \in F_0^k : i(a^{k}) = m\}$.

User $j$’th satellite codebook $C_j$, built over $\mathcal{X}_j$, consists of $\exp\{nL_j\}$ bins, one for each private message $m_{jX} \in \mathcal{M}_{jX} := \{\exp\{nK_j\}\}$. Let $(x_j^n(m_{jX}, b_{jX}) \in \mathcal{X}_j^n : b_{jX} \in \{\exp\{nK_j\}\})$ denote bin corresponding to message $m_{jX} \in \mathcal{M}_{jX}$ and let $c_{jX} := \{\exp\{nK_j\}\}$. Having received message $M_j = (M_{j1}, M_{jX})$, the encoder identifies all pairs $(u_j^n(a^{s_j}), x_j^n(M_{jX}, b_{jX}))$ of jointly typical codewords with $(a^{s_j}, b_{jX}) \in c_{j1}(M_{j1}) \times c_{jX}$. If it finds one or more such pairs, one of them is chosen and the corresponding satellite codeword is fed as input on the channel. Otherwise, an error is declared.

---

5Since the time sharing random variable $Q$ is employed in a standard way, we choose to omit it in this description.

6The use of a coset code instead of a linear code enables ease of analysis. In particular, the key property of statistical pairwise independence of distinct codewords of randomly chosen coset codes is facilitated by choosing a random bias shift. This is employed in the many proof elements, for example that of Lemma 3.
We now describe the decoding rule. Predictably, the decoding rules of users 2 and 3 are identical and we describe this through a generic index \( j \in \{2,3\} \). Decoder \( j \) identifies all \((\hat{m}_{j1}, \hat{m}_{jX})\) for which there exists \((a^*, b_jX) \in c_{j1}(\hat{m}_{j1}) \times c_{jX} \) such that \((u_j^n(a^*), x_j^n(\hat{m}_{jX}, b_jX), Y_j^n)\) is jointly typical with respect to \( p_{U_jX_jY_j} \). If there is exactly one such pair \((\hat{m}_{j1}, \hat{m}_{jX})\), this is declared as the message of user \( j \). Otherwise an error is signaled.

Decoder 1 constructs the sum \( \lambda_2 + \lambda_3 := \{u_2^n \oplus u_3^n : u_j^n \in \lambda_j, j = 2,3\} \) of the cloud center codebooks. Having received \( Y_1^n \), it looks for all potential message \( \hat{m}_1 \) for which there exists a \( u_0^n \in \lambda_2 + \lambda_3 \) such that \((u_0^n, x_1^n(\hat{m}_1), Y_1^n)\) is jointly typical with respect to \( p_{U_2U_3X_1Y_1} \). If it finds exactly one such message \( \hat{m}_1 \), it declares this as the decoded message of user 1. Otherwise, it declares an error.

We characterize the performance of the proposed coding technique in the proof by averaging over the ensemble of codebooks. Since the distribution induced on the codebooks is such that codebooks of users 2 and 3 are statistically correlated and moreover, contain codewords, this involves new elements.

The coding technique proposed in the proof of theorem 2 is indeed a generalization of that proposed for example 1 and moreover capacity achieving for the same. We formalize this through the following corollary.

**Corollary 1.** For the 3-to-1 IC in example 1 if \( \tau * \delta_1 < \min\{\delta_2, \delta_3\} \), then \( \alpha_j^{3-1}(\tau, \frac{1}{2}, \frac{1}{2}) = C(\tau) \).

It can be verified that \( \beta(\tau, \frac{1}{2}, \frac{1}{2}, \delta) = \alpha_j^{3-1}(p_{QU_2X_3Y}) \) where \( P(U_j = X_j = 0) = P(U_j = X_j = 1) = \frac{1}{2}, P(X_1 = 1) = \tau \) and \( Q = \phi \), the empty set, where \( \beta(\tau, \delta) \) is given in (3).

In the sequel, we illustrate through three examples the central claim of this article that the utility of codes endowed with algebraic structure, in particular coset codes, are not restricted to particular symmetric and additive problems. Furthermore, these examples establish the need (i) to achieve rates corresponding to non-uniform distributions which is accomplished via the technique of binning, (ii) to build coset codes over larger fields, and (iii) to analyze decoding of sums of transmitted codewords over arbitrary channels using typical set decoding.

**Example 2:** Consider a binary 3-to-1 IC illustrated in figure 2 with \( X_j = Y_j = \{0,1\} : j \in [3] \) with channel transition probabilities \( W_{Y_jX_j}(y|x) = BSC_{\delta_1}(y_1|x_1 \oplus (x_2 \lor x_3))BSC_{\delta_2}(y_2|x_2)BSC_{\delta_3}(y_3|x_3) \) where \( \lor \) denotes logical OR. Users' inputs are constrained with respect to a Hamming cost function, i.e., \( \kappa_j(x) = x \) for \( x \in \{0,1\} \), and user \( j \)th input is constrained to an average cost per symbol of \( \tau_j \in (0, \frac{1}{2}) \) for \( j \in [3] \).

Clearly, for the above example, \( X_2 \lor X_3 \) is the interfering pattern. If \( X_2 \) and \( X_3 \) are viewed as elements in the ternary field, then observe that \( H(X_2 \lor X_3|X_2 \oplus X_3) = 0 \). The decoder 1 can reconstruct the interfering pattern after having decoded the ternary sum of the codewords. This motivates the use of coset codes for decoding of non-additive interference.

**Proposition 2:** Consider the 3-to-1 IC described in example 2 with \( \delta := \delta_2 = \delta_3 \in (0, \frac{1}{2}) \) and \( \tau := \tau_2 = \tau_3 \in (0, \frac{1}{2}) \). Let \( \beta := \delta_1 \ast (2\tau - \tau^2). \) If

\[
    h_b(\tau * \delta) - h_b(\delta) \leq \theta,
\]

where \( \theta = h_b(\tau) - h_b((1 - \tau)^2) - (2\tau - \tau^2)h_b(\frac{1}{2\tau - \tau^2}) - h_b(\tau_1 \ast \delta_1) + h_b(\tau_1 \ast \beta) \), then \( \beta(\tau, \delta) = C(\tau) = \alpha_j^{3-1}(\tau) \).

\(^7\)BSC(\cdot|\cdot) has been defined in example 1.
Moreover, the rate triple \( (h_b(\tau_1 + \delta_1) - h_b(\delta_1), h_b(\tau \ast \delta) - h_b(\delta_1), h_b(\tau \ast \delta) - h_b(\delta_1)) \) \( \notin \alpha_u(\tau) \) if

\[
h_b(\tau_1 + \delta_1) - h_b(\delta_1) + 2(h_b(\tau \ast \delta) - h_b(\delta_1)) > h_b(\tau_1(1 - \beta) + (1 - \tau_1)\beta) - h_b(\delta_1).
\]

Therefore, if \( 4 \) and \( 5 \) hold, \( \alpha_u(\tau) \triangleq \alpha_f^3(\tau) = C(\tau) \).

Please refer to appendix \( G \) for a proof. Conditions \( 4 \) and \( 5 \) are not mutually exclusive. It maybe verified that the choice \( \tau_1 = \frac{1}{90}, \tau = 0.15, \delta_1 = 0.01, \delta = 0.067 \) satisfies both conditions, thereby establishing the utility of structured codes for examples well beyond particular additive ones.

A skeptical reader may wonder whether the utility of PCC depends crucially on the additive multiple access channel (MAC) \( Y_1 = X_1 \oplus (X_2 \lor X_3) \oplus N_1 \). The following example provides conclusive evidence that this is indeed not the case.

**Example 3:** Consider a binary 3-to-1 IC illustrated in figure 3 with \( X_j = Y_j = \{0, 1\} : j \in [3] \) with channel transition probabilities \( W_{Y_j|X_j}(y|x) = MAC(y_1|x_1, x_2 \lor x_3)BSC_\delta(y_2|x_2)BSC_\delta(y_3|x_3) \), where \( MAC(0, 0, 0) = 0.989, MAC(0, 0, 1) = 0.01, MAC(0, 1, 0) = 0.02, MAC(0, 1, 1) = 0.993 \) and \( MAC(1, b, c) = MAC(0, b, c) = 1 \) for each \( (b, c) \in \{0, 1\}^2 \). Users’ inputs are constrained with respect to a Hamming cost function, i.e., \( \kappa_j(x) = x \) for \( x \in \{0, 1\} \). Assume that user \( j \)th input is constrained to an average cost per symbol of \( \tau_j \in (0, \frac{1}{2}) \), where \( \tau : = \tau_2 = \tau_3 \).

Our study of example 3 closely mimics that of example 2. In particular, we derive conditions under which \( C^* : = (C_1, h_b(\tau \ast \delta) - h_b(\delta), h_b(\tau \ast \delta) - h_b(\delta)) \in \alpha_f^3(\tau) \) and \( C^* \notin \alpha_u(\tau) \), where \( \tau : = (\tau_1, \tau, \tau) \),

\[
C_1 : = \sup_{p_{X|Y} \in D(\tau)} I(X_1; Y_1|X_2 \lor X_3),
\]

\[
D(\tau) : = \left\{ p_{X|Y} \text{ is a pmf on } X \times Y \text{ such that (i) } p_{Y|X} = W_{Y|X} \text{ is the channel transition probabilities of example 3 (ii) } p_{X} = p_{X_1}p_{X_2}p_{X_3}, p_{X_j}(1) = \tau \text{ for } j = 2, 3 \text{ and (iii) } p_{X_1}(1) \leq \tau_1 \right\}.
\]

By strict concavity of \( I(X_1; Y_1|X_2 \lor X_3) \) in \( p_{X_1} \), and the compactness of \( D(\tau) \), there exists a unique \( p_{X|Y}^* \) with respect to which \( I(X_1; Y_1|X_2 \lor X_3) = C_1 \).

\*The reader is reminded that \( \alpha_u(\tau) \) is defined in definition 4.
Proposition 3: Consider example 3 and let $C^*, C_1, D(\tau), p^*_{X,Y}$ be defined as above. If
\[
C_1 + 2(h_b(\tau \ast \delta) - h_b(\delta)) = I(X_1; Y_1 | X_2 \lor X_3) + 2(h_b(\tau \ast \delta) - h_b(\delta)) > I(X; Y_1),
\]
where $I(X_1; Y_1 | X_2 \lor X_3)$, and $I(X; Y_1)$ are evaluated with respect to $p^*_{X,Y}$, then $C^* \notin \alpha_1(\tau)$. If $h_b(\tau^2) + (1 - \tau^2)h_b\left(\frac{(1-\tau^2)}{1-\tau^2}\right) + H(Y_1 | X_2 \lor X_3) - H(Y_1) \leq \min\{H(X_2 | Y_2)H(X_3 | Y_3)\}$, where the entropy terms are evaluated with respect to $p^*_{X,Y}$, then $C^* \in \alpha_1(\tau)$.

Please refer to appendix [H] for a proof. For example 3, with $\tau_1 = 0.01, \tau = \tau_2 = \tau_3 = 0.1525, \delta = 0.067$, the conditions stated in proposition 3 hold simultaneously. For this channel, $p^*_{X_1}(1) = 0.99$,
\[
C_1 + 2(h_b(\tau \ast \delta) - h_b(\delta)) - I(X; Y_1) = 0.0048,
\]
and
\[
\min\{H(X_2 | Y_2)H(X_3 | Y_3)\} - [h_b(\tau^2) + (1 - \tau^2)h_b\left(\frac{(1-\tau^2)}{1-\tau^2}\right) + H(Y_1 | X_2 \lor X_3) - H(Y_1)] = 0.0031.
\]

A note on our choice of the MAC that relates $(X_1, X_2 \lor X_3)$ and $Y_1$ is in order. The reader will recognize that the MAC is ‘quite close’ to the additive scenario $Y_1 = X_1 \oplus (X_2 \lor X_3) \oplus N_1$ studied in example 2. In order for coset codes to outperform unstructured codes, we do not need the MAC to be so ‘close’ to the additive MAC. The need for the MAC to be ‘so close’ is a consequence of our desire to provide an analytical proof for strict sub-optimality of unstructured codes. Note that since we (i) do not resort to outer bounds, (ii) wish to provide analytical upper bounds to the rates achievable using unstructured codes, and (iii) cannot compute any of the associated rates in a reasonable time, we demand the MAC to be such that coset codes achieve the maximum possible rate for user 1, with users 2 and 3 constrained to achieve their PTP capacities\(^9\) and unstructured codes to be strictly sub-optimal. Finally, the above findings indicate that if structured codes yield gains for a particular channel, then one can reason out the presence of such gains for a slightly perturbed channel simply by appealing to the continuity of rate regions in the channel parameters.

In the achievable rate region presented in Theorem 2 for a given 3-IC, there is a union over finite fields. Suppose we want to maximize $\mu_1 R_1 + \mu_2 R_2 + \mu_3 R_3$ for some non-negative vector $\mu$ such that $\|\mu\| = 1$. The finite field that maximizes this objective function depends on the channel in a complicated way. It turns out that for a channel with a fixed interference pattern, as we change the cost functions $\kappa$, and the noise distributions, the optimizing finite field also changes. This is illustrated in the following example.

Example 4: Consider a quaternary 3-to-1 IC with $X_j = Y_j = \{0, 1, 2, 3\}$ : $j \in [3]$ with transition probabilities given by $Y_1 = X_1 +_4 X_2 +_4 X_3 +_4 N_1$, $Y_2 = X_2 +_4 N_2$ and $Y_3 = X_3 +_4 N_3$. $N_1, N_2$ and $N_3$ are mutually independent, and independent of the inputs, and $+_4$ denote addition modulo-4. Let $N_2$ and $N_3$ have the same pmf. Note that the bivariate function characterizing the interference in the channel is addition modulo-4, which is not a finite field. Our objective is to enable each user to attain the corresponding point-to-point capacity. Note that we have not yet specified the pmfs $P_N$ of the noise vector $N$, the cost function vector $\kappa$, and the cost constraint $\tau$.

\(^9\)Note that we are demanding the channel to permit user 1 communicate at a rate as though the receiver knew all of the non-linear interference.
noise pmfs (\(F_{\lambda}, F_t\)) general abelian group. We will restrict our attention to the following two finite fields and an abelian group: \(F_7\), \(F_8\) and \(\mathbb{Z}_4\). This requires appropriate maps from \(F_7\) and \(F_8\) to \(\mathbb{Z}_4\). By doing a computer search, we have obtained the following sample data (see Table I). The rates for the case of \(\mathbb{Z}_4\) is obtained by using theorem 5 from Section VI.

For example, for the distribution in the first row, all users achieve their respective capacities only with PCCs built on \(F_7\). Similarly PCCs built on \(F_8\) and \(\mathbb{Z}_4\) achieve optimality for the distributions of the second and third rows respectively. Note that even though the interference pattern is fixed, the optimizing algebraic structure depends on the cost function and the noise distribution.

### Table I

Examples of cost functions and noise distributions with \(\kappa_2 = \kappa_3\), \(P_{N_2} = P_{N_3}\), \(\tau_2 = \tau_3\) and \(R_2 = R_3\).

| Cost Functions \((\kappa_1, \kappa_2)\) | Cost \((\tau_1, \tau_2)\) | Noise pmfs \((P_{N_1}, P_{N_2})\) | \(R_2(F_7)\) | \(R_2(F_8)\) | \(R_2(\mathbb{Z}_4)\) | \(R_1\) |
|---|---|---|---|---|---|---|
| \([7.7572, 0.3170, 4.9891, 2.2048]\) | 0.8449 | \([0.0011, 0.0094, 0.0010, 0.9886]\) | 0.3300 | 0.1489 | 0.2556 | 0.8449 |
| \([0.2787, 0.3818, 0.3226, 0.6227]\) | 0.3300 | \([0.5777, 0.1423, 0.1002, 0.1798]\) | \(\text{N/A}\) | \(\text{N/A}\) | \(\text{N/A}\) | \(\text{N/A}\) |
| \([6.1610, 1.1621, 5.0165, 0.0283]\) | 0.2245 | \([0.8229, 0.0025, 0.1647, 0.0099]\) | 0.0006 | 0.2179 | 0.0000 | 0.2245 |
| \([0.1357, 0.2906, 0.3514, 0.2344]\) | 0.2179 | \([0.1255, 0.1043, 0.3293, 0.4409]\) | \(\text{N/A}\) | \(\text{N/A}\) | \(\text{N/A}\) | \(\text{N/A}\) |
| \([5.3368, 4.1262, 3.7326, 0.0100]\) | 0.1491 | \([0.0132, 0.0285, 0.0327, 0.9256]\) | 0.6241 | 0.2952 | 1.2832 | 0.1491 |
| \([1.4115, 1.9947, 1.1876, 0.9993]\) | 1.2832 | \([0.8752, 0.0290, 0.0034, 0.0924]\) | \(\text{N/A}\) | \(\text{N/A}\) | \(\text{N/A}\) | \(\text{N/A}\) |

For every triple \((P_{N_1}, \kappa, \tau)\), using Theorem 2 (and its extension to Abelian groups given in Section VI), one can find whether it is possible to attain our objective, and, if so, one can find what is the ‘winning’ finite field, or in general abelian group. We will restrict our attention to the following two finite fields and an abelian group: \(F_7\), \(F_8\) and \(\mathbb{Z}_4\). This requires appropriate maps from \(F_7\) and \(F_8\) to \(\mathbb{Z}_4\). By doing a computer search, we have obtained the following sample data (see Table I). The rates for the case of \(\mathbb{Z}_4\) is obtained by using theorem 5 from Section VI.

For example, for the distribution in the first row, all users achieve their respective capacities only with PCCs built on \(F_7\). Similarly PCCs built on \(F_8\) and \(\mathbb{Z}_4\) achieve optimality for the distributions of the second and third rows respectively. Note that even though the interference pattern is fixed, the optimizing algebraic structure depends on the cost function and the noise distribution.

### B. Step II: PCC rate region for a general discrete 3–IC using codes built over finite fields

In this section, we employ PCC to manage interference seen by every receiver. We describe the coding technique and provide a characterization of the corresponding achievable rate region. In the interest of brevity, we omit the proof of achievability. All the non-trivial elements have been detailed in the proof of theorem 2.

User \(j\) splits its message \(M_j\) of rate \(R_j = L_j + T_{ji} + T_{jk}\) into three parts \((M_{ji}^U, M_{jk}^U, M_{jX}^X)\), where \(i, j, k\) are distinct indices in \(\{1, 2, 3\}\). Let \(U_{ji} = F_\theta_i, U_{jk} = F_\theta_k\) be finite fields. Let \(\lambda_{ji} \subseteq U_{ji}\) denote an \((n, s_{ji}, t_{ji})\) PCC and \(\lambda_{jk} \subseteq U_{jk}\) denote an \((n, s_{jk}, t_{jk})\) PCC. If we let \(S_{ji} = \frac{s_{ji}}{n} \log \theta_i, T_{ji} = \frac{t_{ji}}{n} \log \theta_i\) and \(S_{jk} = \frac{s_{jk}}{n} \log \theta_k, T_{jk} = \frac{t_{jk}}{n} \log \theta_k\), then recall that \(\lambda_{ji}, \lambda_{jk}\) are coset codes of rates \(S_{ji}, S_{jk}\) partitioned into \(\exp\{nT_{ji}\}, \exp\{nT_{jk}\}\) bins respectively. Observe that cosets \(\lambda_{ji}\) and \(\lambda_{jk}\) are built over the same finite field \(F_{\theta_i}\). To contain the range the sum of these cosets, the larger of \(\lambda_{ji}, \lambda_{ki}\) contains the other. A codebook \(C_j\) of rate \(K_j + L_j\) is built over \(\lambda_j\). Codewords of \(C_j\) are partitioned into \(\exp\{nL_j\}\) bins. \(M_{ji}^U, M_{jk}^U\) and \(M_{jX}^X\) index bins in \(\lambda_{ji}, \lambda_{jk}\) and \(C_j\) respectively. Encoder looks for a triplet of codewords from the indexed bins that are jointly typical with respect to a pmf \(p_{U_{ji}, U_{jk}, X_j}\) defined on \(U_{ji} \times U_{jk} \times \lambda_j\). The corresponding codeword chosen from \(C_j\) is transmitted on the channel. Decoder \(j\) receives \(Y_j^n\) and looks for all triples \((u_{ij}^n, u_{jk}^n, x_j^n)\) of codewords in \(\lambda_{ji} \times \lambda_{jk} \times C_j\) for which there exists a \(u_{ij}^n \in (\lambda_{ij} \oplus \lambda_{ki})\) such that \((u_{ij}^n, u_{jk}^n, x_j^n, Y_j^n)\) are jointly typical with respect to \(p_{U_{ij} \oplus U_{kj}, U_{ji} \oplus U_{jk}, X_j, Y_j}\). If it finds all such triples in a unique triple of bins, the corresponding triple of bin indices is declared as decoded message of user \(j\). Otherwise,
an error is declared.

The distribution induced on the ensemble of codebooks is a simple generalization of that employed in proof of theorem 6. In particular, the codewords of \( C_j \) are chosen independently according to \( \prod_{i=1}^{n} p_{X_i|Q}(\cdot|q^i) \), where \( q^n \) is an appropriately chosen time sharing sequence. The three pairs \((A_{12}, A_{32}), (A_{21}, A_{31}), (A_{13}, A_{23})\) of random PCC are mutually independent. Within each such pair, (i) the generator matrix of the smaller PCC is obtained by choosing each of its rows uniformly and independently, and (ii) the generator matrix of the larger is obtained by appending the generator matrix of the smaller with an appropriately chosen number of mutually independent and uniformly distributed rows. All the vectors specifying the coset shifts are chosen independently and uniformly. Moreover, partitioning of all codes into their bins is effectuated uniformly and independently.

**Definition 7:** Let \( \mathbb{D}_f(\mathcal{Z}) \) denote the collection of probability mass functions \( \{p_{QUXY}\} \) defined on \( Q \times U \times X \times Y \), where (i) \( Q \) is an arbitrary finite set, (ii) \( U_{ij} = \mathcal{F}_{\theta_j} \) for each \( 1 \leq i, j \leq 3 \), and \( \mathcal{U} := U_{12} \times U_{13} \times U_{21} \times U_{23} \times U_{31} \times U_{32} \). (iii) \( U := (U_{12}, U_{13}, U_{21}, U_{23}, U_{31}, U_{32}) \), such that (i) the three quadruples \((U_{12}, U_{13}, X_1),\) \((U_{23}, U_{21}, X_2)\) and \((U_{31}, U_{32}, X_3)\) are conditionally mutually independent given \( Q \), (ii) \( p_{QUXY} = p_{QUX} = W_{QUX} \), (iii) \( \mathbb{E}\{\kappa_j(X_j)\} \leq \tau_j \) for \( j = 1, 2, 3 \).

