Achievable rate region for three user discrete broadcast channel based on coset codes

Arun Padakandla
University of Michigan
Ann Arbor, MI 48109, USA
Email: arunpr@umich.edu

S. Sandeep Pradhan
University of Michigan
Ann Arbor, MI 48109, USA
Email: pradhanv@eecs.umich.edu

***Abstract*—We present an achievable rate region for the general three user discrete broadcast channel (DBC), based on coset codes. We identify an example of a three user DBC for which the proposed achievable rate region strictly enlarges that obtained by a natural extension of Marton's [1] rate region. As a step towards deriving the achievable rate region for the general three user DBC, we characterize and derive an achievable rate region for a new class - $3\!-\!\text{to}\!-\!1$ DBC- of broadcast channels of which the aforementioned is an example.**

I. Problem Statement and contributions

The problem of characterizing the capacity region of a broadcast channel (BC) was formulated [2] in 1972. Superposition [3] and binning [1] together yield the currently known largest achievable (Marton's) rate region. The question of it's optimality has since remained open.

Recently, there has been renewed interest [4] in settling this question. Gohari and Anantharam [5] have proved computability of Marton's rate region and identified a class of two user discrete BCs (2-DBC) for which Marton's [1] rate region when computed is strictly smaller than the tightest known outer bound [6]. On the other hand, Weingarten, Steinberg and Shamai [7] have proved Marton's binning (dirty paper coding (DPC)[8] in this context) to be optimal for Gaussian MIMO BC with any number of receivers, and thereby characterized capacity region for the particular class of Gaussian vector BCs.

In this article, we derive an achievable rate region for the general three user discrete BC (3-DBC) based on coset codes and thereby strictly enlarge the currently known largest achievable rate region[1]. A key element of our findings is the identification of a novel 3-DBC for which Marton's coding technique is strictly sub-optimal. We begin by describing the essential aspects of our findings.

II. The central idea

The central aspect of a coding technique designed for a BC is interference management. The two coding techniques - superposition and binning - exemplify two known ways of tacking interference. Superposition enables each user to decode a *univariate* component of the other user's signal and thus subtract it off. Binning enables the encoder counter each user's interfering signal not decoded by the other by precoding for the same. Except for particular cases, the most popular being DPC, precoding results in a rate loss, and is therefore less efficient than decoding the interfering signal at the decoder. The presence of a rate loss motivates each decoder to decode as large a part of interference as possible.[2]

In a 3-BC, reception at each receiver is plagued, in general, by a bivariate function of signals intended for the other users. *It is therefore natural to enable each user decode the relevant bivariate interfering component, not just univariate components of the other two user's signals.* Does the extension of Marton's coding decode a bivariate interfering component of the other user's signals, and if yes, how? Traditional unstructured coding, on which Marton's technique is based does not enable decoding a bivariate component of signals without decoding the arguments in their entirety. The latter strategy is in general inefficient. In the sequel, we lend credence to this statement by referring to the gamut of related problems.

Aptly describing this phenomenon, the problem of reconstructing mod-2 sum of distributed binary sources [9] exemplifies the limitations of traditional unstructured coding.[3] More recently, other problem instances [10], [11], [12] have been identified, wherein the need to decode a bivariate function has been efficiently met by employing structured codebooks. The coding technique proposed herein is based on the framework developed in [10] and in particular reminiscent of that proposed in [12] for the three user interference channel.

How do structured codes enable decode the bivariate interference component more efficiently? This is best described by the use of linear codes in decoding the sum interference component. Let us assume that codebooks of users 2 and 3 are built over the the binary field $\mathcal{F}_2$ and the sum of user 2 and 3 codewords is the interference component at receiver 1. If user 2 and 3 build independent codebooks of rate R_2 and R_3 respectively, the range of interference patterns has rate $R_2 + R_3$. Enabling user 1 decode the sum interference pattern constrains the sum $R_2 + R_3$. Instead if codebooks of users 2

[1]The largest known achievable rate region for 3-DBC is the natural extension of Marton's rate region for 2-DBC. When referred to in the context of 3-DBC, Marton's rate region refers to this natural extension.

[2]For the Gaussian case, there is no rate loss. Thus the encoder can precode all the interference. Indeed, the optimal strategy does not require any user to decode a part of signal not intended for it. This explains why lattices are not necessary to achieve capacity of Gaussian vector BC.