For \( p_{QUXY} \in \mathbb{D}_f(\mathcal{Z}) \), let \( \alpha_f(p_{QUXY}) \) be defined as the set of rate triples \((R_1, R_2, R_3) \in [0, \infty)^3 \) for which there exists non-negative numbers \( S_{ij} : ij \in \{12, 13, 21, 23, 31, 32\}, T_{jk} : jk \in \{12, 13, 21, 23, 31, 32\}, K_j : j \in \{1, 2, 3\}, L_j : j \in \{1, 2, 3\} \) that satisfy \( R_1 = T_{12} + T_{13} + L_1, R_2 = T_{21} + T_{23} + L_2, R_3 = T_{31} + T_{32} + L_3 \) and

\[
S_{A_j} - T_{A_j} > \sum \log |U_{a_j}| + \log \|X_j\|_Q - H(U_{A_j}, X_j|Q),
\]

\[
S_{A_j} - T_{A_j} > \sum \log |U_{a_j}| - H(U_{A_j}|Q),
\]

\[
S_{A_j} < \sum \log |U_{a_j}| - H(U_{A_j}|Q, U_{A_j}, U_{ij} \oplus U_{k_j}, X_j, Y_j)
\]

\[
S_{A_j} + S_{ij} < \sum \log |U_{a_j}| + \log \theta_j - H(U_{A_j}, U_{ij} \oplus U_{k_j}|Q, U_{A_j}, X_j, Y_j)
\]

\[
S_{A_j} + S_{kj} < \sum \log |U_{a_j}| + \log \theta_j - H(U_{A_j}, U_{ij} \oplus U_{k_j}|Q, U_{A_j}, X_j, Y_j)
\]

\[
S_{A_j} + K_j + L_j < \sum \log |U_{a_j}| + H(X_j) - H(U_{A_j}, X_j|Q, U_{A_j}, U_{ij} \oplus U_{k_j}, Y_j)
\]

\[
S_{A_j} + K_j + L_j + S_{ij} < \sum \log |U_{a_j}| + \log \theta_j + H(X_j) - H(U_{A_j}, X_j, U_{ij} \oplus U_{k_j}|Q, U_{A_j}, Y_j)
\]

\[
S_{A_j} + K_j + L_j + S_{kj} < \sum \log |U_{a_j}| + \log \theta_j + H(X_j) - H(U_{A_j}, X_j, U_{ij} \oplus U_{k_j}|Q, U_{A_j}, Y_j)
\]

---

10The reader is encouraged to confirm that the distribution induced herein is a simple generalization of that employed in proof of theorem 6.

11Recall \( \mathcal{F}_{\theta_j} \) is the finite field of cardinality \( \theta_j \).
for every $A_j \subseteq \{ji, jk\}$ with distinct indices $i, j, k$ in $\{1, 2, 3\}$, where $S_{A_j} := \sum_{a_j \in A_j} S_{a_j}, U_{A_j} = \{U_{a_j} : a_j \in A_j\}$. Let

$$\alpha_f(\mathcal{T}) = \coel \left( \bigcup_{p_{QU,XY} \in \mathcal{P}_f(\mathcal{T})} \alpha_f(p_{QU,XY}) \right).$$

**Theorem 3**: For 3-IC $(X,Y,W_{Y|X},\kappa)$, $\alpha_f(\mathcal{T})$ is achievable, i.e., $\alpha_f(\mathcal{T}) \subseteq C(\mathcal{T})$.

Although the rate region given in Theorem 3 has many auxiliary random variables, we illustrate the key ideas by applying it to a carefully constructed channel and avoiding direct computation. The above coding technique presents an approach to simultaneously manage interference at all of the receivers. It is natural to question whether the use of structured codes to manage interference comes at a cost of respective individual communication. We now provide a simple generalization of example 1 that requires managing interference at two receivers. In contrast to [17], wherein the benefit of interference alignment can be exploited at all receivers, channels equipped with finite alphabets, in general, present a fundamental trade-off in managing interference and enabling individual respective communication.

**Example 5**: Consider a binary additive 3--to--1 IC illustrated in figure 4 with $X = Y = \{0, 1\} : j \in [3]$ with channel transition probabilities $W_{Y|X}(y|x) = BSC_{\delta_1}(y_1|x_1 \oplus x_2 \oplus x_3)BSC_{\delta_2}(y_2|x_2 \oplus x_3)BSC_{\delta_3}(y_3|x_3)$. Inputs of users 2 and 3 are not constrained, i.e., $\kappa_j(0) = \kappa_j(1) = 0$ for $j = 2, 3$. User 1’s input is constrained with $\kappa_1(x) = x$ for $x \in \{0, 1\}$ to an average cost of $\tau \in (0, \frac{1}{2})$ per symbol. Let $C(\tau)$ denote the capacity region of this 3--to--1 IC.

In order to illustrate the trade-off, let us consider the case $\delta = \delta_2 = \delta_3$ is arbitrarily close to, but greater than $\tau \ast \delta_1$. For example, one can choose $\delta_1 = 0.01, \tau = \frac{1}{8}$ and $\delta = 0.1326$. If receiver 1 desires communication at $h_b(\delta_1 \ast \tau) - h_b(\delta_1)$, it needs to decode $X_2 \oplus X_3$. To satisfy user 1’s desire, users 2 and 3 have two options. Either employ codes of rates $R_2$ and $R_3$ such that $R_2 + R_3 < 1 - h_b(\delta_1 \ast \tau)$, or employ cosets of the same code with a hope to boost individual rates. In the latter case, user 2 is hampered by the interference caused to it by user 3. While we do not provide a detailed analysis, we encourage the reader to contrast this to the Gaussian IC studied in [17], wherein the richness of the real field enables each receiver to exploit the benefits of alignment. We conjecture an inherent trade-off in the ability to manage interference over finite valued channels using coset codes, and enable individual respective communication. The reader is referred to [25], [26], [6] wherein a similar trade-off is discussed.

In the following we consider a 3-IC that is non-additive and uses non-uniform input distributions and all three users use structured codes to facilitate decoding of interference at all receivers.

**Example 6**: Consider a binary 3-IC with $X = Y = \{0, 1\} : j \in [3]$ with transition probabilities given by $Y_j = (X_j \land N_{j1}) \oplus (X_i \lor X_k) \oplus N_{j2}$ for $i, j, k \in [3]$, and $i, j$ and $k$ are distinct. This is depicted in figure 5. $N_{j1}, j \in [3], i \in [2]$ are mutually independent and independent of the inputs. The cost functions are given by $\kappa_j(i) = i$ for $j \in [3], i \in \{0, 1\}$. $P(N_{j1} = 1) = \beta$ and $P(N_{j2} = 1) = \delta$ for $j \in [3]$. We let $\mathbb{E}[\kappa_j(X_j)] \leq \tau$. In this channel every user suffers from non-linear interference. Moreover all inputs are constrained by a cost function. To make the
example tractable we wish to operate in the high interference regime, and hence we have chosen a Z-channel in the
signal path from the transmitter to the respective receiver. We consider the projection of the capacity region along
the line $R_1 = R_2 = R_3 = R$, and constrain each user to achieve the corresponding PTP capacity. We employ PCC
built on $\mathbb{F}_3$ as was done before. Using the rate region given in theorem 3 for this example, we get the following:

$$R \leq \frac{1}{2} I(X_1; Y_1 | X_2 \lor X_3) + \frac{1}{2} \min \{ I(X_1; Y_1 | X_2 \lor X_3), H(X_2) - H(X_2 \oplus_3 X_3 | Y_1) \} \tag{12}$$

All the three users can achieve their respective PTP capacities if

$$I(X_1; Y_1 | X_2 \lor X_3) \leq H(X_2) - H(X_2 \oplus_3 X_3 | Y_1).$$

It can be verified that the choice $\delta = 0.1$, $\tau = 0.1284$ and $\beta = 0.2210$ satisfies the condition. Hence it is possible
for all the users to attain interference alignment and thus achieve their respective capacities using PCC built on $\mathbb{F}_3$.

In the following we consider an example that illustrates the trade-off between the rates of two users who suffer
from interference with the third user helping one of them. This is referred to as $3$–to–$2$ IC.

**Example 7:** Consider a binary 3-IC with $X_j = Y_j = \{0, 1\}$ : $j \in [3]$ with transition probabilities given by

$$Y_1 = (X_1 \land N_{11}) \oplus (X_2 \oplus X_3) \oplus N_{12}, \quad Y_2 = (X_2 \land N_{21}) \oplus (X_1 \lor X_3) \oplus N_{22}, \quad \text{and} \quad Y_3 = X_3 \oplus N_3.$$ 

All noise components are mutually independent and independent of the inputs. $\kappa_j(i) = i$ for $j \in [3]$ and $i \in \{0, 1\}$.

$$P(N_{12} = 1) = P(N_{22} = 1) = P(N_3 = 1) = \delta, \quad \text{and} \quad P(N_{11} = 1) = P(N_{21} = 1) = \beta.$$ 

We let $E(\kappa_j(X_j)) \leq \tau$ for $j \in [3]$. Note that user 1 and 2 suffer from XOR and logical-OR interference from the other two users, respectively. The dilemma of user 3 is that it can choose to help (i) user 1 by using PCCs built on $\mathbb{F}_2$ and by collaborating with user 2 or (ii) user 2 by using PCCs built on $\mathbb{F}_3$ and by collaborating with user 1, but not both. As in the previous example, to operate in the high interference regime we have chosen the Z-channel between $X_j$ and $Y_j$ for $j = 1, 2$. We evaluate the rates of the users at these two ends of the spectrum of this trade-off. Applying theorem 3 on this example, we get constraints on the rates of the three users. We state these in the following only for the
first operating point for conciseness:

\[
\max\{R_2, R_3\} \leq h(\tau) + h(\tau \ast \tau \ast \delta \ast \tau \beta) - h(\tau \ast \tau) - h(\tau \beta \ast d) \tag{13}
\]

\[
R_3 \leq h(\tau \ast \delta) - h(\delta), \quad R_1 \leq h(\tau \beta \ast \delta) - (1 - \tau)h(\delta) - \tau h(\beta \ast \delta) \tag{14}
\]

\[
R_2 \leq h(\tau \beta \ast \delta \ast (2\tau - \tau^2)) - (1 - \tau)h(2\tau - \tau^2 \ast \delta) - \tau h(\beta \ast (2\tau - \tau^2) \ast \delta) \tag{15}
\]

We provide the following data as a function of \(\tau\) (see Table II). In the first operating point, we look at the corner point when \(R_1\) is maximized. In the second, we look at the corner point when \(R_2\) is maximized. One can see the trade-off between \(R_1\) and \(R_2\). One can also contrast between XOR and logical-OR interference. It is much harder to tackle the latter as can be seen from the rates of user 3.

**C. Step III: Enlarging the PCC rate region using unstructured codes**

Let us describe a coding technique that unifies both unstructured and partitioned coset codes. We follow the approach of Ahlswede and Han [23, Section VI]. Refer to figure 6 for an illustration of the random variables involved. Each user splits its message into 5 parts. The \(W\)-random variable is decoded by all users. In addition, each user decodes a univariate component of the message of the other users. This is represented by the random variable \(V\). Furthermore, it decodes a bivariate interference component denoted using \(U\). Lastly, each decoder decodes all parts of its intended message. Clearly, a description of the above rate region is involved. In the sequel, we illustrate the key elements via a simplified achievable rate region. In particular, we employ PCC and unstructured codes to manage interference seen by only one receiver, say receiver 1 and state the corresponding achievable rate region. We begin with a description of the same.

**Definition 8:** Consider a 3-IC \((\mathcal{X}, \mathcal{Y}, \mathcal{W}, \mathcal{V}_1, \mathcal{V}_2, \mathcal{U})\). Let \(\mathcal{D}_{uf}(\tau)\) denote the collection of distributions \(p_{QUV_2V_3XU}V_1XY\) defined over \(Q \times U_2 \times V_2 \times U_3 \times V_3 \times X \times Y\), where \(U_2 = U_3\) is a finite field and \(V_2\) and \(V_3\) are finite sets, such

| \(\tau\) | user 2 and 3 help user 1 | user 1 and 3 help user 2 |
|---|---|---|
| 0.1 | \(R = [0.0383, 0.0012, 0.3295]\) | \(R = [0.0021, 0.0383, 0.1360]\) |
| 0.2 | \(R = [0.0477, 0.0000, 0.4067]\) | \(R = [0.0005, 0.0477, 0.0570]\) |
| 0.3 | \(R = [0.0520, 0.0018, 0.4364]\) | \(R = [0.0000, 0.0520, 0.0000]\) |
that (i) \( p_{Y_j|U_jV_jV_3} = W_{Y_j|X_j} \), (ii) \( X_j, (U_2, V_2, X_2) \) and \( (U_3, V_3, X_3) \) are conditionally independent given \( Q \), (iii) \( \mathbb{E}\{\kappa_j(X_j)\} \leq \tau_j \) for \( j = 1, 2, 3 \). For \( p_{QU_2V_2V_3XY} \in \mathcal{D}_{uf}(\tau) \), let \( \alpha_{uf}^{3-1}(p_{QU_2V_2V_3XY}) \) be defined as the set of rate triples \( (R_1, R_2, R_3) \in [0, \infty)^3 \) for which \( S_{uf}(p_{QU_2V_2V_3XY}, \mathcal{R}) \) is non-empty, where \( S_{uf}(p_{QU_2V_2V_3XY}, \mathcal{R}) \) is defined as the vectors \( (S_{j1}, T_{j1}, S_{j2}, T_{j2}, L_j : j = 2, 3) \in [0, \infty)^{10} \) that satisfy

\[
S_{j2} - T_{j2} > \log \theta - H(U_j|V_j, Q), \quad R_j = T_{j1} + T_{j2} + L_j : j = 2, 3
\]

\[
L_j < I(X_j; Y_j|V_j, Q), \quad T_{j1} + S_{j2} + L_j < \log \theta - H(U_j|V_j, Q) + I(V_j, X_j; Y_j|U_j, Q) : j = 2, 3
\]

\[
R_1 < I(X_1; Y_1, V_2, V_3, U_2 \oplus U_3|Q), \quad R_k < \log \theta - H(U_2 \oplus U_3|V_3, Q) + I(X_1, U_2 \oplus U_3; V_2, V_3, Y_1|Q) : j = 2, 3
\]

\[
R_1 + T_{j1} < I(X_1, V_j; V_2 \oplus U_3, Y_1|Q) : j = 2, 3, \quad T_{21} + T_{31} + R_1 < I(V_2, V_3, X_2; U_2 \oplus U_3, Y_1|Q)
\]

where \( \theta = |U_2| = |U_3| \). Let

\[
\alpha_{uf}^{3-1}(\tau) = \text{cocl} \left( \bigcup_{p_{QU_2V_2V_3XY} \in \mathcal{D}_{uf}(\tau)} \alpha_{uf}^{3-1}(p_{QU_2V_2V_3XY}) \right)
\]

**Theorem 4:** For 3-IC \((\mathcal{X}, \mathcal{Y}, W_{Y|X}, \kappa)\), \( \alpha_{uf}^{3-1}(\tau) \) is achievable, i.e., \( \alpha_{uf}^{3-1}(\tau) \subseteq \mathbb{C}(\tau) \).

We provide a brief sketch of achievability. For simplicity, user 1 builds an unstructured independent code of rate \( R_1 \) over \( \mathcal{X}_1 \) by choosing codewords independently and identically according to \( p^n_{X_1} \). For \( j = 2, 3 \), user \( j \) builds three random codebooks - one each over \( V_j, U_j, X_j \) respectively. An unstructured and independent codebook of rate \( T_{j1} \) is built over \( V_j \) by choosing codewords independently and identically according to \( p^n_{V_j} \). A random PCC \( (n, nS_{j2}/\log \theta, nT_{j2}/\log \theta, G_j, B_j, I_j) \), denoted \( \Lambda_j \), is built over \( U_j \). As before the PCC’s of users 2 and 3 overlap, i.e., if \( j_1 \leq j_2 \), then \( g_{j_2}^T = [g_{j_1}^T, g_{j_2-j_1}^T] \). Consider a codeword in \( V_j \)-codebook and a bin in the PCC. For every such pair, a random unstructured independent codebook is constructed over \( X_j \).

User \( j \)th message is split into three parts - **univariate** part, **bivariate** part and **private** part. The univariate part indexes a codeword, say \( V_j^n(M_{jV}) \) in \( V_j \)-codebook. The bivariate part indexes a bin in the PCC. A codeword, say \( U_j^n(M_{jU}) \) is chosen in the indexed bin such that \( (V_j^n(M_{jV}), U_j^n(M_{jU})) \) is jointly typical according to the probability distribution \( p_{QU_jV_j} \), the marginal of \( p_{QU_2V_2V_3XY} \in \mathcal{D}_{uf}(\tau) \) in question. The codewords of the codebook built over \( X_j \), corresponding to \((M_{jV}, M_{jU})\), are independently and identically distributed according to \( p_{X_j|U_jV_j}^{n}(\cdot|V_j^n(M_{jV}), U_j^n(M_{jU})) \). The private part \( M_{jX} \) indexes a codeword in this codebook. This codeword is input on the channel by user \( j \). User 1 inputs the codeword from its \( X_1 \)-codebook that is indexed by its message. It can be verified that the inequality in [16] ensures users 2 and 3 find jointly typical triples of codewords.

Users 2 and 3 employ a simple point-to-point decoding technique. However, note that the codebook over \( X_j \) is conditionally built. Therefore, an error in decoding the correct \( U_j \) or \( V_j \)-codeword is interpreted as an error even
in decoding the $X_j$–codeword. It can be verified that (17), (18) ensure the probability of decoding error at receiver $j$ decays exponentially with block length $n$.

User 1 constructs the sum codebook $\Lambda_2 \oplus \Lambda_3 := \{ u_2^n \oplus u_3^n : u_j^n \in \Lambda_j : j = 2, 3 \}$ and decodes into $V_2, V_3, \Lambda_2 \oplus \Lambda_3, X_1$ codebooks. In particular it looks for a quadruple of codewords in these codebooks that are jointly typical with the received vector $Y_1^n$ according to $p_{QV_2,V_3,U_2\oplus U_3|Y_1}$. It can be verified that (19) - (21) imply the probability of decoding error at receiver 1 decays exponentially with block length.

**Example 8:** We briefly describe an example wherein the above coding technique can yield larger achievable rate regions than ones based exclusively either on PCC or on unstructured based codes. Consider the 3–IC depicted in figure 7. For each $j = 1, 2, 3$, the input alphabet $X_j = \times_{k=1}^3 X_{jk}$ and output alphabet is $Y_j = \times_{k=1}^3 Y_{jk}$ where $X_{jk} = Y_{jk} = \{0, 1\}$. Essentially, each user can input three binary digits on the channel and each receiver observes three binary digits per channel use. Let $X_{jk} : k = 1, 2, 3$ denote the three binary digits input by transmitter $j$ and $Y_{jk} : k = 1, 2, 3$ denote the three digits observed by receiver $j$. Figure 7 depicts the input-output relationship. Let us also assume the Bernoulli noise processes $N_{jk} : j = 1, 2, 3, k = 1, 2, 3$ are mutually independent. Users 2 and 3 enjoy complete free point-to-point links for each of the digits. They are only constrained by noise that is modeled by the corresponding Bernoulli noise processes. Receiver 1’s digit $Y_{11}$ experiences bivariate interference. Its 2nd the 3rd digits experience univariate interference. The reader will recognize the need for receiver 1 to decode univariate and bivariate parts of user 2 and 3’s signals. The above coding technique enables the same.

We conclude this section with a discussion, wherein, we employ the notion of common information to argue, more fundamentally, the need to decode bivariate interference components. Let us view the above coding technique from the perspective of common information in the sense of Gacs, Körner and Witsenhausen [27, 28]. Let $K(A; B)$ denote the common information of two random variables $A$ and $B$. Let $\hat{X}_j$ denote the collection of random

---

The IC depicted in figure 7 can be used to model a scenario wherein Tx-Rx pair 1 is assigned frequency bands around carrier frequencies $f_1, f_2, f_3$. Tx-Rx pair 2 is assigned frequency bands around carrier frequencies $f_1, f_2, f_4$, Tx-Rx pair 3 is assigned frequency bands around carrier frequencies $f_1, f_3, f_5$ respectively. If the powers transmitted by users 2 and 3 are large, then user 1 does not cause any appreciable interference to users 2 and 3. The interference caused by signals of Txs 2 and 3 on each other in frequency band around $f_1$ has been ignored by this model.
variables decoded at decoder $j$. The CHK scheme for 2-IC \cite{2} can be interpreted as inducing non-trivial common information between $X_1$ and $X_2$, and $K(X_1; X_2) = H(W_1, W_2)$. The question that comes next is how to extend common information to 3 random variables? We can consider the following vector as the common information among three random variables $A$, $B$ and $C$:

$$[K(A; B; C), K(A; B), K(B; C), K(C; A)],$$

where $K(A; B; C)$ is defined in a natural way. We refer to this as univariate common information as they are characterized using univariate function of the random variables. The $\mathcal{SB}$–technique induces non-trivial univariate common information among $\tilde{X}_1$, $\tilde{X}_2$ and $\tilde{X}_3$, and

$$K(\tilde{X}_1; \tilde{X}_2; \tilde{X}_3) = H(W_1, W_2, W_3), \quad K(\tilde{X}_j; \tilde{X}_k) = H(V_{kj}, V_{jk}).$$

The common information captured via univariate functions can be enhanced with the following components captured via bivariate functions. Define

$$\tilde{K}(A, B; C) := \sup \inf \{H(V_1|V_2) : f_1: A \rightarrow V_1, f_2: B \rightarrow V_2; h, g : V_1 \times V_2 \rightarrow \psi \}.$$  

We define common information among three random variables as a seven-dimensional vector as follows:

$$[K(A; B; C), K(A; B), K(B; C), K(C; A), \tilde{K}(A, B; C), \tilde{K}(B, C; A), \tilde{K}(C, A; B)].$$

We refer to the last three components as bivariate common information. Note that the $\mathcal{SB}$–technique induces non-trivial bivariate common information among $\tilde{X}_1$, $\tilde{X}_2$ and $\tilde{X}_3$. The PCC technique induces non-trivial bivariate common information among them, and $\tilde{K}(\tilde{X}_1; \tilde{X}_2; \tilde{X}_3) = H(U_{ik} \oplus U_{jk})$ for all distinct $i, j, k$.

**VI. Step IV: Achievable rate region using PCC built over Abelian groups**

In this section, we present PCC scheme using codes built on Abelian groups. The rate region we get can be interpreted as an algebraic extension (from finite fields to Abelian groups) of that given in theorem \cite{2}.

**A. Definitions**

For an Abelian group $G$, let $\mathcal{P}(G)$ denote the set of all distinct primes which divide $|G|$ and for a prime $p \in \mathcal{P}(G)$ let $S_p(G)$ be the corresponding Sylow subgroup of $G$. It is known \cite{29} Theorem 3.3.1] that any Abelian group $G$ can be decomposed in the following manner

$$G \cong \bigoplus_{p \in \mathcal{P}(G)} S_p(G) = \bigoplus_{p \in \mathcal{P}(G)} \bigoplus_{r \in \mathcal{R}_p(G)} \mathbb{Z}_{p^r}^{M_{p,r}} = \bigoplus_{p \in \mathcal{P}(G)} \bigoplus_{r \in \mathcal{R}_p(G)} \bigoplus_{m=1}^{M_{p,r}} \mathbb{Z}_{p^r}^{(m)} = \bigoplus_{(p,r,m) \in \mathcal{G}(G)} \mathbb{Z}_{p^r}^{(m)}, \quad (22)$$

where $\mathcal{R}_p(G) \subseteq \mathbb{Z}^+$ and for $r \in \mathcal{R}_p(G)$, $M_{p,r}$ is a positive integer, $\mathcal{G}(G) \subseteq \mathbb{P} \times \mathbb{Z}^+ \times \mathbb{Z}^+$ is defined as:

$$\mathcal{G}(G) = \{(p, r, m) \in \mathbb{P} \times \mathbb{Z}^+ \times \mathbb{Z}^+ | p \in \mathcal{P}(G), r \in \mathcal{R}_p(G), m \in \{1, 2, \cdots, M_{p,r}\}\}$$

With a slight abuse of notation, we represent an element $a$ of $G$ as

$$a = \bigoplus_{(p,r,m) \in \mathcal{G}(G)} a_{p,r,m}$$
We will need to define information theoretic quantities in relation to groups. Define

\[ Q(G) = \{(p, r) | p \in \mathcal{P}(G), r \in \mathcal{R}_p(G)\} \]

Consider vectors \( \hat{\theta}, w \) and \( \theta \), with components, indexed by \( (p, r) \in Q(G) \), given by \( \hat{\theta}_{p,r}, w_{p,r} \) and \( \theta_{p,r} \) respectively. \( w \) is a pmf on \( Q(G) \), \( \hat{\theta}_{p,r} \) is a non-negative integer with \( 0 \leq \hat{\theta}_{p,r} \leq r \), and \( \theta \) is defined as

\[
\theta(\hat{\theta})_{(p, r) \in Q(G)} = \min_{s: (p, s) \in Q(G)} |r - s|^+ + \hat{\theta}_{p,s}.
\]

It turns out that only certain subgroups of \( G \) become important in the achievable rate region when we use Abelian group codes. Define

\[
\Theta = \left\{ \theta(\hat{\theta}) | (\hat{\theta}_{q,s}, (q, s) \in Q(G) : 0 \leq \hat{\theta}_{q,s} \leq s) \right\}.
\]

For \( \theta \in \Theta \), define

\[
\omega_\theta = \frac{\sum_{(p, r) \in Q(G)} \theta_{p,r} w_{p,r} \log p}{\sum_{(p, r) \in Q(G)} r w_{p,r} \log p}, \quad H_\theta = \sum_{(p, r, m) \in Q(G)} p^{\theta_{p,r} z_{p,r}^{(m)}} \leq G.
\]

We give an example in the sequel. Let \( X \) and \( Y \) be two random variables with \( X \) taking values over \( G \) and let \( [X]_\theta = X + H_\theta \) be the random variable taking values from the cosets of \( H_\theta \) in \( G \) that contains \( X \). We define the source coding group mutual information between \( X \) and \( Y \) as

\[
S^G_w(X; Y) = H(X) - \log |G| + \max_{\theta \in \Theta} \frac{1}{\omega_\theta} \log |G : H_\theta| - H([X]_\theta|Y)]
\]

where \( \Theta \) is a vector whose components are indexed by \( (p, r) \in Q(G) \) and whose \( (p, r)^{th} \) component is equal to 0, and \( G : H_\theta \) is the quotient group. We define the channel coding group mutual information between \( X \) and \( Y \) as

\[
C^G_w(X; Y) = H(X) - \log |G| + \min_{\theta \neq \theta'} \frac{1}{1 - \omega_\theta} \left[ \log |G : H_\theta| - H(X|[X]_\theta,Y) \right]
\]

where \( \mathbf{r} \) is a vector whose components are indexed by \( (p, r) \in Q(G) \) and whose \( (p, r)^{th} \) component is equal to \( r \).

For example, let \( G = Z_2 \oplus Z_8 \oplus Z_3 \). In this case, we have \( \mathcal{P}(G) = \{2, 3\}, \mathcal{R}_2(G) = \{1, 3\}, \mathcal{R}_3(G) = \{1\} \) and \( Q(G) = \{ (2, 1), (2, 3), (3, 1) \} \). The vectors \( w, \hat{\theta} \) and \( \theta \) are represented by \( w = (w_{2,1}, w_{2,3}, w_{3,1}) \), \( \hat{\theta} = (\hat{\theta}_{2,1}, \hat{\theta}_{2,3}, \hat{\theta}_{3,1}) \) and \( \theta = (\theta_{2,1}, \theta_{2,3}, \theta_{3,1}) \) and the function \( \theta(\cdot) \) is given by

\[
\theta(\hat{\theta}) = \left( \min(\hat{\theta}_{2,1}, \hat{\theta}_{2,3}), \min(2 + \hat{\theta}_{2,1}, \hat{\theta}_{2,3}), \hat{\theta}_{3,1} \right)
\]

The set \( \Theta \) turns out to be equal to

\[
\Theta = \left\{ (0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (0, 2, 0), (0, 2, 1), (1, 1, 0), (1, 1, 1), (1, 2, 0), (1, 2, 1), (1, 3, 0), (1, 3, 1) \right\}
\]

and we have \( \Theta = (0, 0, 0) \) and \( \mathbf{r} = (1, 3, 1) \). For \( \theta = (1, 1, 0) \), we have \( \omega_\theta = \frac{w_{2,1} + w_{2,3}}{w_{2,1} + w_{2,3} + w_{3,1} \log 3} \) and \( H_\theta = 0 \oplus 2Z_8 \oplus Z_3 \). so that the random variable \([X]_\theta \) takes values from the set of cosets \( 0 \oplus 2Z_8 \oplus Z_3, 0 \oplus (1 + 2Z_8) \oplus Z_3, 1 \oplus 2Z_8 \oplus Z_3, 1 \oplus (1 + 2Z_8) \oplus Z_3 \). Furthermore, for this choice of \( \theta \), we have \(|H_\theta| = 12\) and \(|G : H_\theta| = 4\).
When $G$ is cyclic, i.e., $G = \mathbb{Z}_p^r$, then $w = 1$ and it can be shown that

$$S_w^G(X;Y) = H(X) - \min_{1 \leq \theta \leq r} \frac{r}{\theta} H([X]_{\theta}|Y), \quad C_w^G(X;Y) = H(X) - \max_{0 \leq \theta \leq (r-1)} \frac{r}{\theta} H(X|[X]_{\theta},Y),$$

When $G$ is a primary field, i.e., $G = \mathbb{Z}_p$, then it follows that $S_w^G(X;Y) = I(X;Y) = C_w^G(X;Y)$.

### B. Managing interference seen by one receiver using PCC built over Abelian groups

In this section, we employ PCC built over Abelian groups to manage interference seen by only receiver 1. As the reader might have guessed, receiver 1 decodes the group sum of codewords chosen by receivers 2 and 3. In the following, we characterize an achievable rate region using codes built over groups.

**Definition 9:** Let $\mathcal{D}_g(\mathcal{Z})$ denote the collection of pairs consisting of a distribution $p_{QU_3XY}$ defined over $Q \times U_2 \times U_3 \times X \times Y$, where $U_2 = U_3$ is an Abelian group $G$, and a distribution $w$ on $Q(G)$ satisfying the following conditions: (i) $p_{QU_3X} = W_{|X|,X}$, (ii) $X_1, (U_2, X_2)$ and $(U_3, X_3)$ are conditionally mutually independent given $Q$ and (iii) $\mathbb{E}\{\kappa_j(X_j)\} \leq \tau_j : j \in [3]$ and (iv) $I(X_j;Y_j,Q,U_j) + C_w^G(U_j;Y_j|Q) - S_w^G(U_j;0|Q) \geq 0$ for $j = 2, 3$. For $(p_{QU_3XY}, w) \in \mathcal{D}_g(\mathcal{Z})$, let $\alpha_g^{3-1}(p_{QU_3XY}, w)$ be defined as the set of rate triples $(R_1, R_2, R_3) \in [0, \infty)^3$ that satisfy

$$R_1 < I(X_1;Y_1|QZ) - H(Z|Q) + \min\{H(Z|Q), H(U_j|Q) + C_w^G(Z;Y_1|Q) - S_w^G(U_j;0|Q) : j = 2, 3\}$$

$$R_j < I(X_j;Y_j|QU_j) + C_w^G(U_j;Y_j|Q) : j = 2, 3,$$

$$R_1 + R_j < I(X_1;Y_1|QZ) + C_w^G(Z;Y_1|Q) + H(U_j|Q) - H(Z|Q) + I(X_j;Y_j|QU_j)$$

$$+ \min\{0, C_w^G(U_j;Y_j|Q) - S_w^G(U_j;0|Q)\} : j = 2, 3,$$

where $Z = U_2 \oplus U_3$, and

$$\alpha_g^{3-1}(\mathcal{Z}) = \text{cocl} \left( \bigcup_{(p_{QU_3XY}, w) \in \mathcal{D}_g(\mathcal{Z})} \alpha_g^{3-1}(p_{QU_3XY}) \right).$$

**Theorem 5:** For $3$–IC $(X, Y, W_{|X|,X}, \mathcal{Z})$, the set $\alpha_g^{3-1}(\mathcal{Z})$ is achievable, i.e., $\alpha_g^{3-1}(\mathcal{Z}) \subseteq \mathcal{C}(\mathcal{Z})$.

The proof is given in Appendix 1. We now illustrate the need to build codes over appropriate algebraic objects to enable interference management. In other words, we provide an example where codes built over groups outperform unstructured codes as well as codes built over finite fields.\(^\text{13}\)

**Example 9:** Consider a quaternary $3$–to–$1$ IC with input and output alphabets $X_j = Y_j = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ being the Abelian group of cardinality 4. Let $\oplus_4$ denote the group operation, i.e., addition mod–4 in $\mathbb{Z}_4$. The channel transition probabilities are described through the relation $Y_1 = X_1 \oplus_4 X_2 \oplus_4 X_3 \oplus_4 N_1, Y_2 = X_2 \oplus_4 N_2$ for $j = 2, 3$ such that (i) $N_1, N_2, N_3$ are independent random variables taking values in $\mathbb{Z}_4$ with $P(N_j = 0) = 1 - \delta_j$ and $P(N_j = i) = \frac{\delta_j}{3}$ for $i, j = 1, 2, 3$. Inputs $X_2, X_3$ of users 2 and 3 are not constrained, i.e., $\kappa_j(x_j) = 0$ for

\(^{13}\)While, we do not provide a proof of the statement that codes built over groups outperform PCC built over finite fields, this can be recognized through standard arguments.
\( j = 2, 3 \) and any \( x_j \in \mathcal{X}_j \), whereas \( \kappa_1(x_1) = 1 \) if \( x_1 \in \{1, 2, 3\} \) and \( \kappa_1(0) = 0 \). User 1’s input is constrained to a
average cost of \( \tau \) per symbol.

The reader will recognize that the 3–to–1 IC described in example 9 is analogous to that in example 1 with the
binary field replaced by Abelian group \( \mathbb{Z}_4 \). For simplicity, let us henceforth assume \( \delta_2 = \delta_3 = \delta \). Since users 2 and 3 enjoy interference free point-to-point links, we let them communicate at their respective capacities. This is
possible even while using PCC built on \( \mathbb{Z}_4 \) because if we choose \( U_j = X_j \) and put a uniform distribution on \( X_j \)
for \( j = 2, 3 \), we get the group capacity as

\[
C^G_u(X_j; U_j) = \min\{2 - h_b(\delta) - \delta \log_2(3), 2 + 2h_b(2\delta/3) - 2h_b(\delta) - 2\delta \log_2(3)\} = 2 - h_b(\delta) - \delta \log_2(3),
\]

where the last equality follows from the concavity of entropy. Clearly, user 1 can achieve a rate not greater than
\( C^* := \sup_{P_{X_1}:P_{X_1}(1) \leq \tau} I(X_1; Y_1|X_2 \oplus_4 X_3) \). The following proposition states that \( C^* \) is achievable by group codes
but not by unstructured codes. Our approach is similar to that of section IV. The proof is provided in Appendix J.

**Proposition 4:** Consider the 3–to–1 IC described in example 9 with \( \delta_2 = \delta_3 = \delta \in (0, \frac{1}{4}), \delta_1 \in (0, \frac{1}{2}) \) and \( \tau < \frac{3}{4} \). If \( \delta_1, \tau \) and \( \delta \) are such that

\[
C^* + 2(2 - h_b(\delta) - \delta \log_2(3)) > 2 - h_b(\delta_1) - \delta_1 \log_2(3),
\]

then the rate triple \( (C^*, 2 - h_b(\delta) - \delta \log_2(3), 2 - h_b(\delta) - \delta \log_2(3)) \notin \alpha_u(\tau, 0, 0) \). Moreover, if in addition \( \beta \triangleq \delta_1 + \tau - \frac{4h_b\tau}{3} \leq \delta \), then group codes achieve capacity, i.e., \( (C^*, 2 - h_b(\delta) - \delta \log_2(3), 2 - h_b(\delta) - \delta \log_2(3)) \in \alpha_g(\tau, 0, 0) = \mathcal{C}(\tau, 0, 0) \).

It can be shown that there exists a non-empty set of parameters \( (\delta, \delta_1, \tau) \) that satisfy these conditions. An example is given by \( \delta = \frac{1}{8}, \delta_1 = \tau = \frac{3}{4} - \frac{\sqrt{3}\pi}{8} \).

**ACKNOWLEDGEMENT**

We thank the anonymous reviewers for their insightful comments that have helped us to improve our manuscript considerably.

**APPENDIX A**

**Proof of proposition 1**

We only need to prove the second statement. If \( H(X_j|Q, U_j) = 0 \) for \( j = 2, 3 \), then the upper bound in (2)
reduces to \( R_1 + R_2 + R_3 \leq I(X_2X_3X_1; Y_1|Q) \leq 1 - h_b(\delta_1) \). From the hypothesis, we have \( h_b(\tau \delta_1) - h_b(\delta_1) + 1 - h_b(\delta_2) + 1 - h_b(\delta_3) > 1 - h_b(\delta_1) \) which violates the above upper bound and hence the theorem statement is true.

Henceforth, we assume \( H(X_j|Q, U_j) > 0 \) for \( j = 2 \) or \( j = 3 \). Let us assume \( j, \neq j \) are distinct elements in \( \{2, 3\} \)
and \( H(X_j|Q, U_j) > 0 \). Since \( (U_2, X_2) \) and \( (U_3, X_3) \) are conditionally independent given \( Q \), we have

\[
0 < H(X_j|Q, U_j) = H(X_j|X_{\neq j}, Q, U_2, U_3) = H(X_2 \oplus X_3|X_{\neq j}, Q, U_2, U_3) \leq H(X_2 \oplus X_3|Q, U_2U_3).
\]
The univariate components $U_2, U_3$ leave residual uncertainty in the interfering signal and imply the existence of a $\hat{q}^* = (q^*, u_2^*, u_3^*) \in \hat{Q} : = Q \times U_2 \times U_3$ for which $H(X_2 \oplus X_3)(Q, U_2 U_3) = \hat{q}^* > 0$. Under this condition, we prove that the upper bound \[1\] on $R_1$ is strictly smaller than $h_b(\tau * \delta_1) - h_b(\delta_1)$. Towards that end, we prove a simple observation based on strict concavity of binary entropy function.

**Lemma 1:** If $Z_j : j \in [3]$ are binary random variables such that (i) $H(Z_1) \geq H(Z_2)$, (ii) $Z_3$ is independent of $(Z_1, Z_2)$, then $H(Z_1) - H(Z_2) \geq |H(Z_1 \oplus Z_3) - H(Z_2 \oplus Z_3)|$. Moreover, if $H(Z_1) > H(Z_2)$ and $H(Z_3) > 0$, then the inequality is strict, i.e., $H(Z_1) - H(Z_2) > |H(Z_1 \oplus Z_3) - H(Z_2 \oplus Z_3)|$.

**Proof:** Note that, if either $H(Z_1) = H(Z_2)$ or $H(Z_3) = 0$, then $H(Z_1) - H(Z_2) = H(Z_1 \oplus Z_3) - H(Z_2 \oplus Z_3)$.

We therefore assume $H(Z_1) > H(Z_2)$ and $H(Z_3) > 0$ and prove the case of strict inequality. For $j \in [3]$, let \( \{p_{Z_j}(0), p_{Z_j}(1)\} = \{\delta_j, 1 - \delta_j\} \) with $\delta_j \in [0, \frac{1}{2}]$, $\delta_3 > 0$. Define $f : [0, \frac{1}{2}] \to [0, 1]$ as $f(t) = h_b(\delta_1 * t) - h_b(\delta_2 * t)$. It suffices to prove $f(0) > f(\delta_3)$. By the Taylor series, $f(\delta_3) = f(0) + \delta_3 f'(\zeta)$ for some $\zeta \in [0, \delta_3]$ and therefore it suffices to prove $f'(t) < 0$ for $t \in (0, \frac{1}{2})$.

It may be verified that

\[
f'(t) = (1 - 2\delta_1) \log \frac{1 - \delta_1}{\delta_1} - (1 - 2\delta_2) \log \frac{1 - \delta_2}{\delta_2}, \quad \text{where} \quad \delta_j = \delta_j + t(1 - 2\delta_j) : j \in [2].
\]

Note that (i) $0 \leq (1 - 2\delta_1) < (1 - 2\delta_2) \leq 1$, (ii) $\delta_2 \leq \delta_j + \frac{1}{2}(1 - 2\delta_j) \leq \frac{1}{2}$, (iii) since $\delta_1 > \delta_2$ and $t \leq \frac{1}{2}, \delta_1 - \delta_2 = (\delta_1 - \delta_2)(1 - 2t) \geq 0$. We therefore have $0 \leq \delta_2 \leq \delta_1 \leq \frac{1}{2}$ and thus $\log \frac{1 - \delta_2}{\delta_2} \geq \log \frac{1 - \delta_1}{\delta_1}$. Combining this with the first observation, we conclude $(1 - 2\delta_2) \log \frac{1 - \delta_2}{\delta_2} > (1 - 2\delta_1) \log \frac{1 - \delta_1}{\delta_1}$ which implies $f'(t) < 0$ for $t \in (0, \frac{1}{2})$.

We are now equipped to work with the upper bound \[1\] on $R_1$. Denoting $\hat{Q} : = (Q, U_2, U_3)$ and a generic element $\hat{q} : = (q, u_2, u_3) \in \hat{Q} : = Q \times U_2 \times U_3$, we observe that

\[
I(X_1; Y_1 | \hat{Q}) = \sum_q p_{\hat{Q}}(\hat{q})H(X_1 \oplus N_1 \oplus X_2 \oplus X_3 | \hat{Q} = \hat{q}) - \sum_{x_1, \hat{q}} p_{X_1, \hat{Q}}(x_1, \hat{q})H(N_1 \oplus X_2 \oplus X_3 | \hat{Q} = \hat{q}) \tag{26}
\]

\[
= \sum_q p_{\hat{Q}}(\hat{q})H(X_1 \oplus N_1 \oplus X_2 \oplus X_3 | \hat{Q} = \hat{q}) - \sum_q p_{\hat{Q}}(\hat{q})H(N_1 \oplus X_2 \oplus X_3 | \hat{Q} = \hat{q})
\]

\[
< \sum_q p_{\hat{Q}}(\hat{q})H(X_1 \oplus N_1 | \hat{Q} = \hat{q}) - \sum_q p_{\hat{Q}}(\hat{q})H(N_1 | \hat{Q} = \hat{q}) = \sum_q p_{\hat{Q}}(q)H(X_1 \oplus N_1 | Q = q) - h_b(\delta_1) \tag{27}
\]

\[
= \sum_q p_{\hat{Q}}(q) h_b(p_{X_1 | Q}(1 | q) * \delta_1) - h_b(\delta_1) \leq h_b(E_Q \{p_{X_1 | Q}(1 | q) * \delta_1\}) - h_b(\delta_1) \leq h_b(\tau * \delta_1) - h_b(\delta_1) \tag{28}
\]

where (i) \[26\] follows from independence of $(N_1, X_2, X_3)$ and $X_1$ conditioned on realization of $Q$, (ii) \[27\] follows from the existence of a $\hat{q}^* \in \hat{Q}$ for which $H(X_2 \oplus X_3 | \hat{Q} = \hat{q}^*) > 0$ and substituting $p_{X_1 \oplus N_1 | Q}(\cdot | \hat{q}^*)$ for $p_{Z_1}$, $p_{N_1 | Q}(\cdot | \hat{q}^*)$ for $p_{Z_2}$ and $p_{X_2 \oplus X_3 | Q}(\cdot | \hat{q}^*)$ for $p_{Z_3}$ in lemma \[1\] and noting that $p_{X_1 \oplus N_1 | Q}(1 | \hat{q}^*) > p_{N_1 | Q}(1 | \hat{q}^*)$, (iii) the first inequality in \[28\] follows from Jensen’s inequality and the second follows from the cost constraint that any test channel in $D_u(\tau, 0, 0)$ must satisfy.
APPENDIX B

PROOF OF ACHIEVABILITY

Let $p_{QU,XY} \in \mathbb{D}_f(\mathcal{F})$, $R \in \alpha_f^{3-1}(p_{QU,XY})$ and $\eta > 0$. Let us assume $U_2 = U_3 = \mathcal{F}_\eta$ is the finite field of size $\theta$. For each $n \in \mathbb{N}$ sufficiently large, we prove existence of a 3–IC code $(n, \mathcal{M}, e, d)$ for which $\frac{\log d_k}{n} \geq R_k - \eta$, $\tau_k(c_k) \leq \tau_k + \eta$ for $k \in [3]$ and $\mathcal{E}(e, d) \leq \eta$.

Taking a cue from the above coding technique, we begin with an alternative characterization of $\alpha_f^{3-1}(p_{QU,XY})$ in terms of the parameters of the code.

**Definition 10:** Consider $p_{QU,XY} \in \mathbb{D}_f(\mathcal{F})$ and let $\mathcal{F}_\eta : = U_2 = U_3$. Let $\tilde{\alpha}_f^{3-1}(p_{QU,XY})$ be defined as the set of rate triples $(R_1, R_2, R_3) \in [0, \infty)^3$ for which $\bigcup_{\delta > 0} S(\tilde{R}, p_{QU,XY}, \delta)$ is non-empty, where $S(\tilde{R}, p_{QU,XY}, \delta)$ is defined as the collection of vectors $(S_2, T_2, K_2, L_2, S_3, T_3, K_3, L_3) \in [0, \infty)^8$ that satisfy

$$
R_j = T_j + L_j, \quad K_j > \delta, \quad (S_j - T_j) > \log \theta - H(U_j|Q) + \delta,
$$

$$(S_j - T_j) + K_j > \log \theta + H(X_j|Q) - H(U_j, X_j|Q) + \delta$$

for $j = 2, 3$.