[3]Even after three decades, we are unaware of an unstructured coding technique that achieves rates promised by Körner and Marton.

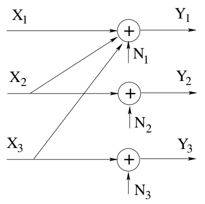

Fig. 1. 3-DBC with octonary input and binary outputs (Example 1).

and 3 are sub-codes of a common linear code, then enabling user 1 to decode the sum will only constrain $\max\{R_2, R_3\}$.

In the following section, we identify a 3-DBC that makes concrete our remarks in this section.

III. A THREE USER BROADCAST CHANNEL

Example 1: Consider the 3-DBC depicted in figure 1. Let the input alphabet $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3$ be a triple Cartesian product of the binary field $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{X}_3 = \mathcal{F}_2$ and the output alphabets $\mathcal{Y}_1 = \mathcal{Y}_2 = \mathcal{Y}_3 = \mathcal{F}_2$ be binary fields. If $X = X_1X_2X_3$ denote the three binary digits input to the channel, then the outputs are $Y_1 = X_1 \oplus X_2 \oplus X_3 \oplus N_1$, $Y_2 = X_2 \oplus N_2$ and $Y_3 = X_3 \oplus N_3$, where (i) N_1, N_2, N_3 are independent binary random variables with $P(N_j = 1) = \delta_j \in (0, \frac{1}{2})$ and (ii) (N_1, N_2, N_3) is independent of the input X. The binary digit X_1 is constrained to an average Hamming weight of $\tau \in (0, \frac{1}{2})$. In other words, $\kappa(x_1x_2x_3) = 1_{\{x_1=1\}}$ and the average cost of input is constrained to $\tau \in (0, \frac{1}{2})$. The channel transition probabilities of this 3-DBC are $W_{\underline{Y}|X}(y_1, y_2, y_3|x_1x_2x_3) = BSC_{\delta_1}(y_1|x_1 \oplus x_2 \oplus x_3)BSC_{\delta_2}(y_2|x_2)BSC_{\delta_3}(y_3|x_3)$, where $\delta_j \in (0, \frac{1}{2}) : j = 1, 2, 3$, $BSC_\eta(1|0) = BSC_\eta(0|1) = 1 - BSC_\eta(0|0) = 1 - BSC_\eta(1|1) = \eta$ for any $\eta \in (0, \frac{1}{2})$ and the cost function $\kappa(x_1x_2x_3) = 1_{\{x_1=1\}}$.

We begin with some observations for the above channel. Users 2 and 3 see *interference free point to point* links from the input. It is therefore possible to communicate to them simultaneously at their point to point capacities using any point to point channel codes achieving their respective capacities. For the purpose of this discussion, let us assume $\delta := \delta_2 = \delta_3$. This enables us employ the same capacity achieving code of rate $1 - h_b(\delta)$ for both users 2 and 3. What about user 1? Three observations are in order. Firstly, if users 2 and 3 are being fed at their respective point to point capacities, then information can be pumped to user 1 only through the first binary digit, henceforth referred to as X_1. In this case, we recognize that the sum of user 2 and 3's transmissions interferes at receiver 1. Thirdly, the first binary digit X_1 is costed, and therefore cannot cancel the interference caused by users 2 and 3.

Since average Hamming weight of X_1 is restricted to τ, $X_1 \oplus N_1$ is restricted to an average Hamming weight of $\tau * \delta_1$. If the rates of users 2 and 3 are sufficiently small, receiver 1 can attempt to decode codewords transmitted to users 2 and 3, cancel the interference and decode the desired codeword. This will require $2 - 2h_b(\delta) \leq 1 - h_b(\delta_1 * \tau)$ or equivalently $\frac{1+h_b(\delta_1*\tau)}{2} \leq h_b(\delta)$. What if this were not the case?

In the case $\frac{1+h_b(\delta_1*\tau)}{2} > h_b(\delta)$, we are left with two choices. The first choice is to enable decoder 1 decode as large a part of each user 2 and 3's transmissions as possible and precode for the rest of the uncertainty in the interference. The second choice is to attempt decoding the sum of user 2 and 3's codewords, instead of the pair. Marton's coding technique is forced to take the first choice which results in it's sub-optimality.[4] Theorem 1 in conjunction with lemma 1 characterize this sub-optimality. We refer the reader to [13] for a proof. Following theorem 1, we pursue the second choice using linear codes.