**Lemma 2:** $\tilde{\alpha}_f^{3-1}(p_{QU,XY}) = \alpha_f^{3-1}(p_{QU,XY})$.

**Proof:** The proof follows by substituting $R_j = T_j + L_j$ in the bounds characterizing $S(\tilde{R}, p_{QU,XY})$ and eliminating $S_j, T_j, K_j, L_j$ for $j = 2, 3$ via the technique of Fourier Motzkin. The resulting characterization will be that of $\alpha_f^{3-1}(p_{QU,XY})$. The presence of strict inequalities in the bounds characterizing $\alpha_f^{3-1}(p_{QU,XY})$ and $S(\tilde{R}, p_{QU,XY}, \delta)$ enables one to prove $\bigcup_{\delta > 0} S(\tilde{R}, p_{QU,XY}, \delta)$ is non-empty for every $\tilde{R} \in \tilde{\alpha}_f^{3-1}(p_{QU,XY})$.

Lemma 8 provides us with $\delta > 0$ and parameters $(S_j, T_j, K_j, L_j)$ for $j = 2, 3$ in $S(\tilde{R}, p_{QU,XY}, \delta)$ of the code whose existence we seek to prove. Define $\eta = \frac{1}{2\pi} \min\{\delta, \eta\}$, where $\eta \in \mathbb{N}$ will be specified in due course. Let $q^n \in T_n(\eta)$ denote the time sharing sequence. User 1’s code contains $\exp\{nR_1\}$ codewords $(x^n_1(m_1) : m_1 \in \mathcal{M}_1)$, where $\mathcal{M}_1 = [\exp\{nR_1\}]$. For $j \in \{2, 3\}$, user $j$’s cloud center codeword $L_j$ is the PCC $(n, s_j, t_j, g_j, b^n_j, i_j)$ built over $U^n_j = \mathcal{F}_\theta^n$ where $s_j = \frac{nS_j}{\log \theta}$ and $t_j = \frac{nT_j}{\log \theta}$. We refer the reader to the coding technique described prior to the proof for the definitions of $u^n_j(a^s)$ and $c_j(m_{j1})$. The PCCs overlap, and without loss of generality, we assume $s_2 \leq s_3$ and therefore $g_3^T = [g_2^T \ g_{3/2}^T]$.

We now specify encoding rules. Encoder 1 feeds codeword $x^n_1(M_1)$ indexed by the message as input. For $j = 2, 3$, encoder $j$ populates

$$
\mathcal{L}_j(M_j) : = \{(u^n_j(a^s), x^n_j(M_j, b_jx)) \in T_2(q^n) : (a^s, b_jx) \in c_j(M_{j1}) \times c_jx\}.
$$

If $\mathcal{L}_j(M_j)$ is non-empty, one of these pairs is chosen. Otherwise, one pair from $\lambda_j \times C_j$ is chosen. Let $(U^n_j(A^s), X^n_j(M_jx, B_jx))$ denote the chosen pair. $X^n_j(M_jx, B_jx)$ is fed as input on the channel.
Decoder 1 constructs the sum $\lambda_2 \oplus \lambda_3 : = \{ u^n_2 \oplus u^n_3 : u^n_j \in \lambda_j, j = 2, 3 \}$ of the cloud center codebooks. Let $u^n_0(a^{s_3}) : = a^{s_3} g_3 \oplus b^n_0 \oplus b^n_3$ denote a generic codeword in $\lambda_2 \oplus \lambda_3$. Note that $\lambda_2 \oplus \lambda_3 = \{ u^n_0(a^{s_3}) : a^{s_3} \in U^n_3 \}$.

Having received $Y^n_1$, it looks for all potential message $\hat{m}_1$ for which there exists a $a^{s_3} \in U^n_3$ such that $(q^n, u^n_0(a^{s_3}), x^n_0(\hat{m}_1), Y^n_1) \in T_{2n}(Q, U_3 \oplus X_3, Y_1)$. If it finds exactly one such message $\hat{m}_1$, it declares this as decoded message of user 1. Otherwise, it declares an error.

For $j \in \{2, 3\}$, decoder $j$ identifies all $(\hat{m}_{j, 1}, \hat{m}_{j, X})$ for which there exists $(a^{s_3}, b_{j, X}) \in c_j(\hat{m}_{j, 1}) \times c_j X$ such that $(q^n, u^n_j(a^{s_3}), x^n_j(\hat{m}_{j, X}, b_{j, X}), Y^n_j) \in T_{2n}(Q, U_2 \oplus X_2, Y_j)$, where $Y^n_j$ is the received vector. If there is exactly one such pair $(\hat{m}_{j, 1}, \hat{m}_{j, X})$, this is declared as message of user $j$. Otherwise an error is signaled.

The above encoding and decoding rules map every quintuple of codes $(C_1, \lambda_2, \lambda_3, C_2, C_3)$ into a corresponding 3–IC code $(n, M, c, d)$ of rate $\frac{\log |M_1|}{n} = R_1$, $\frac{\log |M_2|}{n} = \frac{t_j}{n} \log \theta + L_j = T_j + L_j = R_j : j \in \{2, 3\}$, thus characterizing an ensemble of 3–IC codes, one for each $n \in \mathbb{N}$. We average error probability over this ensemble of 3–IC codes by letting (i) the codewords of $C_1 : = (X^n_1(m_1) : m_1 \in M_1)$, generator matrices $G_2, G_3$, bias vectors $B^n_1, B^n_2$, bin indices $(I_j(a^{s_3})) : a^{s_3} \in U^n_j$ : $j = 2, 3$ and codewords of $C_j : = (X^n_j(m_{j, X}, b_{j, X}) : (m_{j, X}, b_{j, X}) \in M_{j, X} \times c_j X) : j = 2, 3$ be independently, (ii) the codewords of $C_j : j = 1, 2, 3$ are identically distributed according to $\prod_{j = 1}^n p_{X_j}(|q_j|)$, (iii) generator matrices $G_{j, 1}, G_{j, 2, j, 1}$, bias vectors $B^n_1, B^n_2$, bin indices $(I_j(a^{s_3})) : a^{s_3} \in U^n_j$ : $j = 2, 3$ be uniformly distributed over their respective range spaces. We denote the random partitioned coset code $(n, s_3, t_j, G_j, B^n_j, I_j)$ of user $j$ as $A_j$ and let $(i) U^n_1(a^{s_3}) : = a^{s_3} G_j \oplus B^n_j$ denote a generic random codeword in $A_j$, (ii) $U^n_0(a^{s_3}) : = a^{s_3} G_3 \oplus B^n_2 \oplus B^n_3$ denote a generic codeword in $A_2 \oplus A_3$, and (iii) $C_j(\hat{m}_1) : = \{ a^{s_3} \in U^n_j : I_j(a^{s_3}) = \hat{m}_1 \}$ denote the random collection of indices corresponding to message $M_{j, 1}$.

We now proceed towards deriving an upper bound on the probability of error. Towards that end, we begin with a characterization of error events. Let

$\epsilon_{11} : = \{(q^n, X^n_1(M_1)) \notin T_{2n}(Q, X_1)\}$

$\epsilon_{1j} : = \bigcap_{(a^{s_3}, b_{j, X}) \in C_j(\hat{m}_{j, 1}) \times c_j X} \{ (q^n, U^n_j(a^{s_3}), X^n_j(\hat{m}_{j, X}, b_{j, X})) \notin T_{2n}(Q, U_j, X_j) \}, j = 2, 3$

$\epsilon_2 : = \{ (q^n, U^n_2(A^{s_3}), U^n_3(A^{s_3}), X^n_1(M_1), X^n_2(M_2X, B_2X), X^n_3(M_3X, B_3X)) \notin T_{2n}(Q, U_2, U_3, X) \}$

$\epsilon_3 : = \{ (q^n, U^n_2(A^{s_3}), U^n_3(A^{s_3}), X^n_1(M_1), X^n_2(M_2X, B_2X), X^n_3(M_3X, B_3X), Y^n) \notin T_{2n}(Q, X_1, U_2, U_3, X, Y) \}$

$\epsilon_{41} : = \bigcup_{\hat{m}_1 \neq M_1} \bigcup_{a^{s_3} \in U^n_3} \{ (q^n, U^n_0(a^{s_3}), X^n_1(\hat{m}_1), Y^n_1) \in T_{2n}(Q, U_2 \oplus U_3, X_1, Y_1) \}$

$\epsilon_{4j} : = \bigcup_{\hat{m}_j \neq M_j} \bigcup_{c_j \in C_j(\hat{m}_{j, 1})} \bigcup_{b_{j, X} \in c_j X} \{ (q^n, U^n_j(a^{s_3}), X^n_j(\hat{m}_{j, X}, b_{j, X}), Y^n_j) \in T_{2n}(Q, U_j, V_j, Y_j) \}, j = 2, 3$.

14Here we have used the assumption $s_2 \leq s_3$. In general, if $s_{j_1} \leq s_{j_2}$, we have $\lambda_2 \oplus \lambda_3 = \{ u^n_0(a^{s_{j_2}}) : a^{s_{j_2}} \in U^n_{j_2} \}$, where $u^n_0(a^{s_{j_2}}) : = a^{s_{j_2}} g_{j_2} \oplus b^n_0 \oplus b^n_3$ denotes a generic codeword.

15The choice for $\eta_1$ is indicated at the end of the proof.

16Recall, that we have assumed $s_2 \leq s_3$. 


Note that $\epsilon = \bigcup_{j=1}^{3} (\epsilon_1 \cup \epsilon_2 \cup \epsilon_3 \cup \epsilon_{4j})$ contains the error event. We derive an upper bound on the probability of this event by partitioning it appropriately. The following events will aid us identify such a partition. Define $\epsilon_1 := \epsilon_{12} \cup \epsilon_{13}$, where $\epsilon_{ij} := \{\phi_j(q^n, M_j) < \mathcal{L}_j(n)\}$, and $\phi_j(q^n, M_j) := \sum_{(a^r, b^r) \in C_{t1}(M_{t1} \times \mathcal{C})} 1\{(q^n, U^n, X^n) \in \mathbb{T}_n(Q, U_j, X_j)\}$.

$\mathcal{L}_j(n)$ is half of the expected number of jointly typical pairs in the indexed pair of bins. For sufficiently large $n$, we prove $\mathcal{L}_j(n) > 2$. For such an $n$, $\epsilon_{1j} \subseteq \epsilon_{ij} : j = 2, 3$. Since, we can choose $n$ sufficiently large, we will henceforth assume $\epsilon_{1j} \subseteq \epsilon_{ij} : j = 2, 3$. It therefore suffices to derive upper bounds on $P(\epsilon_{11})$, $P(\epsilon_{1j}) : j = 2, 3$, $P(\epsilon_1 \cap \epsilon_2)$, $P((\epsilon_1 \cup \epsilon_2)^c \cap \epsilon_3)$, $P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{4j}) : j = 1, 2, 3$ where $\epsilon_1 := \epsilon_{11} \cup \epsilon_1 = \epsilon_{11} \cup \epsilon_{12} \cup \epsilon_{13}$.

**Upper bound on $P(\epsilon_{11})$** - By conditional frequency typicality [21, Lemma 5], for sufficiently large $n$, $P(\epsilon_{11}) \leq \frac{n}{32}$.

**Upper bound on $P(\epsilon_{1j})$** - Using a second moment method similar to that employed in [21, Appendix A], we derive an upper bound on $P(\epsilon_{1j})$ in appendix C. In particular, we prove

$$P(\epsilon_{1j}) \leq 12 \exp \{-n(\delta - 32\eta)\} \quad (31)$$

for sufficiently large $n$. In deriving the above upper bound, we employed, among others, the bounds

$$K_j > \delta > 0, \quad (S_j - T_j) - [\log \theta - H(U_j|Q)] > \delta > 0$$

$$(S_j - T_j) + K_j - [\log \theta + H(X_j|Q) - H(U_j, X_j|Q)] > \delta > 0.$$  

**Upper bounds on $P(\epsilon_1 \cap \epsilon_2)$, $P((\epsilon_1 \cup \epsilon_2)^c \cap \epsilon_3)$** - These events are related to the following two events. (i) The codewords chosen by the distributed encoders are not jointly typical, and (ii) the channel produces a triple of outputs that is not jointly typical with the chosen and input codewords. In deriving upper bounds on $P(\epsilon_1 \cap \epsilon_2)$, $P((\epsilon_1 \cup \epsilon_2)^c \cap \epsilon_3)$, we employ (i) conditional mutual independence of the triplet $X_1, (U_j, X_j) : j = 2, 3$ given $Q$ and (ii) the Markov chain $(U_j : j = 2, 3) - X - Y$. For a technique based on unstructured and independent codes, the analysis of this event is quite standard. However, since our coding technique relies on codewords chosen from statistically correlated codebooks, we present the steps in deriving an upper bound in appendix D. In particular, we prove that for sufficiently large $n$,

$$P(\epsilon_1 \cap \epsilon_2) + P((\epsilon_1 \cup \epsilon_2)^c \cap \epsilon_3) \leq 2 \exp \{-n(\mu_\eta_1^2 - 32\eta)\} + \frac{n}{32} \quad (32)$$

**Upper bound on $P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{41})$** - In appendix E, we prove

$$P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{41}) \leq 4 \exp \{-n(\delta - 28\eta - 12\eta)\} \quad (33)$$

for sufficiently large $n$. In deriving [33], we employed, among others, the bounds

$$\log \theta + H(X_1|Q) - H(X_1, U_2 \oplus U_3|Y_1, Q) - (R_1 + \max\{S_2, S_3\}) > \delta > 0, I(X_1; Y_1, U_2 \oplus U_3|Q) - R_1 > \delta > 0.$$  

\textsuperscript{17}Since the precise value of $\mathcal{L}_j(n)$ is necessary only in the derivation of the upper bound, it is provided in appendix C.
Upper bound on $P((\epsilon_1 \cup \epsilon_3)^c \cap \epsilon_4)$: In appendix \textbf{F}, we prove

$$P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_4) \leq 10 \exp \{ -n (\delta - (9\eta + 16\eta_1)) \}$$

(34)

for sufficiently large $n$. In deriving (34), we employed, among others, the bounds

$$\log \theta - H(U_j|X_j,Y_j,Q)) - S_j > \delta > 0, \quad \log \theta + H(X_j|Q) - (S_j + K_j) > \delta > 0,$$

$$I(X_1;Y_1;U_2 \oplus U_3|Q) - R_1 > \delta > 0, \quad (I(X_j;U_j,Y_j|Q)) - (K_j + L_j) > \delta > 0,$$

$$\log \theta + H(X_j|Q) - H(X_j,U_j|Y_j,Q)) - (K_j + L_j + S_j) > \delta > 0.$$

We now collect the derived upper bounds. From (31), (32), (33) and (34), we have

$$P\left( \bigcup_{j=1}^{3} (\epsilon_{1j} \cup \epsilon_{3j} \cup \epsilon_{4j}) \right) \leq \frac{n}{32} + 24 \exp \{ -n (\delta - 32\eta) \} + 2 \exp \{ -n (n^2 \mu \eta_1^2 - 32\eta) \} + \frac{n}{32}
$$

$$+ 4 \exp \{ -n [\delta - 28\eta] \} + 20 \exp \{ -n (\delta - (9\eta + 16\eta_1)) \}$$

The reader may recall that we need $\eta = \frac{1}{2\tilde{\eta}} \min\{\tilde{\eta}, \delta\}$ and that $\eta_1 \geq 4\eta$ for the above bounds to hold. The reader may verify that, by choosing $d$ sufficiently large, one can choose $\eta$ and $\eta_1 \geq 4\eta$ such that the upper bound above decays exponentially. This completes the derivation of an upper bound on the probability of error.

We only need to argue that the chosen input codewords satisfy the cost constraint. For sufficiently large $n$, we have proved that the chosen input codewords are jointly typical with respect to $p_{Q,U_2,U_3,X,Y}$, a distribution that satisfies $E\{\kappa_j(X_j)\} \leq \tau_j$. Using standard typicality arguments and finiteness of $\max \{\kappa_k(x_k) : x_k \in \mathcal{X}_k : k \in [3]\}$, it is straightforward to show that the average cost of the codeword output by encoder $j$ is close to $\tau_j$ per symbol.

APPENDIX C

UPPER BOUND ON $P(\epsilon_{1j})$

Recall

$$\phi_j(q^n, M_j) = \sum_{a^{\ast} \in U^{\ast}} \sum_{b_{jX} \in \mathcal{C}_{jX}} \sum_{jX^n} 1_{\{I_j(a^{\ast}) = M_j, \{a^{\ast},X^n\} \in \mathcal{T}_{2n}(U_j,X_j)|q^n\}} \mathcal{L}_j(n) = \frac{1}{2} E\{\phi_j(q^n, M_j)\}$$

and $\epsilon_{1j} = \{\phi_j(q^n, M_j) < \mathcal{L}_j(n)\}$. Employing Chebychev’s inequality, we have

$$P(\epsilon_{1j}) = P(\phi_j(q^n, M_j) < \mathcal{L}_j(n)) \leq P(\|\phi_j(q^n, M_j) - E\{\phi_j(q^n, M_j)\}\| \geq \frac{1}{2} E\{\phi_j(q^n, M_j)\}) \leq \frac{4 \text{Var}\{\phi_j(q^n, M_j)\}}{(E\{\phi_j(q^n, M_j)\})^2}. $$

Note that $\text{Var}\{\phi_j(q^n, M_j)\} = \mathcal{T}_0 + \mathcal{T}_1 + \mathcal{T}_2 + \mathcal{T}_3 - \mathcal{T}_0^2$, where

$$\mathcal{T}_0 = \sum_{a^{\ast} \in U^{\ast}} \sum_{b_{jX} \in \mathcal{C}_{jX}} \sum_{jX^n} 1_{\{I_j(a^{\ast}) = M_j, \{a^{\ast},X^n\} \in \mathcal{T}_{2n}(U_j,X_j)|q^n\}} \mathcal{E}\{\phi_j(q^n, M_j)\},$$

$$\mathcal{T}_1 = \sum_{a^{\ast} \in U^{\ast}} \sum_{b_{jX} \in \mathcal{C}_{jX}} \sum_{jX^n} \sum_{b_{jX} \neq b_{jX}} 1_{\{a^{\ast},X^n \in \mathcal{C}_{jX},(a^{\ast},\tilde{X}^{j^n}) \in \mathcal{T}_{2n}(U_j,X_j)|q^n\}} \mathcal{P}\{I_j(a^{\ast}) = M_j, X^n = \tilde{X}^{j^n}, (a^{\ast},\tilde{X}^{j^n}) \in \mathcal{T}_{2n}(U_j,X_j)|q^n\},$$

$$\mathcal{T}_2 = \sum_{a^{\ast} \in U^{\ast}} \sum_{b_{jX} \in \mathcal{C}_{jX}} \sum_{jX^n} \sum_{a^{\ast} \neq \tilde{a}^{\ast}} 1_{\{I_{j1}(a^{\ast}) = M_{j1}, I_{j2}(\tilde{a}^{\ast}) = M_{j2}, \{a^{\ast},\tilde{a}^{\ast}\} \in \mathcal{T}_{2n}(U_j,X_j)|q^n\}} \mathcal{P}\{I_{j1}(a^{\ast}) = M_{j1}, I_{j2}(\tilde{a}^{\ast}) = M_{j2}, X^n = \tilde{X}^{j^n}, \tilde{X}^{j^n} = \tilde{X}^{j^n},(a^{\ast},\tilde{a}^{\ast}) \in \mathcal{T}_{2n}(U_j,X_j)|q^n\}.$$
\[ T_3 = \sum_{a \neq \tilde{a}} \sum_{a^* \notin U^*} P \left( I_j(a^*) = M_j, X_j^n(M_j, b_j, x) = x_j^n, U_j^n(a^*) = u_j^n \right) P \left( I_j(\tilde{a}^*) = M_j, X_j^n(M_j, b_j, x) = \tilde{x}_j^n, U_j^n(\tilde{a}^*) = \tilde{u}_j^n \right). \]

The codewords of PCC \( A_j \) are pairwise independent [24 Theorem 6.2.1], and therefore

\[ P \left( I_j(a^*) = M_j, X_j^n(M_j, b_j, x) = x_j^n, U_j^n(a^*) = u_j^n \right) P \left( I_j(\tilde{a}^*) = M_j, X_j^n(M_j, b_j, x) = \tilde{x}_j^n, U_j^n(\tilde{a}^*) = \tilde{u}_j^n \right). \]

It can be verified that \( T_3 \leq T_2^2 \), and therefore, \( P(\epsilon_{1j}) \leq 4 \frac{\mathcal{R}_0 + \mathcal{R}_1 + \mathcal{R}_2}{\mathcal{R}_0} \). For sufficiently large \( n \), we employ upper bounds on conditional probability and the number of conditional typical sequences to conclude

\[ \mathcal{R}_0 \geq \exp \left\{ -nH(X_j|Q) - 4mn \right\} |c_jX||T_{2\eta}(U_j, X_j|q^n)| \]
\[ \mathcal{R}_1 \leq \exp \left\{ -2nH(X_j|Q) + 8\eta + nH(U_j|X_j, Q) + 8\eta \right\} |c_jX||T_{2\eta}(U_j, X_j|q^n)| \]
\[ \mathcal{R}_2 \leq \exp \left\{ -nH(X_j|Q) + 4\eta + nH(U_j|X_j, Q) + 8\eta \right\} |c_jX||T_{2\eta}(U_j, X_j|q^n)| \].

For sufficiently large \( n \), \( \exp \{-4\eta \} \leq \exp \{-nH(U_j, X_j|Q)\} |T_{2\eta}(U_j, X_j|q^n)| \leq \exp \{4\eta \} \). Substituting \( S_j = \frac{s_j\log \theta}{n}, T_j = \frac{t_j\log \theta}{n} \) and \( |c_jX| = \exp \{nK_j\} \), it may be verified that, for sufficiently large \( n \),

\[ P(\epsilon_{1j}) \leq 4 \exp \left\{ -n[S_j - T_j + K_j - (\log \theta + H(X_j|Q) - H(U_j, X_j|Q)) - 8\eta] \right\} + 4 \exp \left\{ -n[S_j - T_j - (\log \theta - H(U_j|Q)) - 28\eta] \right\} + 4 \exp \left\{ -n[K_j - 32\eta] \right\}. \]

Using the bounds on \( S_j, T_j \) and \( K_j \) as given in definition [11] in terms of \( \delta \), we have

\[ P(\epsilon_{1j}) \leq 12 \exp \left\{ -n(\delta - 32\eta) \right\} \]

for sufficiently large \( n \). Before we conclude this appendix, let us confirm \( \mathcal{L}_j(n) \) grows exponentially with \( n \). This would imply \( \epsilon_{1j} \subseteq \epsilon_{i} \), and therefore \( \epsilon_{1j} \cap \epsilon_{i} = \phi \), the empty set. From (35), (36), we have for sufficiently large \( n \),

\[ \mathcal{L}_j(n) = \frac{1}{2} \mathbb{E} \{ \phi_j(q^n, M_j) \} \geq \frac{\mathcal{R}_0}{2} \exp \left\{ -nH(X_j|Q) - 4\eta \right\} |c_jX||T_{2\eta}(U_j, X_j|q^n)| \]
\[ \geq \frac{1}{2} \exp \left\{ n[S_j - T_j + K_j - (\log \theta + H(X_j|Q) - H(U_j, X_j|Q)) - 8\eta] \right\} \geq \frac{1}{2} \exp \left\{ n[\delta - 8\eta] \right\} \]

where, as before, we have employed \( S_j = \frac{s_j\log \theta}{n}, T_j = \frac{t_j\log \theta}{n} \) and \( |c_jX| = \exp \{nK_j\} \), the lower bounds on \( |T_{2\eta}(U_j, X_j|q^n)| \) and the definition of \( \delta \).

**APPENDIX D**

**UPPER BOUNDS ON \( P(\tilde{\epsilon}_1 \cap \epsilon_2)\), \( P((\tilde{\epsilon}_1 \cup \epsilon_2)^c \cap \epsilon_3)\)**

In the first step, we derive an upper bound on \( P(\tilde{\epsilon}_1 \cap \epsilon_2) \), where \( \tilde{\epsilon}_1 = \epsilon_1 \cup \epsilon_l \), and

\[ \epsilon_2 = \{q^n_u, U_2^n(A^{2^n}), U_3^n(A^{3^n}), X_2^n(M_1), X_2^n(M_2, B_{2^n}), X_2^n(M_3, B_{3^n}) \notin T_{n_1}(Q, U_2, U_3, X) \}. \]

was defined in [29]. In the second step, we employ the result of conditional frequency typicality [21 Lemma 4 and 5] to provide an upper bound on \( P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3) \cap (\epsilon_{31} \cup \epsilon_{32} \cup \epsilon_{33})) \).
As an astute reader might have guessed, the proof of first step will employ conditional independence of the triple \( X_1, (U_2, X_2), (U_3, X_3) \) given \( Q \). The proof is non-trivial because of statistical dependence of the codebooks. We begin with the definition

\[
\Theta(q^n) := \left\{ (u^n_2, u^n_3, x^n) \in \mathcal{U}^n_2 \times \mathcal{U}^n_3 \times \mathcal{X}^n : (q^n, u^n_2, x^n_j) \in T_{2q}(Q, U_j, X_j) \right\}.
\]

Observe that

\[
P(\varepsilon_1 \cap \varepsilon_2) = \sum_{(u^n_2, u^n_3, x^n) \in \Theta(q^n)} P \left( I_j(A_j) = M_{j1}, U_j^n(A_j) = u^n_j, X_j^n(M_j, X_j) = x^n_j \right)
\]

\[
= \sum_{(u^n_2, u^n_3, x^n) \in \Theta(q^n)} \sum_{a_2 \in \mathcal{U}^n_2} \sum_{a_3 \in \mathcal{U}^n_3} \sum_{b_x \in \mathcal{B}_x} \sum_{c_x \in \mathcal{C}_x} P \left( I_j(a_j) = M_{j1}, U_j^n(a_j) = u^n_j, X_j^n(M_j, X_j) = x^n_j \right) \prod_{j=2}^3 P \left( X_j^n(M_j, X_j) = x^n_j \right).
\]

Let us now evaluate a generic term in the above sum \([40]\). Since the codebooks \( C_1, C_2, C_3, \Lambda_2, \Lambda_3 \) are mutually independent, the probability of the event in question factors as

\[
P \left( U_j^n(a_j) = u^n_j, X_j^n(M_j, X_j) = x^n_j \right) = P \left( X_j^n(M_j) = x^n_j \right) \prod_{j=2}^3 P \left( X_j^n(M_j, X_j) = x^n_j \right)
\]

Furthermore, (i) mutual independence of \( I_j(a^*_j) : a^*_j \in \mathcal{U}^n_j \) : \( j = 2, 3, G_3, B_2^n, B_3^n \), (ii) uniform distribution of the indices \( I_j(a^*_j) : a^*_j \in \mathcal{U}^n_j \) : \( j = 2, 3 \) and (iii) distribution of codewords in \( C_j : j = 1, 2, 3 \) imply

\[
P \left( U_j^n(a_j) = u^n_j, X_j^n(M_j, X_j) = x^n_j \right) = P \left( U_j^n(a_j) = u^n_j \right) = 2^{-n} \prod_{j=2}^3 P \left( X_j^n(M_j, X_j) = x^n_j \right)
\]

The following simple lemma enables us to characterize \( P(U_j^n(a_j) = u^n_j : j = 2, 3) \).

**Lemma 3:** Let \( s_2, s_3, n \in \mathbb{N} \) be such that \( s_2 \leq s_3 \). Let \( G_{3/2}^T := [G_{3/2}^T, G_{3/2}^T] \in \mathcal{F}_0^{s_3 \times n} \) be a random matrix such that \( G_2 \in \mathcal{F}_0^{s_2 \times n} \) and \( B_2^n, B_3^n \in \mathcal{F}_0^n \) be random vectors such that \( G_3, B_2^n, B_3^n \) be mutually independent and uniformly distributed over their respective range spaces. For \( j = 2, 3 \) and any \( a^*_j \in \mathcal{U}^n_j \), let \( U(a^*_j) := a^*_j G_j + B^t_j \) be a random vector in the corresponding coset. Then \( P(U_j^n(a^*_j) = u^n_j : j = 2, 3) = \frac{1}{2^{n/4}} \).

The proof follows from a simple counting argument and is omitted. We therefore have

\[
P \left( U_j^n(a_j) = u^n_j, X_j^n(M_j, X_j) = x^n_j \right) = \prod_{j=2}^3 \prod_{t=1}^{s_3} P_{X_j | Q}(x_j | q_t) \exp \left\{ -nH(X_j | Q) \right\} \exp \left\{ -8nq_t + nH(X_j | Q) \right\} 2^{n/2 + t + s_3}
\]

Encoders 2 and 3 choose one among the jointly typical pairs uniformly at random. Hence,\n
\[
\prod_{j=2}^3 P \left( A_j|x_j^t = a_j^t, \phi_j(q^n, M_j) \geq \frac{1}{2} \mathbb{E} \{ \phi_j(q^n, M_j) \} \right) \leq \frac{4}{\mathbb{E} \{ \phi_2(q^n, M_2) \} \mathbb{E} \{ \phi_3(q^n, M_3) \}}.
\]
It may be verified from (35) that

\[ 2L_n(n) = \mathbb{E} \{ \phi_j(q^n, M_j) \} \geq \theta^{t_{j-n}} |c_j| \exp \{-n(H(X_j | Q) + 4\eta)\} |T_{2\eta}(U_j, X_j | q^n)\}. \tag{44} \]

Substituting (44), (43) and (42) in (40), we have

\[
P(\tilde{\epsilon}_1 \cap \epsilon_2) \leq \sum_{(u^n_2, u^n_3, x^n) \in \Theta(q^n)} \exp\{n16\eta\} \prod_{t=1}^n p_{X_t | Q}(x_{1t} | q_t) \frac{\exp\{24n\eta - nH(U_3, X_3 | Q)\}}{\exp\{nH(U_2, X_2 | Q)\}} \]

\[
\leq \sum_{(u^n_2, u^n_3, x^n) \in \Theta(q^n)} \prod_{t=1}^n p_{X_t | Q}(x_{1t} | q_t) \exp\{32n\eta\}, \tag{45} \]

where the last inequality follows from lower bound on size of the conditional typical set. We now employ the lower bound for conditional probability of jointly typical vectors. In particular,

\[
\exp \{-nH(U_j, X_j | Q) - 4n\eta\} \leq \prod_{t=1}^n p_{U_t, X_j | Q}(u_{jt}, x_{jt} | q_t) \leq \exp \{-nH(U_j, X_j | Q) + 4n\eta\} \tag{46} \]

for any \((u^n_2, u^n_3, x^n) \in \Theta(q^n)\). Substituting lower bound (46) in (45), for \(n\) sufficiently large, we have

\[
P(\tilde{\epsilon}_1 \cap \epsilon_2) \leq \left[ \sum_{(u^n_2, u^n_3, x^n) \in \Theta(q^n)} \prod_{t=1}^n p_{X_t | Q}(x_{1t} | q_t) \prod_{j=2}^3 \prod_{t=1}^n p_{U_j, X_j | Q}(u_{jt}, x_{jt} | q_t) \right] \exp\{32n\eta\} \]

\[
\leq \left[ \sum_{(u^n_2, u^n_3, x^n) \in \Theta(q^n)} \prod_{t=1}^n p_{X_1 U_2 X_2 X_3 | Q}(x_{1t}, u_{2t}, x_{2t}, u_{3t}, x_{3t} | q_t) \right] \exp\{32n\eta\}, \tag{47} \]

where (47) follows from conditional mutual independence of the triple \((X_1, U_2, X_2) \) and \((U_3, X_3) \) given \(Q\). We now employ the exponential upper bound due to Hoeffding [30], Sanov [31]. Under the condition \(\eta_1 \geq 4\eta\), a ‘conditional version’ of Sanov’s lemma [31] guarantees

\[
\sum_{(u^n_2, u^n_3, x^n) \in \Theta(q^n)} \prod_{t=1}^n p_{X_1 U_2 X_2 X_3 | Q}(x_{1t}, u_{2t}, x_{2t}, u_{3t}, x_{3t} | q_t) \leq 2 \exp\{-n^3 \mu^2_1\} \tag{48} \]

for sufficiently large \(n\). Thus we conclude

\[
P(\tilde{\epsilon}_1 \cap \epsilon_2) \leq 2 \exp\{-n(n^2 \mu^2_1 - 32\eta)\} \tag{49} \]

for such an \(n\).

This gets us to the second step where we seek an upper bound on \(P((\tilde{\epsilon}_1 \cup \epsilon_2)^c \cap \epsilon_3)\), where

\[
\epsilon_3 = \{(q^n, U^n_2(A^n), U^n_3(A^n), X^n_1(M_1), X^n_2(M_2X, B_2X), X^n_3(M_3X, B_3X), Y^n) \notin T_{2\eta_1}(Q, X_1, U_2, U_3, X, Y, X, Y)\} \tag{50} \]

was defined in (30). Deriving an upper bound on \(P((\tilde{\epsilon}_1 \cup \epsilon_2)^c \cap \epsilon_3)\) employs conditional frequency typicality [21] Lemma 4 and 5] and the Markov chain \((Q, U_2, U_3) = X - Y\). In the sequel, we prove \(P(\epsilon_2^n \cap \epsilon_3) \leq \frac{n}{42}\) for sufficiently large \(n\).
If

$$\mathfrak{G}(q^n) := \left\{ \left( u_2^n, u_3^n, x^n, y^n \right) \in U_2^n \times U_3^n \times X^n \times Y^n : \begin{align*}
(u_2^n, u_3^n, x^n, y^n) &\in T_{\eta n}(U_2, U_3, X|q^n), \\
(u_2^n, u_3^n, x^n, y^n) &\notin T_{2\eta n}(U_2, U_3, X, Y|q^n)
\end{align*} \right\},$$

then

$$P(\epsilon_2^n \cap \epsilon_3) = \sum_{(u_2^n, u_3^n, x^n, y^n) \in \mathfrak{G}(q^n)} P \left( \left. \begin{array}{c}
U^n_j(A^n) = u^n_j, X^n_j(M_j, x_j, B_j, x_j) = x^n_j : j = 2, 3, X^n_1(M_1) = x^n_1, Y^n = y^n
\end{array} \right| q^n \right)$$

$$= \sum_{(u_2^n, u_3^n, x^n, y^n) \in \mathfrak{G}(q^n)} \prod_{t=1}^n W_t|X(y_t|e_t),$$

$$\leq \sum_{(u_2^n, u_3^n, x^n, y^n) \in T_{\eta n}(U_2, U_3, X, Y|q^n)} \prod_{t=1}^n W_t|X(y_t|e_t), \quad n \geq 32,$$

for sufficiently large \(n\), where (51) follows from the Markov chain \((Q, U_2, U_3) - X - Y\) and the last inequality in (52) follows from conditional typicality.

**APPENDIX E**

**AN UPPER BOUND ON \(P((\hat{\epsilon}_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{e_{41}})\)**

In this appendix, our objective is to derive an upper bound on \(P((\hat{\epsilon}_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{e_{41}})\). Recall that \(\hat{\epsilon}_1 = \epsilon_1 \cup \epsilon_t, (\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{e_{41}} = \bigcup_{a^s \in U_{\alpha}^a} \bigcup_{m_i \neq m_1} \bigcup_{t \in T_{\alpha}} \left\{ \left( \begin{array}{c}
U^n_j(A^n) : j = 2, 3, X^n_j(M_j) = x^n_j, X^n_1(M_1) = x^n_1, Y^n = y^n
\end{array} \right) \in T_{\epsilon_{e_{41}}}(U_2 \oplus U_3, X_1, Y_1|q^n) \right\}, \)

where

$$\mathcal{T}(q^n) := \left\{ \left( u_2^n, u_3^n, x^n, y^n \right) \in U_2^n \times U_3^n \times X^n \times Y^n : \begin{align*}
(u_2^n, u_3^n, x^n, y^n) &\in T_{\eta n}(U_2, U_3, X, Y|q^n), \\
(u_2^n, u_3^n, x^n, y^n) &\notin T_{2\eta n}(U_2, U_3, X, Y|q^n)
\end{align*} \right\}.$$

Employing the union bound, we have

$$P((\hat{\epsilon}_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{e_{41}}) \leq \sum_{\hat{\alpha}^s \in T_{\alpha}} \sum_{m_i \neq m_1} \sum_{t \in T_{\alpha}} \sum_{\hat{(u_2^n, u_3^n, x^n, y^n)} \in \mathcal{T}(q^n)} \prod_{t=1}^n W_t|X(y_t|e_t).$$

We evaluate a generic term in the above sum. Defining \(\mathcal{J}(\hat{\alpha}^s) := \{ (a_{s^2}, a_{s^3}) \in U_{\alpha}^2 \times U_{\alpha}^3 : a_{s^2} \oplus a_{s^3} \neq \hat{a}_{s^3} \} \),

where \(s_+ := s_3 - s_2, \mathcal{J}_+(\hat{a}^s) := (U_{\alpha}^2 \times U_{\alpha}^3) \setminus \mathcal{J}(\hat{a}^s)\), and

$$E := \left\{ \left( \begin{array}{c}
X^n_j(M_j, x_j, B_j, x_j) = x^n_j, U^n_j(A^n) = u^n_j, M_j = m_j
\end{array} \right) : \begin{align*}
I_j(a^n_j) = x^n_j, U^n_j(\hat{a}^s) = \hat{u}^n, \\
X^n_j(m_j) = \hat{x}_j^n, M_j = m_j, i = 2, 3.
\end{align*} \right\},$$

$$\mathcal{J}_+(\hat{a}^s) = (U_{\alpha}^2 \times U_{\alpha}^3) \setminus \mathcal{J}(\hat{a}^s),$$

and

$$E := \left\{ \left( \begin{array}{c}
X^n_j(M_j, x_j, B_j, x_j) = x^n_j, U^n_j(A^n) = u^n_j, M_j = m_j
\end{array} \right) : \begin{align*}
I_j(a^n_j) = x^n_j, U^n_j(\hat{a}^s) = \hat{u}^n, \\
X^n_j(m_j) = \hat{x}_j^n, M_j = m_j, i = 2, 3.
\end{align*} \right\}.$$
we have

\[
P \left( \left\{ X_i^n(M_1,x,B_1,x) = x_i^n, U_i^n(A'_i) = u_i^n \right\} \cap \mathcal{E}_j \right) = \sum_{m_2,m_3} \sum_{b_2,b_3} \sum_{(a')^2} P \left( E \cap \mathcal{E}_j \cap \left\{ Y_i^n = y_i^n, A'_i = a'_i \right\} \right)
\]

\[
+ \sum_{m_2,m_3} \sum_{b_2,b_3} \sum_{(a')^2} P \left( E \cap \mathcal{E}_j \cap \left\{ Y_i^n = y_i^n, A'_i = a'_i \right\} \right)
\]

(54)

Note that

\[
P \left( Y_i^n = y_i^n \cap E \cap \mathcal{E}_j \cap \left\{ B_{j,x} = b_{j,x} \right\} \right) = W_{Y_i|x}(y_i^n|x^n),
\]

(55)

\[
P \left( E \cap \mathcal{E}_j \cap B_{j,x} = b_{j,x} \right) = P(E)P \left( B_{j,x} = b_{j,x} \right) \mid E \cap \mathcal{E}_j \right) = P(E)\mathcal{Z}_2(n)\mathcal{Z}_3(n)
\]

(56)

Moreover, for \((u_i^n, u_i^n, x_1^n, x_2^n, x_3^n, y_i^n) \in \tilde{T}(q^n), (\hat{u}_i^n, \hat{y}_i^n) \in T_{4n} U_2^2 U_3, X_1|y_i^n, q^n), \) we have

\[
P(E) \leq \begin{cases} 
\theta^{sn+2t+3} \exp \{n(H(\{X_i^n\}|Q) + \sum_{j=1}^{2n} H(\{X_i^n\}|Q - 20n1)\} & \text{if } (a^{s_2}, a^{s_3}) \in \mathcal{F}(\hat{a}^{s_3}), \\
\theta^{sn+2t+3} \exp \{n(H(\{X_i^n\}|Q) + \sum_{j=1}^{2n} H(\{X_i^n\}|Q - 20n1)\} & \text{if } (a^{s_2}, a^{s_3}) \in \mathcal{F}(\hat{a}^{s_3}).
\end{cases}
\]

(57)

In deriving the above upper bounds, we have used the upper bound on conditional probability of jointly typical sequences. We have also employed independence of (triple in the former and pair in the latter) codewords in the coset code. Substituting (55), (56) and (57), in (54), we have

\[
P \left( E \cap \mathcal{E}_j \cap \left\{ B_{j,x} = b_{j,x} \right\} \right) \leq \sum_{n_1} \sum_{m_1} W_{Y|x}(y_i^n|x^n) \theta^{s_2 t + s_3 t} \exp \{n(H(\{X_i^n\}|Q) + \sum_{j=1}^{2n} H(\{X_i^n\}|Q - 20n1)\} \mathcal{Z}_2(n)\mathcal{Z}_3(n).
\]

(58)

Our next step is to substitute (58) in (53). Let us restate (53) below as (59) for ease of reference.

\[
P(\mathcal{E}_1 \cup \mathcal{E}_2) \leq \sum_{\hat{u}_i^n} \sum_{\hat{y}_i^n} \sum_{\mathcal{E}_j} \sum_{\tilde{T}(q^n)} \sum_{T_{4n}(U_2^2 U_3, X_1|y_i^n, q^n)} P \left( \left\{ X_i^n(M_1,x,B_1,x) = x_i^n, U_i^n(A'_i) = u_i^n \right\} \cap \mathcal{E}_j \right)
\]

(59)

We do some spade work before we substitute (58) in (59). (58) is a sum of two terms. The first term is not dependent on the arguments of the innermost summation in (59). By conditional frequency typicality lemma [21] Lemma 5], for sufficiently large \(n\) we have \(|T_{4n}(U_2^2 U_3, X_1|y_i^n, q^n)| \leq \exp \{n(H(U_2 U_3, X_1|Y_1, Q) + 8n1)\}. Substituting this upper bound, the summation in (59) corresponding to the first term in (58) is upper bounded by

\[
\mathcal{F}_1 : = \sum_{\hat{u}_i^n} \sum_{\hat{y}_i^n} \sum_{\mathcal{E}_j} \sum_{\tilde{T}(q^n)} \sum_{T_{4n}(U_2^2 U_3, X_1|y_i^n, q^n)} W_{Y|x}(y_i^n|x^n) \theta^{s_2 t + s_3 t} \exp \{n(H(\{X_i^n\}|Q) + \sum_{j=1}^{2n} H(\{X_i^n\}|Q - 20n1)\} \mathcal{Z}_2(n)\mathcal{Z}_3(n).
\]

The indicator in the second term of (58) restricts the outermost summation in (59) to \(\hat{x}_i^n \in T_{4n}(X_1|u_i^n, u_i^n, y_i^n, q^n).\) As earlier, note that the second term is independent of \(\hat{x}_i^n.\) Once again, employing the conditional frequency typicality lemma [21] Lemma 5], for sufficiently large \(n\), \(|T_{4n}(X_1|u_i^n, u_i^n, y_i^n, q^n)| \leq \exp \{n(H(X_1|U_2 U_3, Y_1, Q) + 8n1)\}. Substituting this upper bound, the summation in (59) corresponding to the second term in (58) is upper bounded by

\[
\mathcal{F}_2 : = \sum_{\hat{u}_i^n} \sum_{\hat{y}_i^n} \sum_{\mathcal{E}_j} \sum_{\tilde{T}(q^n)} \sum_{T_{4n}(U_2^2 U_3, X_1|y_i^n, q^n)} W_{Y|x}(y_i^n|x^n) \theta^{s_2 t + s_3 t} \exp \{n(H(X_1|U_2 U_3, Y_1, Q) + \sum_{j=1}^{2n} H(\{X_i^n\}|Q - 20n1)\} \mathcal{Z}_2(n)\mathcal{Z}_3(n).
\]
It can be verified that

\[
\sum_{(u_1, u_2, u_3, y^n) \in T(q^n)} W^n_{Y_1}(y^n \mid x^n) \leq \min \{ |T_2n(U_2, X_2 | q^n)| |T_2n(U_3, X_3 | q^n)|, |T_2n(U_1, U_2, X | q^n)| \}. \tag{60}
\]

Using (60) and lower bounds \( \mathcal{L}_j(n) : j = 2, 3 \) from (44), we have

\[
\mathcal{F}_1 \leq 2 \frac{\theta^{\epsilon_3} \exp \{ -n(2H(X_1 | Q) - 8\eta - R_1) \} |T_2n(U_1, U_2, X_1 | q^n)|}{\theta^n \exp \{ -n(H(U_2 \oplus U_3, X_1 | Y_1, Q) + 28\eta_1) \}} \leq 2 \frac{\theta^{\epsilon_3} \exp \{ -n(H(X_1 | Q) - 12\eta - R_1) \}}{\theta^n \exp \{ -n(H(U_2 \oplus U_3, X_1 | Y_1, Q) + 28\eta_1) \}},
\]

where the last inequality above follows from upper bound on \( |T_2n(U_1, U_2, X_1 | q^n)| \). An identical sequence of steps yields

\[
\mathcal{F}_2 \leq 2 \frac{\exp \{ -n(H(X_1 | Q) - 28\eta_1 - R_1) \}}{\exp \{ -n(H(U_2 \oplus U_3, X_1 | Y_1, Q) + 12\eta) \}},
\]

for sufficiently large \( n \). Substituting \( \frac{s_1 \log \theta}{n} = S_3 \), we have

\[
P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{41}) \leq 2 \exp \{ n(28\eta_1 + 12\eta + S_3 + R_1 - \log \theta - H(X_1 | Q) + H(X_1, U_2 \oplus U_3 | Y_1, Q)) \}
\]

\[
+ 2 \exp \{ n(28\eta_1 + 12\eta + R_1 - I(X_1; U_2 \oplus U_3, Y_1 | Q)) \}.
\]

Employing the definition of \( \delta \), we have

\[
P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{41}) \leq 4 \exp \{ -n [\delta - 28\eta_1 - 12\eta] \}. \tag{61}
\]

for sufficiently large \( n \).