Theorem 1: Consider the 3-DBC in example 1. If $2h_b(\delta) < 1 + h_b(\delta_1 * \tau)$, then $(h_b(\tau * \delta_1) - h_b(\delta_1), 1 - h_b(\delta), 1 - h_b(\delta))$ is not achievable using Marton's coding technique for this 3-DBC.

Since linear codes achieve capacity of binary symmetric channels, there exists a single linear code, or a coset thereof, of rate $1 - h_b(\delta)$ that achieves capacity of both user 2 and 3 channels. Let us employ this linear code for communicating to users 2 and 3. The code being linear or affine, the collection of sums of all possible pairs of codewords is restricted to a coset of rate $1 - h_b(\delta)$. This suggests that decoder 1 decode the sum of user 2 and 3 codewords. Indeed, if $1 - h_b(\delta) \leq 1 - h_b(\tau * \delta_1)$, or equivalently $\tau * \delta_1 \leq \delta$, then user 1 can first decode the interference, peel it off, and then go on to decode the desired signal. Under this case, a rate $h_b(\tau * \delta_1) - h_b(\delta_1)$ is achievable for user 1 even while communicating independent information at rate $1 - h_b(\delta)$ for both users 2 and 3. We have therefore proposed a coding technique based on linear codes that achieves the rate triple $(h_b(\tau * \delta_1) - h_b(\delta_1), 1 - h_b(\delta), 1 - h_b(\delta))$ if $\tau * \delta_1 \leq \delta = \delta_2 = \delta_3$. These arguments are summarized in the following lemma.

Lemma 1: Consider the 3-DBC in example 1. If $\tau * \delta_1 \leq \delta = \delta_2 = \delta_3$, then $(h_b(\tau * \delta_1) - h_b(\delta_1), 1 - h_b(\delta), 1 - h_b(\delta)) \in \mathbb{C}(\tau)$.

We emphasize the import of theorem 1 and lemma 1 in the following corollary.

Corollary 1: Consider the 3-DBC in example 1 with $\delta = \delta_2 = \delta_3$. If $h_b(\tau * \delta_1) \leq h_b(\delta) < \frac{1+h_b(\delta_1*\tau)}{2}$, then $(h_b(\tau * \delta_1) - h_b(\delta_1), 1 - h_b(\delta), 1 - h_b(\delta))$ is not achievable using Marton's coding technique. However, $(h_b(\tau * \delta_1) - h_b(\delta_1), 1 - h_b(\delta), 1 - h_b(\delta)) \in \mathbb{C}(\tau)$ and thus Marton's coding technique when extended to the case of three users is strictly sub-optimal. In particular, if $\delta_1 = 0.01$ and $\delta_2 \in (0.1325, 0.21)$, then $\mathbb{C}(\frac{1}{8})$ is not achievable using Marton's coding technique.

We refer the reader to [13] for a study of the case $\delta_2 \neq \delta_3$.

IV. DEFINITIONS: 3-DBC AND $3-$TO-1 DBC

The main emphasis in this article is to build on the phenomenon exemplified by example 1 and propose a more

[4] Since X_1 is costed, precoding results in a rate loss, i.e., in terms of rate achieved, the technique of precoding is in general inferior to the technique of decoding interference. This motivates a preference for decoding the interference as against to precoding. However, for the Gaussian case, precoding suffers *no* rate loss. This is the precise reason for dirty paper coding being optimal for vector Gaussian BCs [7].

efficient strategy for communicating over an arbitrary 3-DBC.[5] The rest of the article is therefore aimed at presenting an achievable rate region for general 3-DBC based on coset codes. In this section, we characterize $3-$to-1 DBC which provides an ideal pedagogical step in presenting our rate region. We begin by defining a general 3-DBC.