**APPENDIX F**

AN UPPER BOUND ON \( P((\epsilon_1 \cup \epsilon_2 \cup \epsilon_3)^c \cap \epsilon_{4j}) \)

While it seems that analysis of this event is similar to the error event over a point-to-point channel, and is therefore straightforward, the structure of the code lends this considerable complexity. A few remarks are in order. Firstly, the distribution induced on the codebooks does not lend the bins \( C_{3j} (m_{3j}) : m_{3j} \in \mathcal{M}_{3j} \) to be statistically independent. Secondly, since the cloud center and satellite codebooks are binned, the error event needs to be carefully partitioned and analyzed separately.

In this appendix, we seek an upper bound on \( P((\epsilon_1 \cup \epsilon_3)^c \cap \epsilon_{4j}) \) for \( j = 2, 3 \). Let \( (\epsilon_1 \cup \epsilon_3)^c \cap \epsilon_{4j} = \epsilon_{4j}^1 \cup \epsilon_{4j}^2 \cup \epsilon_{4j}^3 \), where

\[
\epsilon_{4j}^1 := \bigcup_{\tilde{M}_{3j} \neq M_{3j}} \bigcup_{\tilde{\alpha}_{3j} \in \mathcal{U}_{3j}} \bigcup_{\tilde{b}_{3j} \in \mathcal{C}_{3j}} \left\{ (q^n, U_j(\tilde{\alpha}_{3j}), X_j(M_{3j}, \tilde{\alpha}_{3j}, \tilde{b}_{3j}, X_j \in T_{2n}(Q, U_j, Y_1, Y_2)) \right\},
\]

\[
\epsilon_{4j}^2 := \bigcup_{\tilde{M}_{3j} \neq M_{3j}} \bigcup_{\tilde{\alpha}_{3j} \in \mathcal{U}_{3j}} \bigcup_{\tilde{b}_{3j} \in \mathcal{C}_{3j}} \left\{ (q^n, U_j(\tilde{\alpha}_{3j}), X_j(M_{3j}, \tilde{\alpha}_{3j}, \tilde{b}_{3j}, X_j \in T_{2n}(Q, U_j, Y_1, Y_2)) \right\},
\]

\[
\epsilon_{4j}^3 := \bigcup_{\tilde{M}_{3j} \neq M_{3j}} \bigcup_{\tilde{\alpha}_{3j} \in \mathcal{U}_{3j}} \bigcup_{\tilde{b}_{3j} \in \mathcal{C}_{3j}} \left\{ (q^n, U_j(\tilde{\alpha}_{3j}), X_j(M_{3j}, \tilde{\alpha}_{3j}, \tilde{b}_{3j}, X_j \in T_{2n}(Q, U_j, Y_1, Y_2)) \right\},
\]
We now consider two factors of generic term in the above summation. Since 
and 
Before we substitute the right hand sides of the above two identities in (63), we simplify the terms involved in the 
We now consider two factors of generic term in the above summation. Since 
and 
the above two identities in (63), we simplify the terms involved in the 

By the law of total probability, we have

Now recognize that a generic term of the sum in (63) is a product of the left hand sides of the above two identities.

Before we substitute the right hand sides of the above two identities in (63), we simplify the terms involved in the second identity (involving the two sums). Denoting

Let us work with 

1. If 

if 
otherwise.
Substituting the above observations in (63), we have

\[
P(\epsilon_j^c \cap \epsilon_{k,j}^c) \leq \sum_{m_j \in M, \hat{m}_j \neq m_j, \hat{a}_j \neq a_j} \sum_{a_j \neq a_j} \sum_{x_j \in \mathcal{C}_j} \sum_{x_j \neq x_j} \sum_{T(q)} \theta(y_j^n|x_j^n) \sum_{m_j \in M} P(M_j = m_j) \exp \{-2nH(X_j|Q)\} \frac{\theta^2(q^n)}{\theta^2(q^n)} \exp \{-nH(U_j, X_j|Y_j, Q)\} + \\
+ \sum_{m_j \in M, \hat{m}_j \neq m_j, \hat{a}_j \neq a_j} \sum_{x_j \in \mathcal{C}_j} \sum_{x_j \neq x_j} \sum_{T(q)} \theta(y_j^n|x_j^n) \sum_{m_j \in M} P(M_j = m_j) \exp \{-nH(X_j|Q)\} \frac{\theta^2(q^n)}{\theta^2(q^n)} \exp \{-nH(U_j, X_j|Y_j, Q)\} \mathbb{Z}_j(n).
\]

Using the upper bounds on the size of the conditional frequency typical sets \(T_{4n_1}(U_j, X_j|y_j^n, q^n)\) and \(T_{4n_1}(U_j|x_j^n, y_j^n, q^n)\), for sufficiently large \(n\) (Lemma 5), we have

\[
P(\epsilon_j^c \cap \epsilon_{k,j}^c) \leq \sum_{m_j \in M, \hat{m}_j \neq m_j, \hat{a}_j \neq a_j} \sum_{a_j \neq a_j} \sum_{x_j \in \mathcal{C}_j} \sum_{x_j \neq x_j} \sum_{T(q)} \theta(y_j^n|x_j^n) \sum_{m_j \in M} P(M_j = m_j) \exp \{-2nH(X_j|Q) + 8n\} \exp \{-nH(U_j, X_j|Y_j, Q)\} \mathbb{Z}_j(n) + \\
+ \sum_{m_j \in M, \hat{m}_j \neq m_j, \hat{a}_j \neq a_j} \sum_{a_j \neq a_j} \sum_{x_j \in \mathcal{C}_j} \sum_{x_j \neq x_j} \sum_{T(q)} \theta(y_j^n|x_j^n) \sum_{m_j \in M} P(M_j = m_j) \exp \{-nH(X_j|Q) + 8n\} \exp \{-nH(U_j, X_j|Y_j, Q)\} \mathbb{Z}_j(n).
\]

Substituting the lower bound for \(\mathbb{Z}_j(n)\) from (44) and noting that the terms in the summation do not depend on the arguments of the sum, for \(n \geq N_{11}(\eta_1)\), it can be verified that

\[
P(\epsilon_j^c \cap \epsilon_{k,j}^c) \leq 2 \frac{\theta^\eta}{\theta^\eta} \exp \{-nH(X_j|Q) + 8n\} \exp \{-nH(U_j, X_j|Y_j, Q)\} \mathbb{Z}_j(n) + 1.
\]

Finally, substituting \(\frac{s_j \log \theta}{n} = S_j, \delta\), we have, for sufficiently large \(n\),

\[
P(\epsilon_j^c \cap \epsilon_{k,j}^c) \leq 2 \exp \{-n[\log \theta - H(U_j|X_j, Y_j, Q)] - S_j - (8\eta_1 + 4\eta)\} + \\
+ 2 \exp \{-n[\log \theta + H(X_j|Q) - H(U_j, X_j|Y_j, Q)] - (S_j + K_j) - (16\eta_1 + 4\eta)\} + \\
\leq 4 \exp \{-n[\delta - (16\eta_1 + 8\eta)]\}.
\]

We follow a similar sequence of steps to derive an upper bound on \(P(\epsilon_j^c)\). Defining \(\widetilde{T}(q^n)\) as in (62), we have

\[
P(\epsilon_j^c \cap \epsilon_{k,j}^c) \leq \sum_{m_j \in M, \hat{m}_j \neq m_j, \hat{a}_j \neq a_j} \sum_{a_j \neq a_j} \sum_{x_j \in \mathcal{C}_j} \sum_{x_j \neq x_j} \sum_{T(q^n)} P \left\{ Y_j^n = y_j^n \left| \begin{array}{l} X_j^n(m_j, \hat{b}_j, X_j) = z_j^n, U_j(\hat{a}_j) = \hat{u}_j, Y_j^n = u_j^n, \\
X_j^n(M_j, B_j) = x_j^n, U_j(A_j) = u_j^n \end{array} \right. \right\} \cap \epsilon_j^c.
\]

We now consider two factors of a generic term in the above sum. Since \(X_j^n(M_1), X_j^n(M_\pi X, B_\pi X)\) is independent of the collection \(X_j^n(\hat{m}_j, \hat{b}_j, X_j), U_j(\hat{a}_j), I_j(\hat{a}_j), I_j(\hat{a}_j), M_j, X_j^n(M_j, B_j, X_j), U_j(A_j)\) for any \(\hat{a}_j, \hat{b}_j, X_j\) as long as \(\hat{m}_j \neq M_j\), and \(Y_j^n - (X_j^n(M_1), X_j^n(M_j, B_j, X_j) : j = 2, 3) - (X_j^n(\hat{m}_j, \hat{b}_j, X_j), U_j(\hat{a}_j), I_j(\hat{a}_j), I_j(\hat{a}_j), M_j, X_j^n(M_j, B_j, X_j), U_j(A_j))\) is a Markov chain, we have

\[
P \left\{ Y_j^n = y_j^n \left| \begin{array}{l} X_j^n(\hat{m}_j, \hat{b}_j, X_j) = z_j^n, U_j(\hat{a}_j) = \hat{u}_j, \\
I_j(A_j) = I_j(\hat{a}_j), M_j, X_j^n(m_j, \hat{b}_j, X_j) = x_j^n, U_j(A_j) = u_j^n \end{array} \right. \right\} \cap \epsilon_j^c = P \left\{ Y_j^n = y_j^n \left| X_j^n(M_j, B_j) = x_j^n \right. \right\} = \hat{\theta}(y_j^n|x_j^n).
\]

By the law of total probability, we have

\[
P \left\{ \begin{array}{l} X_j^n(\hat{m}_j, \hat{b}_j, X_j) = \hat{z}_j^n, U_j(\hat{a}_j) = \hat{u}_j, \\
I_j(A_j) = I_j(\hat{a}_j) = M_j, X_j^n(m_j, \hat{b}_j, X_j) = x_j^n, U_j(A_j) = u_j^n \end{array} \right\} \cap \epsilon_j^c = \sum_{m_j \in M, \hat{m}_j \neq m_j, \hat{a}_j \neq a_j} \sum_{a_j \neq a_j} \sum_{x_j \in \mathcal{C}_j} \sum_{x_j \neq x_j} \sum_{T(q^n)} P \left\{ \begin{array}{l} X_j^n(\hat{m}_j, \hat{b}_j, X_j) = \hat{z}_j^n, U_j(\hat{a}_j) = \hat{u}_j, \\
I_j(A_j) = I_j(\hat{a}_j) = M_j, X_j^n(m_j, \hat{b}_j, X_j) = x_j^n, U_j(A_j) = u_j^n \end{array} \right\} \cap \epsilon_j^c.
\]
\[
\begin{align*}
\sum_{m_j \in M, \hat{b} \in \epsilon} & \sum_{m_j \in M, \hat{b} \in \epsilon} P \left( \left\{ X_n^p(\hat{m}_i, \hat{b}_j) = \hat{x}_n^p, U_j(\hat{a}^{\prime}_i) = \hat{a}^{\prime}_i \right\} \right) \cap \epsilon_j^2
\end{align*}
\]

Now recognize that a generic term of the sum in (67) is a product of the left hand sides of the above two identities. Before we substitute the right hand sides of the above two identities in (67), we simplify the terms involved in the second identity (the two sums). Denoting

\[
E^2 := \left\{ X_n^p(\hat{m}_i, \hat{b}_j) = \hat{x}_n^p, U_j(\hat{a}^{\prime}_i) = \hat{a}^{\prime}_i \right\} \cap \epsilon_j^2
\]

and evaluating \(P(E_2)\) (similar to \(P(E_1)\)), and substituting this in (67), we get

\[
P(\epsilon_j^c \cap \epsilon_j^2) = \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} P \left( \left\{ X_n^p(\hat{m}_i, \hat{b}_j) = \hat{x}_n^p, U_j(\hat{a}^{\prime}_i) = \hat{a}^{\prime}_i \right\} \right) \cap \epsilon_j^2
\]

We now employ the upper bounds on \(|T_{4\eta}(X_j|u_n^p, y_n^p, q^n)|\) and \(|T_{4\eta}(U_j, Y_j|u_n^p, y_n^p, q^n)|\). For sufficiently large \(n\),\n
\[
|T_{4\eta}(X_j|u_n^p, y_n^p, q^n)| \leq \exp \{ n(H(X_j|U_j, Y_j, Q) + 8\eta) \}
\]

for all \((u_n^p, y_n^p, q^n) \in T_{2\eta}(U_j, Y_j, Q)\). For such an \(n\), we have

\[
P(\epsilon_j^c \cap \epsilon_j^2) \leq \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} P \left( \left\{ X_n^p(\hat{m}_i, \hat{b}_j) = \hat{x}_n^p, U_j(\hat{a}^{\prime}_i) = \hat{a}^{\prime}_i \right\} \right) \cap \epsilon_j^2
\]

Substituting the lower bound for \(\mathcal{L}_j(n)\) from (44), we have

\[
P(\epsilon_j^c \cap \epsilon_j^2) \leq 2 \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} P \left( \left\{ X_n^p(\hat{m}_i, \hat{b}_j) = \hat{x}_n^p, U_j(\hat{a}^{\prime}_i) = \hat{a}^{\prime}_i \right\} \right) \cap \epsilon_j^2
\]

Finally, we get

\[
P(\epsilon_j^c \cap \epsilon_j^2) \leq 2 \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} \sum_{m_j \in M, \hat{b} \in \epsilon} P \left( \left\{ X_n^p(\hat{m}_i, \hat{b}_j) = \hat{x}_n^p, U_j(\hat{a}^{\prime}_i) = \hat{a}^{\prime}_i \right\} \right) \cap \epsilon_j^2
\]
We are left to study

\[ P_{\text{union bound}} \] yields

\[
\begin{align*}
P\left( Y_j = y_j \bigg| X_j = x_j, U_j = u_j, A_j = a_j \right) &= \hat{\theta}(y_j^n|x_j^n), \\
\mathbb{E}[Y_j] &= \sum_{y_j, x_j, \theta} P(Y_j = y_j) \cdot y_j \cdot P(X_j = x_j) \cdot P(U_j = u_j) \cdot P(A_j = a_j) \\
&= \sum_{y_j, x_j} P(Y_j = y_j) \cdot y_j \cdot P(X_j = x_j) \cdot P(U_j = u_j) \cdot P(A_j = a_j).
\end{align*}
\]

We have for sufficiently large \( n \)

\[
P(\epsilon_i^c \cap \epsilon_j^c) \leq 2 \exp \left\{ -n \left( I(X_j; U_j, Y_j) - K_j - L_j - \left( \log^\theta + H(X_j|Y_j, Q) \right) \right) \right\}
\]

We are left to study \( P(\epsilon_A^c). \) Defining \( \hat{T}(\eta) \) as in (62), and

\[
E^3 := \left\{ \left. X_j^n = x_j^n, B_j = b_j, U_j = u_j, A_j = a_j \right| (u_j^n, x_j^n, a_j^n) \in \hat{T}(\eta), \hat{T}(\eta) \right\}
\]

As earlier, we consider a generic term in the above sum and simplify the same. Observe that

\[
P\left( Y_j^n \bigg| \hat{T}(\eta) \right) = P\left( Y_j^n \bigg| X_j^n = x_j^n \right).
\]

Substituting the above observations in (70), we have

\[
P(\epsilon_i^c \cap \epsilon_j^c) \leq \sum_{m_{ij}, \tilde{m}_{ij}} \sum_{m_{ij} \neq \tilde{m}_{ij}} \sum_{m_{ij} \neq \tilde{m}_{ij}} \sum_{\eta, \theta} P(\theta) \cdot \hat{T}(\eta)^2 \cdot \sum_{y_j, x_j} P(Y_j = y_j, \theta) \cdot P \left( \left. X_j = x_j \right| \theta \right) \cdot P \left( \left. U_j = u_j \right| \theta \right) \cdot P \left( \left. A_j = a_j \right| \theta \right) \cdot \mathbb{E}[Y_j | y_j^n, x_j^n, \theta].
\]

There exists \( N_{15}(\eta) \in \mathbb{N} \) such that for all \( n \geq \max\{N_{12}(\eta), N_{15}(\eta)\} \), we have

\[
|T_{n, (U_j, X_j^n, Y_j^n)}| \leq \exp \left\{ n(\theta(\eta) + H(X_j|Y_j, Q)) + 8n \eta \right\}
\]

and hence

\[
P(\epsilon_i^c \cap \epsilon_j^c) \leq \sum_{m_{ij}, \tilde{m}_{ij}} \sum_{m_{ij} \neq \tilde{m}_{ij}} \sum_{\eta, \theta} P(\theta) \cdot \hat{T}(\eta)^2 \cdot \sum_{y_j, x_j} P(Y_j = y_j, \theta) \cdot P \left( \left. X_j = x_j \right| \theta \right) \cdot P \left( \left. U_j = u_j \right| \theta \right) \cdot P \left( \left. A_j = a_j \right| \theta \right) \cdot \mathbb{E}[Y_j | y_j^n, x_j^n, \theta].
\]
APPENDIX G

PROOF OF PROPOSITION[2]

We begin by stating the conditions for sub-optimality of \( \mu SB \)–technique.

**Lemma 4:** Consider example[3] with \( \delta := \delta_2 = \delta_3 \in (0, \frac{1}{2}) \) and \( \tau := \tau_2 = \tau_3 \in (0, \frac{1}{2}) \). Let \( \beta := \beta_1 = \beta_2 \). Let \( \beta : = \beta_1 * (2\tau^2) \). The rate triple \( \beta, \gamma, \delta \) satisfy

\[
\gamma, \delta \in \mathbb{R}^{3-1}(\tau_1, \tau_2, \delta_1) \quad \text{if} \quad h_b(\gamma, \delta) > h_b(\gamma_1(1 - \beta) + (1 - \tau_1)\beta - h_b(\delta_1)
\]

In particular, if \( \tau_1 \) is true, \( \alpha_\mu (\tau) \subseteq \beta(\tau, \delta) \), where \( \beta(\tau, \delta) \) is defined in [3].

**Proof:** We prove this by contradiction. Suppose \( \beta, \gamma, \delta \in \text{cl}(\alpha_j^{3-1}(p_{\mu Q_j} u_j \alpha_j)) \text{ for some } p_{\mu Q_j} u_j \alpha_j \in \mathbb{D}^{3-1}(\tau_1, \tau_2, \delta_1) \). In the sequel, we characterize such \( p_{\mu Q_j} u_j \alpha_j \) and employ the same to derive a contradiction. Our first claim is that \( p_{X_2|Q}(1|q) = p_{X_1|Q}(1|q) = \tau \) for all \( q \in Q \).

From (1) we have

\[
R_j \leq I(U_j X_j; Y_j|Q) = H(Y_j|Q) - H(Y_j|X_j U_j Q) = H(Y_j|Q) - h_b(\delta) = \sum_{q \in Q} p_Q(q) H(Y_j|Q = q) - h_b(\delta)
\]

If \( \tau_1 := p_{X_1|Q}(1|q) \), then independence of the pair \( N_j \times X_j \) implies \( p_{X_j|Q}(1|q) = \tau(1 - \delta) + (1 - \tau_1)\delta = \tau_1(1 - \delta) + \delta \). Substituting the same in (73), we have

\[
R_j \leq \sum_{q \in Q} p_Q(q) h_b(\gamma_1(1 - 2\delta) + \delta) - h_b(\delta) \leq h_b(p_{X_1}(1) - 2(1 - \delta) + \delta) - h_b(\delta)
\]

from Jensen’s inequality. Since \( p_{X_1}(1) \leq \tau < \frac{1}{2} \), we have \( p_{X_1}(1) - 2(1 - \delta) + \delta < \frac{1}{2} (1 - 2\delta) + \delta = \frac{1}{2} \).

The term \( h_b(p_{X_1}(1) - 2(1 - \delta) + \delta) \) is therefore strictly increasing in \( p_{X_1}(1) \) and is at most \( h_b(\gamma_1 + \delta) \). Moreover, the condition for equality in Jensen’s inequality implies \( R_j = h_b(\gamma_1 + \delta) - h_b(\delta) \) if and only if \( p_{X_1|Q}(1|q) = \tau \) for all \( q \in Q \) that satisfies \( p_Q(q) > 0 \). We have therefore proved our first claim.

Our second claim is an analogous statement for \( p_{X_1|Q}(1|q) \). In particular, our second claim is that \( p_{X_1|Q}(1|q) = \tau_1 \) for each \( q \in Q \) of positive probability. We begin with the upper bound on \( R_1 \) in (1). As in proof of proposition[1] we let \( \hat{Q} := Q \times U_2 \times U_3 \), \( \hat{q} = (q, u_2, u_3) \in \hat{Q} \) denote a generic element and \( \hat{Q} := (Q, U_2, U_3) \). The steps we employ in proving the second claim borrows steps from proof of proposition[1] and the proof of the first claim presented above. Note that

\[
R_1 \leq I(X_1; Y_1|\hat{Q}) = H(Y_1|\hat{Q}) - H(Y_1|\hat{Q}X_1)
\]

\[
= \sum_{\hat{q}} p_{\hat{Q}}(\hat{q}) H(X_1 \oplus N_1 \oplus (X_2 \vee X_3)|\hat{Q} = \hat{q}) - \sum_{x_1, \hat{q}} p_{X_1,\hat{Q}}(x_1, \hat{q}) H(N_1 \oplus (X_2 \vee X_3)|\hat{Q} = \hat{q})
\]

\[
\leq \sum_{\hat{q}} p_{\hat{Q}}(\hat{q}) H(X_1 \oplus N_1|\hat{Q} = \hat{q}) - \sum_{\hat{q}} p_{\hat{Q}}(\hat{q}) H(N_1|\hat{Q} = \hat{q}) = \sum_{\hat{q}} p_{\hat{Q}}(\hat{q}) H(X_1 \oplus N_1|\hat{Q} = \hat{q}) - h_b(\delta_1)
\]

\[
= \sum_{\hat{q}} p_{\hat{Q}}(\hat{q}) h_b(\gamma_1 + \delta) - h_b(\delta_1) \leq h_b(\mathbb{E}_{\hat{Q}}[\gamma_1 + \delta] - h_b(\delta_1) = h_b(p_{X_1}(1) + \delta_1) - h_b(\delta_1)
\]

\[
\text{Here we have used the positivity of } (1 - 2\delta), \text{ or equivalently } \delta \text{ being in the range } (0, \frac{1}{2}).
\]
where (i) follows from substituting $p_{X_i \oplus N_i|Q}(\cdot|q)$ for $p_{Z_i}$, $p_{N_i|Q}(\cdot|q)$ for $p_{Z_2}$ and $p_{X_2 \land X_3|Q}(\cdot|q)$ for $p_{Z_3}$ in lemma \[1\] (iii) the first inequality in (76) follows from Jensen’s inequality. Since $p_{X_1}(1) \leq \tau_1 < \frac{1}{2}$, we have $p_{X_1}(1) * \delta_1 = p_{X_1}(1 - \delta_1) + (1 - p_{X_1}(1)) \delta_1 = p_{X_1}(1)(1 - 2\delta_1) + \delta_1 \leq \tau_1(1 - 2\delta_1) + \delta_1 \leq \frac{1}{2}(1 - 2\delta_1) + \delta_1 = \frac{1}{2}$. Therefore $h_b(p_{X_1}(1) * \delta_1)$ is increasing\[19\] in $p_{X_1}(1)$ and is bounded above by $h_b(\tau_1 * \delta_1)$. Moreover, the condition for equality in Jensen’s inequality implies $R_1 = h_b(\tau_1 * \delta_1) - h_b(\delta_1)$ if and only if $p_{X_1|Q}(1|q) = \tau_1$ for all $q \in \tilde{Q}$.

We have therefore proved our second claim\[20\]

Our third claim is that either $H(X_2|Q, U_2) > 0$ or $H(X_3|Q, U_3) > 0$. Suppose not, i.e., $H(X_2|Q, U_2) = H(X_3|Q, U_3) = 0$. In this case, the upper bound on $R_1 + R_2 + R_3$ in (2) is

$$R_1 + R_2 + R_3 \leq I(X_2, X_3; X_1; Y_1|Q) = H(Y_1|Q) - H(Y_1|Q, X_1, X_2, X_3)$$

where the last equality follows from substituting $p_{X_j|Q}$: $j = 1, 2, 3$ derived in the earlier two claims\[21\]. The hypothesis \[72\] therefore precludes $(h_0(\tau_1 * \delta_1) - h_b(\delta_1), h_b(\tau * \delta) - h_b(\delta), h_b(\tau * \delta) - h_b(\delta)) \in \alpha_j^{-1}(p_{QU_2U_3XY})$ if $H(X_2|Q, U_2) = H(X_3|Q, U_3) = 0$. This proves our third claim.

Our fourth claim is $H(X_2 \lor X_3|Q, U_2, U_3) > 0$. The proof of this claim rests on each of the earlier three claims. Note that we have either $H(X_2|Q, U_2) > 0$ or $H(X_3|Q, U_3) > 0$. Without loss of generality, we assume $H(X_2|Q, U_2) > 0$. We therefore have a $u_2^* \in U_2$ such that $p_{U_2|Q}(u_2^*|q^*) > 0$ and $H(X_2|U_2 = u_2^*, Q = q^*) > 0$. This implies $p_{X_2|U_2Q}(x_2|u_2^*, q^*) \notin \{0, 1\}$ for each $x_2 \in \{0, 1\}$. Since $p_Q(q^*) > 0$, from the first claim we have $0 < 1 - \tau = p_{X_3|Q}(0|q^*) = \sum_{q_3 \in U_3} p_{X_3|U_3Q}(0, u_3^*|q^*)$. This guarantees existence of $u_3^* \in U_3$ such that $p_{X_3|U_3Q}(0, u_3^*|q^*) > 0$. We therefore have $p_{U_3|Q}(u_3^*|q^*) > 0$ and $1 \geq p_{X_3|U_3Q}(0|u_3^*|q^*) > 0$.

We have therefore identified $(q^*, u_2^*, u_3^*) \in \mathcal{Q} \times \mathcal{U}_2 \times \mathcal{U}_3$ such that $p_Q(q^*) > 0$, $p_{U_2|Q}(u_2^*|q^*) > 0$, $p_{U_3|Q}(u_3^*|q^*) > 0$, $p_{X_2|U_2Q}(x_2|u_2^*, q^*) \notin \{0, 1\}$ for each $x_2 \in \{0, 1\}$ and $1 \geq p_{X_3|U_3Q}(0|u_3^*|q^*) > 0$. By conditional independence of the pairs $(X_2, U_2)$ and $(X_3, U_3)$ given $Q$, we also have $p_{X_2|U_2Q}(x_2|u_2^*, u_3^*, q^*) \notin \{0, 1\}$ for each $x_2 \in \{0, 1\}$ and $1 \geq p_{X_3|U_3Q}(0|u_3^*|q^*) > 0$. The reader may now verify $p_{p_{Q|U_3Q}(u_3^*|q^*)} p_{Q|U_3Q}(u_3^*|q^*) p_{U_3|Q}(u_3^*|q^*) > 0$, we have proved the fourth claim.

Our fifth and final claim is $R_1 < h_b(\tau_1 * \delta_1) - h_b(\delta_1)$. This follows from a sequence of steps employed in proof of the second claim herein, or in the proof of proposition \[1\]. Denoting $\tilde{Q} = (Q, U_2, U_3)$ and a generic element

\[19\] This also employs the positivity of $1 - 2\delta_1$, or equivalently $\delta_1$ being in the range $(0, \frac{1}{2})$.

\[20\] We have only proved $p_{X_j|Q}(1|q, u_2, u_3 = \tau_1)$ for all $(q, u_2, u_3) \in \mathcal{Q} \times \mathcal{U}_2 \times \mathcal{U}_3$ of positive probability. The claim now follows from conditional independence of $X_1$ and $U_2, U_3$ given $Q$.

\[21\] $\beta = (1 - \tau)^2 \delta_1 + (2\tau - \tau^2)(1 - \delta_1)$ is as defined in the statement of the lemma.
\[ R_1 \leq I(X_1; Y_1 | \tilde{Q}) = \sum_{\hat{q}} p_{\tilde{Q}}(\hat{q}) H(X_1 \oplus N_1 \oplus (X_2 \vee X_3) | \tilde{Q} = \hat{q}) - \sum_{\hat{q}} p_{\tilde{Q}}(\hat{q}) H(N_1 \oplus (X_2 \vee X_3) | \tilde{Q} = \hat{q}) \]
\[ < \sum_{\hat{q}} p_{\tilde{Q}}(\hat{q}) H(X_1 \oplus N_1 \tilde{Q} = \hat{q}) - \sum_{\hat{q}} p_{\tilde{Q}}(\hat{q}) H(N_1 \tilde{Q} = \hat{q}) = \sum_{\hat{q}} p_{\tilde{Q}}(\hat{q}) H(X_1 \oplus N_1 | \tilde{Q} = \hat{q}) - h_b(\delta_1) \] (77)
\[ = \sum_{\hat{q}} p_{\tilde{Q}}(\hat{q}) h_b(\tau_1 \hat{q} \ast \delta_1) - h_b(\delta_1) \leq h_b(\mathbb{E}_{\tilde{Q}} \{ \tau_1 \hat{q} \ast \delta_1 \}) - h_b(\delta_1) = h_b(p_{X_1}(1) \ast \delta_1) - h_b(\delta_1), \] (78)

where (i) (77) follows from existence of a \( \hat{q}^* \) in \( \tilde{Q} \) for which \( H(X_2 \vee X_3 | \tilde{Q} = \hat{q}^*) > 0 \) and substituting \( p_{X_1 \oplus N_1 | \tilde{Q}}(\cdot | \hat{q}^*) \) for \( p_{Z_1}, p_{N_1 | \tilde{Q}}(\cdot | \hat{q}^*) \) for \( p_{Z_2} \) and \( p_{X_2 \vee X_3 | \tilde{Q}}(\cdot | \hat{q}^*) \) for \( p_{Z_3} \) in lemma \( \text{II} \). (iii) the first inequality in (78) follows from Jensen’s inequality. Since \( p_{X_1}(1) \ast \delta_1 = p_{X_1}(1 - \delta_1) + (1 - p_{X_1}(1))\delta_1 = p_{X_1}(1)(1 - 2\delta_1) + \delta_1 \leq \tau_1(1 - 2\delta_1) + \delta_1 \leq \frac{1}{2}(1 - 2\delta_1) + \delta_1 = \frac{1}{2}. \) Therefore \( h_b(p_{X_1}(1) \ast \delta_1) \) is increasing \(^{22}\) in \( p_{X_1}(1) \) and is bounded above by \( h_b(\tau_1 \ast \delta_1). \) We therefore have \( R_1 < h_b(\tau_1 \ast \delta_1) - h_b(\delta_1). \)

We now derive conditions under which \( \alpha_j^{3-1}(\tau_1, \tau, \tau) = \mathbb{C}(\tau_1, \tau, \tau). \) Clearly, \( \mathbb{C}(\tau_1, \tau, \tau) \subseteq \mathbb{B}(\tau, \hat{\delta}) \) where \( \tau = (\tau_1, \tau, \tau) \) and \( \hat{\delta} = (\delta_1, \delta, \delta). \) It therefore suffices to derive conditions under which \( (h_b(\tau_1 \ast \delta_1) - h_b(\delta_1), h_b(\tau \ast \delta) - h_b(\delta), h_b(\tau \ast \delta) - h_b(\delta)) \in \alpha_j^{3-1}(\tau_1, \tau, \tau) \).

**Lemma 5:** Consider example \( \text{II} \) with \( \delta_1 = \delta_2 = \delta_3 \in (0, \frac{1}{2}) \) and \( \tau_1 = \tau_2 = \tau_3 \in (0, \frac{1}{2}). \) Let \( \beta_1 = \delta_1 \ast (2\tau - \tau^2). \) The rate triple \( (h_b(\tau_1 \ast \delta_1) - h_b(\delta_1), h_b(\tau \ast \delta) - h_b(\delta), h_b(\tau \ast \delta) - h_b(\delta)) \in \alpha_j^{3-1}(\tau_1, \tau, \tau) \) i.e., achievable using coset codes, if,

\[ h_b(\tau \ast \delta) - h_b(\delta) \leq \theta, \]

where \( \theta = h_b(\tau) - h_b((1 - \tau^2) - (2\tau - \tau^2)h_b(\frac{x^2}{2\tau - \tau^2}) - h_b(\tau \ast \delta_1) + h_b(\tau \ast \beta_1). \) We therefore have \( \alpha_j^{3-1}(\tau_1, \tau, \tau) = \mathbb{C}(\tau_1, \tau, \tau) \) if (79) holds.

**Proof:** The proof only involves identifying the appropriate test channel \( p_{QU_{\hat{U}}X_{\hat{Y}}} \in D_j^{3-1}(\tau_1, \tau, \tau). \) Let \( \hat{Q} = \phi \) be empty, \( \hat{U} = \{0, 1, 2\}. \) Let \( p_{X_1}(1) = 1 - p_{X_1}(0) = \tau_1. \) Let \( p_{U_j X_j}(0, 0) = 1 - p_{U_j X_j}(1, 1) = 1 - \tau \) and therefore \( P(U_j = 2) = P(X_j \neq U_j) = 0 \) for \( j = 2, 3. \) It is easily verified that \( p_{QU_{\hat{U}}X_{\hat{Y}}} \in D_j^{3-1}(\tau_1, \tau, \tau) \) i.e., in particular respects the cost constraints. The choice of this test channel, particularly the ternary field, is motivated by \( H(X_2 \vee X_3 U_2 \oplus U_3) = 0. \) The decoder 1 can reconstruct the interfering pattern after having decoded the ternary sum of the codewords.

**APPENDIX H**

**PROOF OF PROPOSITION 3**

We prove proposition \( \text{III} \) by splitting the same into the two following lemmas.

**Lemma 6:** Consider example \( \text{III} \) and let \( \mathbb{C}^*, C_1, D(\tau), p_{X_{\hat{Y}}}^* \) be defined as above. If

\[ C_1 + 2(h_b(\tau \ast \delta) - h_b(\delta)) = I(X_1; Y_1 | X_2 \vee X_3) + 2(h_b(\tau \ast \delta) - h_b(\delta)) \geq I(X_1; Y_1), \]

\(^{22}\)This also employs the positivity of \( 1 - 2\delta_1 \), or equivalently \( \delta_1 \) being in the range \( (0, \frac{1}{2}). \)
where the mutual information terms \( I(X_1; Y_1 | X_2 \lor X_3), I(X_2; Y_1) \) are evaluated with respect to \( p_{XY}^* \), then \( C^* \notin \alpha_u(\mathcal{X}) \).

The reader will recognize that above lemma is the counterpart of lemma 4 for example 5.

Proof: The proof here closely mimics proof of lemma 4. In fact, we allude to appendix G to avoid restating certain elements.

We assume \( C^* \in \alpha_u(\mathcal{X}) \), and derive a contradiction. Suppose \( C^* \in \text{cocl}(\alpha_u(p_{QU_3XY})) \) for some \( p_{QU_3XY} \in \mathcal{D}_u(\mathcal{T}) \).

In the sequel, we characterize such a \( p_{QU_3XY} \) and employ the same to derive a contradiction. Our first claim, as in appendix G, is \( \alpha_u(\mathcal{X}) \) holds verbatim, we allude to the same for a proof of this claim. We conclude the triplet \((Q, X_1), X_2, X_3\) to be mutually independent, and in particular \( X_1, X_2, X_3 \) to be mutually independent. We conclude that for any \( p_{QU_3XY} \in \mathcal{D}_u(\mathcal{T}) \) for which \( C^* \in \text{cocl}(\alpha_u(p_{QU_3XY})) \), we have its corresponding marginal \( p_{XY} \in \mathcal{D}(\mathcal{T}) \).

Our second claim is \( p_{X_1|Q}(1|q) = p_{X_1}(1) \) for every \( q \in \mathcal{Q} \) for which \( p_{Q}(q) > 0 \). We begin with the upper bound on \( R_1 \) in (1). Denoting

\[
I(p_{A|C}(\cdot|c); p_{B|A,C}(\cdot|\cdot|c)) : = I(A; B|C = c)
\]

for any random variables \( A, B, C \), we have,

\[
I(X_1; Y_1 | Q, U_2, U_3) \leq I(X_1; Y_1 | Q, X_2 \lor X_3) \quad (81)
\]

\[
= \sum_{s} p_{X_2 \lor X_3}(s) \sum_{q} p_{Q|X_2 \lor X_3}(q|s) I \left( p_{X_1|Q, X_2 \lor X_3}(\cdot|q, s); p_{Y_1|X_1, Q, X_2 \lor X_3}(\cdot|q, s) \right) \quad (82)
\]

\[
\leq \sum_{s} p_{X_2 \lor X_3}(s) I \left( \sum_{q} p_{Q|X_2 \lor X_3}(q|s) p_{X_1|Q, X_2 \lor X_3}(\cdot|q, s); p_{Y_1|X_1, Q, X_2 \lor X_3}(\cdot|q, s) \right) \quad (83)
\]

\[
= \sum_{s} p_{X_2 \lor X_3}(s) I \left( p_{X_1|Q, X_2 \lor X_3}(\cdot|s); p_{Y_1|X_1, Q, X_2 \lor X_3}(\cdot|s) \right) = I(X_1; Y_1 | X_2 \lor X_3) \leq C_1 \quad (84)
\]

where (i) follows from the Markov chains \((U_2, U_3) - (X_2 \lor X_3) - Y_1\) and \((U_2, U_3) - (X_1, X_2 \lor X_3) - Y_1\), (ii) follows from the Markov chain \( Q - X_1, X_2 \lor X_3 - Y_1 \) resulting from the nature of the channel from the inputs to \( Y_1 \), (iii) follows from Jensen’s inequality, and (iv) follows from \( p_{XY} \in \mathcal{D}(\mathcal{T}) \) and definition of \( C_1 \). The strict concavity of \( I(p_A(\cdot); p_B(\cdot|\cdot)) \) in \( p_A(\cdot) \) implies equality holds in (83) if and only if \( p_{X_1|Q, X_2 \lor X_3}(1|q, s) = p_{X_1|Q}(1|q) \) is invariant with \( q \) for every \( q \in \mathcal{Q} \) for which \( p_{Q}(q) > 0 \). By the uniqueness of \( p_{XY}^* \), and in particular \( p_{X_1}^* \), we conclude \( p_{X_1|Q}(1|q) = p_{X_1}(1) \) for every \( q \in \mathcal{Q} \) for which \( p_{Q}(q) > 0 \).

Our first and second claims imply that if \( C^* \in \text{cocl}(\alpha_u(p_{QU_3XY})) \) for some \( p_{QU_3XY} \in \mathcal{D}_u(\mathcal{T}) \), then \( p_{QU_3XY} \in \mathcal{D}(\mathcal{T}) \), and furthermore, \( Q \) is independent of \( X \). We therefore reiterate that any entropy or mutual information terms involving random variables in \( X, Y \), stated in the sequel, is evaluated with respect to \( p_{XY}^* \).

23 Recall \( \mathcal{T} : = (\tau_1, \tau, \tau) \).

24 We have proved in our first claim \( Q \) and \((X_2, X_3)\) are independent.
Our third claim is that either \( H(X_2|Q, U_2) > 0 \) or \( H(X_3|Q, U_3) > 0 \). Suppose not, i.e., \( H(X_2|Q, U_2) = H(X_3|Q, U_3) = 0 \). In this case, the upper bound on \( R_1 + R_2 + R_3 = C_1 + 2(h_b(\tau * \delta) - h_b(\delta)) \) in (2) is

\[
R_1 + R_2 + R_3 = C_1 + 2(h_b(\tau * \delta) - h_b(\delta)) \leq I(X_2, X_3, X_1; Y_1|Q) = I(\tilde{X}; Y_1)
\]

where the last equality follows from independence of \( X \) and \( \tilde{X} \) and thereby implying independence of \( Q \) and \( X \). \((85)\) contradicts the hypothesis \((80)\) of the lemma.

Our fourth claim is \( H(X_2 \vee X_3|Q, U_2, U_3) > 0 \). The proof of this claim is identical to the proof of the corresponding claim in appendix \( \Box \) and the reader is alluded to the same. As a consequence of \( H(X_2 \vee X_3|\tilde{Q}) > 0 \), where \( \tilde{Q} : = (Q, U_2, U_3) \), there exists \( \tilde{q}^* : = (q^*, u_2^*, u_3^*) \in \tilde{Q} : = Q \times U_2 \times U_3 \) for which \( p_{\tilde{Q}}(\tilde{q}^*) > 0 \) and \( H(X_2 \vee X_3|\tilde{Q} = \tilde{q}^*) > 0 \).

Our fifth claim and final claim is that \( H(X_2 \vee X_3|Q, U_2, U_3) > 0 \) implies \( C_1 < I(X_1; Y_1|X_2 \vee X_3) \) thereby contradicting the definition of \( C_1 \) \((6)\). The reader will recognize that our proof for the fifth claim in appendix \( \Box \) cannot be employed here. We employ a more powerful technique that we will have opportunity to use in our study of example \( \Box \) The upper bound \( (1) \) on \( R_1 \) implies

\[
C_1 = R_1 \leq I(X_1; Y_1|\tilde{Q}) = \sum_{\tilde{q}} p_{\tilde{Q}}(\tilde{q})I(p_{X_1|\tilde{Q}}(\cdot|\tilde{q}); p_{Y_1|X_1, \tilde{Q}}(\cdot, \tilde{q}))
\]

\[
= \sum_{\tilde{q}} p_{\tilde{Q}}(\tilde{q}) \left( \sum_{s} p_{Y_1|X_1, X_2 \vee X_3, \tilde{Q}}(\cdot, s, \tilde{q}) p_{X_2 \vee X_3|\tilde{Q}}(s|\tilde{q}) \right)
\]

\[
< \sum_{s, \tilde{q}} p_{\tilde{Q}}(\tilde{q}) \sum_{s} p_{X_2 \vee X_3}(s|\tilde{q})I(p_{X_1|\tilde{Q}}(\cdot|\tilde{q}); p_{Y_1|X_1, X_2 \vee X_3}(\cdot|s, \tilde{q})) \tag{86}
\]

\[
= \sum_{s, \tilde{q}} p_{\tilde{Q}}(\tilde{q}) p_{X_2 \vee X_3}(\tilde{q}|s)I(p_{X_1}(\cdot); p_{Y_1|X_1, X_2 \vee X_3}(\cdot|s)) \tag{87}
\]

\[
= \sum_{s, \tilde{q}} p_{\tilde{Q}}(\tilde{q}) p_{X_2 \vee X_3}(\tilde{q}|s)I(p_{X_1|X_2 \vee X_3}(\cdot|s); p_{Y_1|X_1, X_2 \vee X_3}(\cdot|s)) = I(X_1; Y_1|X_2 \vee X_3) \leq C_1, \tag{88}
\]

where (i) \((86)\) follows from strict convexity of the mutual information in the conditional distribution (channel transition probabilities), the presence of \( \tilde{q}^* \in \tilde{Q} \) for which \( p_{X_2 \vee X_3|Q}(\cdot|\tilde{q}^*) \) is non-degenerate and \( p_{Y_1|X_1, X_2 \vee X_3, \tilde{Q}}(\cdot, s, \tilde{q}^*) \) distinct, (ii) \((87)\) follows from conditional independence of \( X_1 \) and \( (U_2, U_3) \) given \( Q \), the second claim above, and the Markov chain \( \tilde{Q} = X_1, X_2 \vee X_3 \) induced by the nature of the channel, and (iii) \((88)\) follows from \( X_1, X_2, X_3 \) being mutually independent, \( p_{X_2 X_3} \in D(\tau) \) and the definition of \( C_1 \). We have thus derived a contradiction \( C_1 < C_1 \).

Lemma 7: Consider example \( \Box \) Let \( C_1, p_{X_2 X_3} \) be as defined above. If \( h_b(\tau^2) + (1 - \tau^2)h_b\left(\frac{1+2\tau^2}{1-\tau^2}\right) + H(Y_1|X_2 \vee X_3) - H(Y_1) \leq \min\{H(X_2|Y_2), H(X_3|Y_3)\} \), where the entropies are evaluated with respect to \( p_{X_2 X_3} \), then \( (C_1, h_b(\delta * \tau) - h_b(\delta), h_b(\delta * \tau) - h_b(\delta)) \in \alpha_{f}^{3-1}(\tau) \).

Proof: As in proof of lemma \( \Box \) we identify an appropriate test channel \( p_{U_2 U_3 X_2 X_3} \in D_f(\tau) \) for which

\[
(C_1, h_b(\delta * \tau) - h_b(\delta), h_b(\delta * \tau) - h_b(\delta)) \in \alpha_{f}^{3-1}(p_{U_2 U_3 X_2 X_3}) \). Let \( Q = \phi \) be empty, \( U_2 = U_3 = \{0, 1, 2\} \). Let \( p_X = p_{X_2}^\tau \). Let \( p_{U_j, X_j}(0, 0) = 1 - p_{U_j, X_j}(1, 1) = 1 - \tau \) and therefore \( P(U_j = 2) = P(X_j \neq U_j) = 0 \) for \( j = 2, 3 \). It is easily verified that \( p_{U_2 U_3 X_2 X_3} \in D_{f}^{3-1}(\tau) \), i.e., in particular respects the cost constraints.
It maybe verified that the hypothesis \(h_b(\tau^2) + (1 - \tau^2)h_b\left(\frac{(1-\tau)^2}{\tau}\right) + H(Y_1|X_2 \lor X_3) - H(Y_1) = H(U_2 \oplus U_3) + H(Y_1|X_2 \lor X_3) - H(Y_1) = H(U_2 \oplus U_3) + H(Y_1|U_2 \oplus U_3) - H(Y_1) = H(U_2 \oplus U_3 | Y_1)\). We therefore have \(H(U_2 \oplus U_3 | Y_1) \leq \min\{H(X_2|Y_2)H(X_3|Y_3)\}\). This implies (i) \(H(U_j) \geq H(U_2 \oplus U_3 | Y_1)\) and (ii) \(H(U_j) - H(U_2 \oplus U_3 | Y_1) \geq H(U_j - H(U_j | Y_j) = I(U_j; Y_j) = I(X_j; Y_j) = h_b\).