A 3-DBC consists of a finite input alphabet set $\mathcal{X}$ and three finite output alphabet sets $\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3$. The discrete time channel is time invariant, memoryless, and used without feedback. Let $W_{\underline{Y}|X}(\underline{y}|x) = W_{Y_1Y_2Y_3|X}(y_1, y_2, y_3|x)$ denote probability of observing $\underline{y} \in \underline{\mathcal{Y}}$ at the respective outputs conditioned on $x \in \mathcal{X}$ being input. The input is constrained with respect to an additive cost function $\kappa : \mathcal{X} \to [0, \infty)$. We refer to this 3-DBC as $(\mathcal{X}, \underline{\mathcal{Y}}, W_{\underline{Y}|X}, \kappa)$. We refer the reader to [1] for relevant standard definitions of a BC. In this article, we restrict attention to communicating private messages to the users and let $\mathbb{C}(W_{\underline{Y}|X}, \kappa, \tau) := \text{cl}\{\underline{R} \in \mathbb{R}^3 : (\underline{R}, \tau) \text{ is achievable}\}$ denote the (private message) capacity region of 3-DBC $(\mathcal{X}, \underline{\mathcal{Y}}, W_{\underline{Y}|X}, \kappa)$ when constrained to average cost of τ. We let $\mathbb{C}(\tau)$ abbreviate $\mathbb{C}(W_{\underline{Y}|X}, \kappa, \tau)$ when the 3-DBC is clear from context.

A 3-DBC $(\mathcal{X}, \underline{\mathcal{Y}}, W_{\underline{Y}|X})$ is a 3-to-1 DBC if $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3$ is a Cartesian product of three alphabet sets such that $W_{Y_2|X}(y_2|(x_1, x_2, x_3)) = W_{Y_2|X_2}(y_2|x_2)$ and $W_{Y_3|X}(y_3|(x_1, x_2, x_3)) = W_{Y_3|X_3}(y_3|x_3)$. Note that transition probabilities $W_{Y_1,Y_2,Y_3|X}$ of a 3-to-1 DBC can be denoted as $W_{Y_1,Y_2,Y_3|X_1X_2X_3}$. Since users 2 and 3 enjoy interference free point to point links, the corresponding receivers need to decode only signals intended for them. Therefore, there is (i) no component of the signal transmitted that is decoded by all receivers and (ii) no components of the signal transmitted that is decoded by users 2 and 3.

V. Achievable rate region for $3-$to-1 DBC using coset codes

In this section, we present the first step in deriving an achievable rate region for the general 3-DBC using coset codes [14]. In particular, we restrict attention to $3-$to-1 DBCs and derive an achievable rate region for this class using the ensemble of coset codes. The coding technique we propose is a generalization of the simple linear coding strategy proposed for example 1. The reader may wish to revisit the same.

A. *Decoding sum of codewords using coset codes : A new achievable rate region for $3-$to-1 DBC*

The essential aspect of the linear coding strategy proposed for example 1 is that users 2 and 3 employ a code that is closed under addition, the linear code being the simplest such example. Since linear codes only achieve symmetric capacity, we are forced to bin codewords from a larger linear code in order to find codewords that are typical with respect to a nonuniform distribution. This is akin to binning for channels with state information, wherein $\exp\{nI(U;S)\}$ codewords, each picked according to $\prod_{t=1}^n p_T$, are chosen for each message in order to find a codeword in $T_\delta(U|s^n)$ jointly typical with state sequence s^n. We now generalize the coding technique proposed for example 1.

Consider auxiliary alphabet sets $\mathcal{V}_1, \mathcal{U}_{21}, \mathcal{U}_{31}$ where $\mathcal{U}_{21} = \mathcal{U}_{31} = \mathcal{F}_q$ be the finite field of cardinality q and let $p_{V_1U_{21}U_{31}X\underline{Y}}$ be a pmf on $\mathcal{V}_1 \times \mathcal{U}_{21} \times \mathcal{U}_{31} \times \mathcal{X} \times \underline{\mathcal{Y}}$. For $j = 2, 3$, let $\lambda_j \subseteq \mathcal{U}_{j1}^n$ be coset of a linear code $\overline{\lambda_j} \subseteq \mathcal{F}_q^n$ of rate $S_{j1} + T_{j1}$. The linear codes are contained in one another, i.e., if $S_{j_11} + T_{j_11} \leq S_{j_22} + T_{j_22}$, then $\overline{\lambda_{j_1}} \subseteq \overline{\lambda_{j_2}}$. Codewords of λ_j are partitioned independently and uniformly into $\exp\{nT_j\}$ bins. A codebook $\mathcal{C}_1$ of rate $K_1 + L_1$ is built over $\mathcal{V}_1$. The codewords of $\mathcal{C}_1$ are independently and uniformly partitioned into $\exp\{nL_1\}$ bins. Messages of users $1, 2, 3$ at rates L_1, T_{21}, T_{31} is used to index a bins in $\mathcal{C}_1, \lambda_2, \lambda_3$ respectively. The encoder looks for a jointly typical triple, with respect to $p_{V_1U_{21}U_{31}}$, of codewords in the indexed triple of bins. Following a second moment method similar to that employed in [14], it can be proved that the encoder finds at least one jointly typical triple if

$$S_{21} \geq \log q - H(U_{21}), S_{31} \geq \log q - H(U_{31}), K_1 \geq 0 \quad (1)$$

$$S_{21} + S_{31} \geq 2\log q - H(U_{21}) - H(U_{31}) + I(U_{21}; U_{31}) \quad (2)$$

$$S_{j1} + K_1 \geq \log q - H(U_{j1}) + I(U_{j1}; V_1) : j = 2, 3 \quad (3)$$

$$\sum_{j=2}^{3} S_{j1} + K_1 \geq 2\log q - \sum_{j=2}^{3} H(U_{j1}) + I(U_{21}; U_{31}; V_1). \quad (4)$$

Having chosen one such jointly typical triple, say $V_1^n, U_{21}^n, U_{31}^n$, it generates a vector X^n according to $\prod_{t=1}^n p_{X|V_1U_{21}U_{31}}(\cdot|V_1^n, U_{21}^n, U_{31}^n)$. This is fed as input to the channel.

Decoders 2 and 3 perform a standard point to point channel decoding. It can be proved by following the technique similar to [14, Proof of Theorem 1] that if

$$S_{j1} + T_{j1} \leq \log q - H(U_{j1}|Y_j) : j = 2, 3 \quad (5)$$

then probability of decoding error at decoders 2 and 3 can be made arbitrarily small for sufficiently large n.

Having received Y_1^n, decoder 1 looks for all codewords $v_1^n \in \mathcal{C}_1$ for which there exists a codeword $u_{2\oplus3}^n \in (\lambda_2 \oplus \lambda_3)$ such that $(v_1^n, u_{2\oplus3}^n, Y_1^n)$ are jointly typical with respect to $p_{U_{21}\oplus U_3, V_1, Y_1}$. Here $(\lambda_2 \oplus \lambda_3) := \{v_2^n \oplus v_3^n : v_j^n \in \lambda_j^n : j = 2, 3\}$.[6] If all such codewords in $\mathcal{C}_1$ belong to a unique bin, the corresponding bin index is declared as the decoded message. Again following the technique similar to [14, Proof of Theorem 1], it can be proved, that if

$$KL_1 \leq H(V_1) - H(V_1|U_{21} \oplus U_{31}, Y_1) \quad (6)$$

$$KL_1 + ST_{j1} \leq \log q + H(V_1) - H(V_1, U_{21} \oplus U_{31}|Y_1) \quad (7)$$

for $j = 2, 3$, where $KL_1 := K_1 + L_1, ST_{j1} = S_{j1} + T_{j1}$, then probability of decoding error at decoders 1 falls exponentially.

[5]Just as Gelfand's ingenious coding technique for the Blackwell channel is a particular instance of Marton's binning, we believe strategies based on linear and nested linear codes such as [9] point to a general theory based on structured codes. We therefore emphasize the need to build on these examples.

[6]Recall that structure of λ_2, λ_3 contains cardinality of $(\lambda_2 \oplus \lambda_3)$. In particular $|(\lambda_2 \oplus \lambda_3)| \leq \exp\{\min\{S_{21} + T_{21}, S_{31} + T_{31}\}\}$

Since L_1, T_{21}, T_{31} denotes rate achievable by users $1, 2, 3$ respectively, eliminating K_1, S_{21}, S_{31} from the set of equations (1)-(7) yields an achievable rate region. The following definition and theorem provide a precise mathematical characterization of this achievable rate region.