Employing these in bounds characterizing \(\alpha_f^{-1}(p_{QU_{XY}^{U_3}})\) and the marginal \(p_{XY} = p_{XY}^{U_3}\), it can be verified that \((C_1, h_b(\delta * \tau) - h_b(\delta), h_b(\delta * \tau) - h_b(\delta)) \in \alpha_f^{-1}(p_{QU_{XY}^{U_3}})\).

\[\blacksquare\]

**APPENDIX I**

**PROOF OF THEOREM 5**

We provide an illustration of the main arguments of the proof without giving complete details. In view of our detailed proof of theorem 5, the interested reader can fill in the details. We begin with an alternate characterization of \(\alpha_f^{-1}(p_{XY})\) in terms of the parameters of the code.

**Definition 11:** Consider \((p_{QU_{XY}^{U_3}}, w) \in \mathbb{D}_g(\mathbb{Z})\) and let \(G : = U_2 = U_3\). Let \(\tilde{\alpha}_f^{-1}(p_{QU_{XY}^{U_3}}, w)\) be defined as the set of rate triples \((R_1, R_2, R_3) \in [0, \infty)^3\) for which \(\bigcup_{\delta > 0} \tilde{S}(R_1, p_{QU_{XY}^{U_3}}, w, \delta)\) is non-empty, where \(\tilde{S}(R_1, p_{QU_{XY}^{U_3}}, w, \delta)\) is defined as the collection of vectors \((S_2, T_2, L_2, S_3, T_3, L_3, R_g) \in [0, \infty)^9\) that satisfy for \(j = 2, 3\), with \(Z = U_2 \oplus U_3\).

\[
R_j = T_j + L_j, \quad (S_j - T_j) > \log |G| - H(U_j|Q) + \delta, \quad R_g > S_j + \delta
\]

\[
S_j < S_{U_2}^G(U_j; 0|Q) + \log |G| - H(U_j|Q) + \delta, \quad T_j > \delta, \quad L_j > \delta, \quad L_j < I(X_j; Y_j|U_j Q) - \delta,
\]

\[
S_j + L_j < \log |G| + I(X_j; Y_j|U_j Q) + C_w^G(U_j; Y_j|Q) - H(U_j|Q) - \delta, \quad R_1 < I(X_1; Y_1|ZQ) - \delta
\]

\[
R_1 + R_g < \log |G| + I(X_1; Y_1|ZQ) + C_w^G(Z; Y_1|Q) - H(Z|Q) - \delta
\]

**Lemma 8:** \(\tilde{\alpha}_f^{-1}(p_{QU_{XY}^{U_3}}, w) = \alpha_f^{-1}(p_{QU_{XY}^{U_3}}, w)\).

**Proof:** The proof follows from Fourier-Motzkin elimination.

Choose the parameters \((R_1, S_2, T_2, L_2, S_3, T_3, L_3, R_g) \in [0, \infty)^10\). The coding technique is exactly the same as that considered in the case of finite fields and is given in the proof of Theorem 5. The main exception is that the PCCs are built on the abelian group \(G\). Instead of constructing vector spaces of \(\mathcal{F}^n\), we construct subgroups of \(G^n\). The cloud center codebook \(\lambda_j\) of user \(j\) is characterized as follows. Let

\[
J_j = \bigoplus_{(p, r) \in \mathbb{Q}(G)} \mathbb{Z}_{p}^{q, w, r}\quad J = \bigoplus_{(p, r) \in \mathbb{Q}(G)} \mathbb{Z}_{p}^{q, w, r}
\]

for \(j = 2, 3\) with \(s = \max\{s_2, s_3\}\), where \(s_j\) will be specified shortly. Note that \(J_j \leq J\) for \(j = 2, 3\). Let \(\phi\) be a homomorphism from \(J\) into \(G^n\). Let \(\phi_j\) be the restriction of \(\phi\) to \(J_j\) for \(j = 2, 3\). It is shown in [32 Equation 11] that \(\phi\) has the following representation

\[
\phi(a) = \bigoplus_{(p, r, m) \in \mathbb{Q}(G^n)(q, t, l) \in \mathbb{Q}(J)} a_{(q, t, l);(q, t, l) \in \mathbb{Q}(J)}
\]
where \( g_{(q,t,l),(p,r,m)} = 0 \) for \( p \neq q \) and \( g_{(q,t,l),(p,r,m)} \) is uniformly distributed over \( p^{r-t}Z_{p^r} \) for \( p = q \). The code \( \lambda_j \) is given by \( \phi_j(J_j) \oplus b_j^p \), where \( b_j^p \) is a bias vector in \( G^n \). Choose \( s_2, s_3 \) and \( s \) such that

\[

s_2 = \frac{nS_2}{\sum_{(p,r) \in Q(G)} rw_{p,r} \log p}, \quad s_3 = \frac{nS_3}{\sum_{(p,r) \in Q(G)} rw_{p,r} \log p}, \quad s = \frac{nR_g}{\sum_{(p,r) \in Q(G)} rw_{p,r} \log p}

\]

Note that

\[

\frac{1}{n} \log |J| = \frac{s}{n} \sum_{(p,r) \in Q(G)} rw_{p,r} \log p = R_g, \quad \frac{1}{n} \log |J_j| = S_j : j = 2, 3.

\]

The binning functions \( i_j \) are defined analogously: \( i_j : J_j \rightarrow |G|^{|t_j|} \), where \( t_j \log |G| = nT_j \), for \( j = 2, 3 \). The encoding and decoding operations are defined analogously. This implies that \( |M_1| = 2^{nR_1} \), \( |M_{j1}| = |G|^{|t_j|} \) for \( j = 2, 3 \). The homomorphism and the bias vectors are chosen independently and with uniform probability over their ranges.

For any \( a, \tilde{a} \in J \), and \( (q,s,l) \in \mathcal{G}(J) \), let \( \theta_{q,s,l}(a) = \min_{(p,r) \in \mathcal{Q}(G)} |r - s| + \hat{\theta}_{q,s,l} \).

Define for any \( a \in J \), and any \( \theta = (\theta_{p,r})_{(p,r) \in Q(G)} \), the set \( T_{I_2}(a) = \{ \tilde{a} \in J : \forall (p,r) \in Q(G), \theta_{p,r}(a, \tilde{a}) = \theta_{p,r} \} \).

It can be shown that the expected value of the probability of all the error events over the ensemble approach zero as the block length increases if the parameters of the code belong to \( \hat{\mathcal{A}}_g^{3-t} \left( p_{QU_2U_3XY}, w \right) \). For conciseness, we give proofs of the elements in this argument that are new as compared to the analysis done in the case of fields.

**Upper bound on \( P(e_{I_2}) \):** Given a message \( m_2 \) that indexes the bin in the cloud center codebook, define

\[

\psi_2(m_{21}) = \sum_{a \in J_2} \sum_{u_2 \in T_{2n}(U_2)} 1_{\{ \phi(a) + b_2 = u_2, I_2(a) = m_{21} \}}

\]

We have

\[

\mathbb{E} \{ \psi_2(m_{21}) \} = \sum_{a \in J_2} \sum_{u_2 \in T_{2n}(U_2)} 1_{\{ \phi(a) + b_2 = u_2, I_2(a) = m_{21} \}} \frac{1}{|G|^n} \cdot \frac{1}{|G|^t_2} = \frac{|J_2| \cdot |T_{2n}(U_2)|}{|G|^n} \cdot \frac{1}{|G|^t_2}

\]

and let \( r, 0 \) be vectors whose components are indexed by \( (p,r) \in Q(G) \), and whose \( (p,r) \)th component is equal to \( r \) and 0, respectively. Then,

\[

\mathbb{E} \{ \psi_2(m_{21})^2 \} = \sum_{\theta \in \Theta} \sum_{a \in J_2} \sum_{\tilde{a} \in T_{2n}(U_2)} \sum_{u_2 \in T_{2n}(U_2)} \sum_{u_2' \in T_{2n}(U_2)} 1_{\{ \phi(a) + b_2 = u_2 + u_2', I_2(a) = m_{21} \}} \frac{1}{|G|^n} \cdot \frac{1}{|G|^t_2}

\]

\[

= \sum_{a \in J_2} \sum_{u_2 \in T_{2n}(U_2)} \frac{1}{|G|^n} \cdot \frac{1}{|G|^t_2} + \sum_{\theta \in \Theta} \sum_{a \in J_2} \sum_{\tilde{a} \in T_{2n}(U_2)} \sum_{u_2 \in T_{2n}(U_2)} \sum_{u_2' \in T_{2n}(U_2)} \frac{1}{|G|^n} \cdot \frac{1}{|H_0|^n} \cdot \frac{1}{|G|^t_2} \cdot \mathbb{E} \{ |T_{2n}(U_2)| \}

\]

\[

\leq \frac{|J_2| \cdot |T_{2n}(U_2)|}{|G|^n} \cdot \frac{1}{|G|^t_2} + \sum_{\theta \in \Theta} \sum_{a \in J_2} |T_{2n}(U_2) \cdot |T_{2n}(U_2)| \cdot |T_{2n}(U_2) \cap (u_2 + H_0^n)| \cdot \frac{1}{|G|^n} \cdot \frac{1}{|H_0|^n} \cdot \frac{1}{|G|^t_2} \cdot \mathbb{E} \{ |T_{2n}(U_2)| \}

\]
Using Lemma IX.2, we get
\[
\frac{\mathbb{V}(\psi_2(m_{21})^2)}{\mathbb{E}^2(\psi_2(m_{21}))} \leq \frac{|G|^n \cdot |G^t|}{|J_2| \cdot 2^n[H(U_2|Q) - \eta]} + \sum_{\theta \in \Theta} \sum_{a \in J_2} \frac{|G|^n \cdot |T_{J_2, \theta}(a)| \cdot 2^n[H(U_2|Q) + \eta]}{|J_2| |H_\theta|^n \cdot 2^n[H(U_2|Q) - \eta]}
\]

Using Lemma IX.2] we have \(|T_{J_2, \theta}(a)| \leq 2^n(1 - \omega_\theta)(S_2 + \eta_3)\), and hence for the probability of error to go to zero, we require
\[
(S_2 - T_2) > \log |G| - H(U_2|Q), \quad S_2 > \max_{\theta \neq 0} \frac{1}{\omega_\theta} \log |G : H_\theta| - H([U_2|\theta]Q).
\]

**Upper bound on \(P_1\)**: This probability can be decomposed into two parts: (i) the first, \(P_1\), is the probability of the event that \(X_1^n\) and \(U_2^n + U_3^n\) are both decoded incorrectly and (ii) the second, \(P_2\), is the probability of the event that \(X_1^n\) is decoded incorrectly but \(U_2^n + U_3^n\) is decoded correctly. In the following we provide an upper bound only on the first part. For a fixed code we have,
\[
P_1 \leq \frac{1}{|M_1|} \sum_{m_1} \sum_{x_1, u_2, u_3 \in T_{2n_2}(X_1, U_2, U_3)} \frac{1}{|G|^2} \sum_{m_{21}, m_{31}} \frac{1}{|G|^2} \mathbb{E} \left\{ \psi_2(m_{21}) \right\} \sum_{u_4 \in T_{2n_2}(U_3)} \frac{1}{|G|^2} \mathbb{E} \left\{ \psi_3(m_{31}) \right\} \sum_{y_1 \in Y_1^n} \left\{ \prod_{i=1}^n \phi_{x_i, u_i, u_{i-1}, Z} \right\} \sum_{\tilde{z} \neq z} \left\{ \tilde{z} = (\tilde{x}_1, \tilde{y}_1, \tilde{z}) \right\} \left\{ \exists \epsilon \in J : \phi(\tilde{z}) + b_2 = \tilde{z}, \tilde{z} \neq a + b \right\}
\]

Taking expectation and using the union bound we get
\[
\mathbb{E}(P_1) \leq \sum_{\theta \neq \theta} \sum_{a \in J_2} \frac{2^{-n_4} 2^{-n_4} 2^n[H(X_1|Z, Y_1) + \eta]}{|J_2|} \frac{|T_{J_2, \theta}(a + b)|}{|H_\theta|^n} \cdot 2^n[H(X_1|Q) - \eta].
\]

Using Lemma IX.2, note that \(|T_{J_2, \theta}(a + b)| \leq 2^n(1 - \omega_\theta)R_g\). Therefore, it suffices to have
\[
R_1 + (1 - \omega_\theta)R_g < I(X_1; Y_1|Q) + \log |H_\theta| - H(Z|\theta Y_1|Q)
\]

for \(\theta \neq r\). For optimum weights \(\{w_{p,r}\}_{(p,r) \in \Theta(G)}\), the condition \(R_1 + R_g < I(X_1; Y_1|Q) + C_G(Z; Y_1|Q) + \log |G| - H(Z|Q)\) implies
\[
R_g < \min_{\theta \neq r} \frac{1}{1 - \omega_\theta} \left[ I(X_1; Y_1|Q) - R_1 \right] + \min_{\theta \neq r} \frac{1}{1 - \omega_\theta} \left[ \log |H_\theta| - H(Z|Z_\theta Y_1) \right]
\]

which is the desired condition. In the above equations, \((a)\) follows since the maximum of \(1 - \omega_\theta\) is attained for \(\theta = 0\) and is equal to 1. We have thus proved the bounds provided in definition (11) suffice to drive the probability of incorrect decoding exponentially down to 0.
APPENDIX J

PROOF OF PROPOSITION 4

We first note that for any \( p_{QU}^{X_3|XY} \in \mathcal{D}_u(\tau, 0, 0) \) with \( H(X_j|Q,U_j) = 0 \) for \( j = 2, 3 \), we have \( R_1 + R_2 + R_3 < I(X;Y_1) \leq \sup_{p_{X_1|X_2}p_{X_3}} I(X;Y_1) \). This follows from substituting the corresponding quantities in (23). It can be easily verified that

\[
\sup_{p_{X_1|X_2}p_{X_3}} I(X;Y_1) = 2 - h_b(\delta_1) - \delta_1 \log_2 3
\]

which is achieved for all those distributions \( p_{X_1|X_2}p_{X_3} \) that ensure \( Y_1 \) is uniformly distributed. Condition (25) therefore implies \( (C^*, 2 - h_b(\delta) - \delta \log_2 3, 2 - h_b(\delta) - \delta \log_2 3) \notin \alpha_u(p_{QU}^{X_3|XY}) \) if \( H(X_j|Q,U_j) = 0 \) for \( j = 2, 3 \). Hence either \( H(X_2|Q,U_2) > 0 \) or \( H(X_3|Q,U_3) > 0 \). Assume \( H(X_j|Q,U_j) > 0 \) and \( \{j, \ell\} = \{2, 3\} \). By the conditional independence of \( (U_2, X_2) \) and \( (U_3, X_3) \) given \( Q \), we have \( 0 < H(X_j|Q,U_j) = H(X_j|Q,U_j,U_\ell,X_\ell) = H(X_j \oplus_4 X_\ell|Q,U_j,U_\ell,X_\ell) = H(X_j \oplus_4 X_3|Q,U_2,U_3,X_\ell) \leq H(X_2 \oplus_3 X_3|Q,U_2,U_3) \). We only need to prove \( H(X_2 \oplus_3 X_3|Q,U_2,U_3) > 0 \) implies \( I(X_1|Y_1; Q,U_2,U_3) < C^* \). For this, we allude to the proof of fifth claim in appendix H. Therein, we have proved an analogous statement for example [3] The statement herein can be proved through an analogous sequence of steps and we let the reader fill in these details.

We now show that user 1 can achieve rate equal to \( C^* \) exploiting the fact that user 2 and 3 use group codes. We also derive the condition (25) in terms of parameters \( \delta_1, \tau, \delta \). Note that the channel between \( X_2 \oplus_4 X_3 \) and \( Y_1 \) is additive with noise given by \( X_1 \oplus_4 N_1 \). Let us choose \( p_{X_1}(x_1) = \frac{x_1}{3} \) for \( x_1 \in \{1, 2, 3\} \). The resulting distribution of \( X_1 \oplus_4 N_1 \) is given by \( p_{X_1 \oplus_4 N_1}(a) = \beta/3 \) for \( a \in \{1, 2, 3\} \). Using concavity of entropy once again, we get

\[
C_w^G(X_2 \oplus_4 X_3; Y) = \min\{2 - h_b(\beta) - \beta \log_2 3, 2 + 2h_b(2\beta/3) - 2h_b(\beta) - 2\beta \log_2 3\} = 2 - h_b(\beta) - \beta \log_2 3.
\]

Note that for \( \delta_1 \in (0, \frac{1}{4}) \) and \( \tau < \frac{3}{4} \), using the fact that \( X_1 \) and \( N_1 \) are independent, we get \( \beta \in (0, \frac{3}{4}) \). Note also that \( 2 - h_b(\beta) - \beta \log_2 3 \) is monotone decreasing for \( \beta \in (0, 3/4) \). Hence if \( \beta \leq \delta \), the signal \( X_2 \oplus_4 X_3 \) can be decoded at decoder 1, and user 1 can communicate at the rate \( C^* \). A simple calculation yields

\[
C^* = h_b(\beta) + \beta \log_2 3 - h_b(\delta_1) - \delta_1 \log_2 3.
\]

REFERENCES

[1] A. Carleial, “Interference channels,” Information Theory, IEEE Transactions on, vol. 24, no. 1, pp. 60–70, 1978.
[2] T. Han and K. Kobayashi, “A new achievable rate region for the interference channel,” Information Theory, IEEE Transactions on, vol. 27, no. 1, pp. 49 – 60, jan 1981.
[3] M. Maddah-Ali, A. Motahari, and A. Khandani, “Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis,” Information Theory, IEEE Transactions on, vol. 54, no. 8, pp. 3457–3470, Aug 2008.
[4] V. Cadambe and S. Jafar, “Interference alignment and degrees of freedom of the k -user interference channel,” IEEE Trans. on Info. Th., vol. 54, no. 8, pp. 3425–3441, 2008.
[5] G. Bresler, A. Parekh, and D. Tse, “The approximate capacity of the many-to-one and one-to-many Gaussian interference channels,” Information Theory, IEEE Transactions on, vol. 56, no. 9, pp. 4566 –4592, sept. 2010.
[6] S.-N. Hong and G. Caire, “On interference networks over finite fields,” Information Theory, IEEE Transactions on, vol. 60, no. 8, pp. 4902–4921, Aug 2014.
[7] S. Krishnamurthy and S. Jafar, “On the capacity of the finite field counterparts of wireless interference networks,” Information Theory, IEEE Transactions on, vol. 60, no. 7, pp. 4101–4124, July 2014.
[8] U. Niesen and M. Maddah-Ali, “Interference alignment: From degrees of freedom to constant-gap capacity approximations,” Information Theory, IEEE Transactions on, vol. 59, no. 8, pp. 4855–4888, Aug 2013.
[9] J. Körner and K. Marton, “How to encode the modulo-two sum of binary sources (corresp.),” IEEE Trans. Inform. Theory, vol. 25, no. 2, pp. 219 – 221, Mar 1979.

[10] 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.

[11] T. Philosof, R. Zamir, U. Erez, and A. Khisti, “Lattice strategies for the dirty multiple access channel,” Information Theory, IEEE Transactions on, vol. 57, no. 8, pp. 5006–5035, Aug 2011.

[12] Y. Kochman, A. Khina, U. Erez, and R. Zamir, “Rematch and forward: Joint source/channel coding for communications,” in Electrical and Electronics Engineers in Israel, 2008. IEEE 2008. IEEE 25th Convention of, Dec 2008, pp. 779–783.

[13] Y. Kochman and R. Zamir, “Joint wyner-ziv/dirty-paper coding by modulo-lattice modulation,” Information Theory, IEEE Transactions on, vol. 55, no. 11, pp. 4878–4889, Nov 2009.

[14] D. Krithivasan and S. Pradhan, “Distributed source coding using abelian group codes: A new achievable rate-distortion region,” Information Theory, IEEE Transactions on, vol. 57, no. 3, pp. 1495–1519, March 2011.

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

[16] M. Maddah-Ali, A. Motahari, and A. Khandani, “Signaling over MIMO multi-base systems: Combination of multi-access and broadcast schemes;” in Information Theory, 2006 IEEE International Symposium on, July 2006, pp. 2104–2108.

[17] S. Sridharan, A. Jafarian, S. Vishwanath, S. Jafar, and S. Shamai, “A layered lattice coding scheme for a class of three user Gaussian interference channels,” in 2008 46th Annual Allerton Conference Proceedings on, sept. 2008, pp. 531 –538.

[18] A. Jafarian and S. Vishwanath, “Achievable rates for k-user Gaussian interference channels,” submitted to IEEE Trans. of Information theory 2011, available at http://arxiv.org/abs/1109.5336.

[19] O. Ordentlich, U. Erez, and B. Nazer, “The approximate sum capacity of the symmetric Gaussian K-user interference channel,” in Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on, July 2012, pp. 2072–2076.

[20] B. Bandemer and A. El Gamal, “Interference decoding for deterministic channels,” Information Theory, IEEE Transactions on, vol. 57, no. 5, pp. 2966–2975, 2011.

[21] A. Padakandla and S. Pradhan, “Achievable rate region based on coset codes for multiple access channel with states,” submitted to IEEE Trans. on Info. Th., available at http://arxiv.org/abs/1301.5655.

[22] V. R. Cadambe and S. A. Jafar, “Interference alignment and a noisy interference regime for many-to-one interference channels,” available at http://arxiv.org/abs/0912.3029.

[23] 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 Trans. on Info. Th., vol. 29, no. 3, pp. 396 – 412, may 1983.

[24] R. G. Gallager, Information Theory and Reliable Communication. New York: John Wiley & Sons, 1968.

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

[26] S. R. Krishnamurthy and S. A. Jafar, “On the capacity of the finite field counterparts of wireless interference networks,” available at http://arxiv.org/abs/1304.7745.

[27] P. Gács and J. Körner, “Common information is far less than mutual information,” Problems of Control and Information Theory, vol. 2, no. 2, pp. 119–162, 1972.

[28] H. S. Witsenhausen, “On sequences of pairs of dependent random variables,” SIAM Journal of Applied Mathematics, vol. 28, no. 1, pp. 100–113, January 1975.

[29] M. Hall, The theory of groups. New York: Macmillan, 1959.

[30] W. Hoeffding, “Asymptotically optimal tests for multinomial distributions,” Annals of Mathematical Statistics, vol. 36, no. 2, pp. 369–401, 1965.

[31] I. Sanov, “On the probability of large deviations of random variables,” Matematicheskii Sbornik, vol. 42(84), pp. 11–44, 1957, translated by Dana E. A. Quade, Institute of Statistics, Mimeograph Series No. 192, March 1958, available at.

[32] A. Sahebi and S. Pradhan, “Abelian group codes for source coding and channel coding,” submitted to IEEE Trans. of Information theory, April 2013, available at http://arxiv.org/abs/1305.1598.