Definition 1: Let $\mathbb{D}_1(W_{\underline{Y}|X}, \kappa, \tau)$ denote the collection of pmf's $p_{U_{21}U_{31}V_1X\underline{Y}}$ defined on $\mathcal{U}_{21} \times \mathcal{U}_{31} \times \mathcal{V}_1 \times \mathcal{X} \times \underline{\mathcal{Y}}$, where (i) $\mathcal{U}_{21} = \mathcal{U}_{31} = \mathcal{F}_q$ is the finite field of cardinality q, $\mathcal{V}_1$ is a finite set, (ii) $p_{\underline{Y}|XV_1\underline{U}} = p_{\underline{Y}|X} = W_{\underline{Y}|X}$, and (iii) $\mathbb{E}\{\kappa(X)\} \leq \tau$. For $p_{\underline{U}V_1X\underline{Y}} \in \mathbb{D}_1(W_{\underline{Y}|X}, \kappa, \tau)$, let $\beta_1(p_{\underline{U}V_1X\underline{Y}})$ be defined as the set of triples (R_1, R_2, R_3) that satisfy

$$
\begin{aligned}
&0 \leq R_1 \leq I(V_1; \mathscr{S}, Y_1), 0 \leq R_j \leq I(U_{j1}; Y_j) : j = 2, 3\\
&R_1 + R_j \leq H(V_1U_{j1}) - H(V_1, \mathscr{S}|Y_1) : j = 2, 3\\
&R_1 + R_j \leq H(V_1U_{j1}) - H(U_{j1}|Y_j) - H(V_1|\mathscr{S}, Y_1) : j = 2, 3\\
&R_2 + R_3 \leq I(U_{21}; Y_2) + I(U_{31}; Y_3) - I(U_{21}; U_{31}),\\
&\sum_{k=1}^{3} R_k \leq H(U_{21}U_{31}V_1) - H(V_1, \mathscr{S}|Y_1) - \max\left\{\begin{smallmatrix} H(U_{21}|Y_2)\\ H(U_{31}|Y_3)\end{smallmatrix}\right\}\\
&\sum_{k=1}^{3} R_k \leq H(U_{21}U_{31}V_1) - H(V_1|\mathscr{S}, Y_1) - \sum_{k=2}^{3} H(U_{k1}|Y_k)\\
&R_1 + \sum_{k=1}^{3} R_k \leq H(V_1) + H(U_{21}U_{31}V_1) - 2H(V_1, \mathscr{S}|Y_1)
\end{aligned}
$$

where $\mathscr{S} := U_{21} \oplus U_{31}$. Define

$$
\beta_1(W_{\underline{Y}|X}, \kappa, \tau) = \text{cocl}\left(\bigcup_{\substack{p_{\underline{U}V_1X\underline{Y}}\\ \in \mathbb{D}_1(W_{\underline{Y}|X}, \kappa, \tau)}} \beta_1(p_{\underline{U}V_1X\underline{Y}})\right).
$$

Theorem 2: For a 3-DBC $(\mathcal{X}, \underline{\mathcal{Y}}, W_{\underline{Y}|X}, \kappa)$, $\beta_1(W_{\underline{Y}|X}, \kappa, \tau) \subseteq \mathbb{C}(W_{\underline{Y}|X}, \kappa, \tau)$.

We refer the reader to [13] for an outline of the proof. The key elements of the proof is the interplay of joint typical encoding and decoding with correlated codebooks.[7] Indeed, codebooks being cosets of a common linear code are correlated and moreover, it's codewords are correlated. The analysis of error events contain several new elements.

For example 1, if $\tau * \delta_1 \leq \min\{\delta_2, \delta_3\}$, then $(h_b(\tau * \delta_1) - h_b(\delta_1), 1 - h_b(\delta_2), 1 - h_b(\delta_3)) \in \beta_1(\tau)$. Indeed, it can be verified that if $\tau * \delta_1 \leq \min\{\delta_2, \delta_3\}$, then $(h_b(\tau * \delta_1) - h_b(\delta_1), 1 - h_b(\delta_2), 1 - h_b(\delta_3)) \in \beta_1(p_{\underline{U}V_1X\underline{Y}})$, where $p_{\underline{U}V_1X} = p_{V_1}p_{U_{21}}p_{U_{31}}1_{\{X_1=V_1\}}1_{\{X_2=U_{21}\}}1_{\{X_3=U_{31}\}}$, $p_{U_{21}}(1) = p_{U_{31}}(1) = \frac{1}{2}$ and $p_{V_1}(1) = \tau$.

Let us revisit the coding technique proposed herein. Observe that (i) user 1 decodes a sum of the entire codewords/signals transmitted to users 2 and 3 and (ii) users 2 and 3 decode only their respective codewords. This technique may be enhanced in the following way. User 1 can decode the sum of *one component* of user 2 and 3 signals. In other words, we may include private codebooks for users 2 and 3. We refer the reader to [13, Section V.B] for a description of this enhancement for $3-$to-1 DBC. While, we omit this pedagogical step in here, the achievable rate region presented in the following section subsumes this enlarged achievable rate region for a general $3-$to-1 DBC.

VI. Achievable rate region for general 3-DBC based on coset codes

In section V-A, only user 1 decoded a bivariate interference component. Users 2 and 3 only decoded from their respective codebooks. This maybe sufficient if only user 1 is subjected to interference, as in $3-$to-1 BC. In general, each user would attempt to decode a bivariate interference component of the other user signals. Consider the following generalization.

User j splits it's message M_j into three $(M^U_{ji}, M^U_{jk}, M^V_j)$, where i, j, k are distinct indices in $\{1, 2, 3\}$. Let $\mathcal{U}_{ji} = \mathcal{F}_{q_i}, \mathcal{U}_{jk} = \mathcal{F}_{q_k}$ be finite fields and $\mathcal{V}_j$ an arbitrary finite set. Let $\lambda_{ji} \subseteq \mathcal{U}^n_{ji}$, $\lambda_{jk} \subseteq \mathcal{U}^n_{jk}$ denote cosets of linear codes $\overline{\lambda_{ji}}, \overline{\lambda_{jk}}$ of rates $S_{ji} + T_{ji}, S_{jk} + T_{jk}$ respectively. Note that cosets λ_{ji} and λ_{ki} are built over the same finite field $\mathcal{F}_{q_i}$. To enable contain range of sum of these cosets, the larger of λ_{ji}, λ_{ki} contains the other. Codewords of λ_{ji} and λ_{jk} are independently and uniformly partitioned into $\exp\{nT_{ji}\}$ and $\exp\{nT_{jk}\}$ bins respectively. A codebook $\mathcal{C}_j$ of rate $K_j + L_j$ is built over $\mathcal{V}_j$. $\mathcal{C}_j$ is similarly partitioned into $\exp\{nL_j\}$ bins.

M^U_{ji},M^U_{jk} and M^V_j index bins in λ_{ji}, λ_{jk} and $\mathcal{C}_j$ respectively. The encoder looks for a collection of 9 codewords from the indexed bins that are jointly typical with respect to a pmf $p_{\underline{UV}}$ defined on $\underline{\mathcal{U}} \times \underline{\mathcal{V}}$.[8] Following a second moment method similar to that employed in [14], it can be proved that the encoder finds at least one jointly typical collection if

$$
S_A + K_B \geq \sum_{a \in A} \log|\mathcal{U}_a| + \sum_{b \in B} H(V_b) - H(U_A, V_B) \quad (8)
$$

for all $A \subseteq \{12, 13, 21, 23, 31, 32\}, B \subseteq \{1, 2, 3\}$, where $S_A = \sum_{jk \in A} S_{jk}$, $K_B = \sum_{b \in B} K_b$, $U_A = (U_{jk} : jk \in A)$ and $V_B = (V_b : b \in B)$. Having chosen one such jointly typical collection, say $(\underline{U}^n, \underline{V}^n)$, the encoder generates X^n according to $\prod_{t=1}^n p_{X|\underline{UV}}(\cdot|\underline{U}^n, \underline{V}^n)$ and inputs the same.

Decoder j receives Y^n_j and looks for all triples $(u^n_{ji}, u^n_{jk}, v^n_j)$ of codewords in $\lambda_{ji} \times \lambda_{jk} \times \mathcal{C}_j$ such that there exists a $u^n_{ij \oplus kj} \in \lambda_{ij} \oplus \lambda_{kj}$ such that $(u^n_{ij \oplus kj}, u^n_{ji}, u^n_{jk}, v^n_j, Y^n_j)$ is jointly typical with respect to $p_{U_{ij} \oplus U_{kj}, U_{ji}, U_{jk}, V_j, Y_j}$. If all such triples are in a unique triple of bins, the corresponding triple of bin indices is declared as decoded message of user j. Else an error is declared. Decoding is successful if

$$
\begin{aligned}
&ST_{A_j} \leq \mathcal{A}_j - H(U_A|U_{A^c}, \mathscr{S}_j, V_j, Y_j)\\
&ST_{A_j} + ST_{ij} \leq \mathcal{A}_j + \theta_j - H(U_A, \mathscr{S}_j|U_{A^c}, V_j, Y_j)\\
&ST_{A_j} + ST_{kj} \leq \mathcal{A}_j + \theta_j - H(U_A, \mathscr{S}_j|U_{A^c}, V_j, Y_j)\\
&ST_{A_j} + KL_j \leq \mathcal{A}_j + H(V_j) - H(U_A, V_j|U_{A^c}, \mathscr{S}_j, Y_j)\\
&ST_{A_j} + KL_j + ST_{ij} \leq \mathcal{A}_j + \theta_j + H(V_j) - H(U_A, V_j, \mathscr{S}_j|U_{A^c}, Y_j)\\
&ST_{A_j} + KL_j + ST_{kj} \leq \mathcal{A}_j + \theta_j + H(V_j) - H(U_A, V_j, \mathscr{S}_j|U_{A^c}, Y_j)
\end{aligned} \quad (9)
$$

[7] While particular decoding rules such as syndrome decoding of linear codes can achieve capacity of particular channels such as binary symmetric, we will need to employ typical decoding to achieve capacity of arbitrary channels.

[8] $\underline{U}$ abbreviates $U_{12}U_{13}U_{21}U_{23}U_{31}U_{32}$.

where $\theta_j = \log_2 q_j$, $\mathcal{A}_j = \sum_{a\in A_j} \log|\mathcal{U}_a|$, $\mathscr{S}_j = U_{ij} \oplus U_{kj}$ for every $A_j \subseteq \{ji, jk\}$ with distinct indices i, j, k in $\{1, 2, 3\}$, $ST_{A_j} := S_{A_j} + T_{A_j}$, $S_{A_j} = \sum_{a\in A_j} S_a$, $T_{A_j} = \sum_{a\in A_j} T_a$, $ST_{ij} := S_{ij} + T_{ij}$, $ST_{kj} = S_{kj} + T_{kj}$, $KL_j = K_j + L_j$. Recognize that user j's rate $R_j = T_{ji} + T_{jk} + L_j$. We are now equipped to state an achievable rate region for the general 3-DBC using nested coset codes.

Definition 2: Let $\mathbb{D}_f(W_{\underline{Y}|X}, \kappa, \tau)$ denote the collection of probability mass functions $p_{\underline{U}\underline{V}X\underline{Y}}$ defined on $\underline{\mathcal{U}} \times \underline{\mathcal{V}} \times \mathcal{X} \times \underline{\mathcal{Y}}$, where $\underline{U} := (U_{12}, U_{13}, U_{21}, U_{23}, U_{31}, U_{32})$, $\underline{V} := (V_1, V_2, V_3)$, $\underline{\mathcal{U}} := \mathcal{U}_{12} \times \mathcal{U}_{13} \times \mathcal{U}_{21} \times \mathcal{U}_{23} \times \mathcal{U}_{31} \times \mathcal{U}_{32}$, $\underline{\mathcal{V}} := \mathcal{V}_1 \times \mathcal{V}_2 \times \mathcal{V}_3$, $\mathcal{U}_{ij} = \mathcal{F}_{q_j}$, the finite field of cardinality q_j for each $1 \le i, j \le 3$, $\mathcal{U}_i$ is an arbitrary finite set such that (i) $p_{\underline{Y}|X\underline{V}\underline{U}} = p_{\underline{Y}|X} = W_{\underline{Y}|X}$, (ii) $\mathbb{E}\{\kappa(X)\} \le \tau$.

For $p_{\underline{U}\underline{V}X\underline{Y}} \in \mathbb{D}_f(W_{\underline{Y}|X}, \kappa, \tau)$, let $\beta_f(p_{\underline{U}\underline{V}X\underline{Y}})$ is defined as the set of rate triples $(R_1, R_2, R_3) \in [0, \infty]^3$ for which there exists nonnegative numbers $S_{ij} : ij \in \{12, 13, 21, 23, 31, 32\}$, $T_{jk} : jk \in \{12, 13, 21, 23, 31, 32\}$, $K_j : j\{1, 2, 3\}$, $L_j : \{1, 2, 3\}$ that satisfy (8)-(9) and $R_1 = T_{12} + T_{13} + L_1, R_2 = T_{21} + T_{23} + L_2, R_3 = T_{31} + T_{32} + L_3$. Let

$$\beta_f(W_{\underline{Y}|X}, \kappa, \tau) = \mathrm{cocl}\left(\bigcup_{\substack{p_{\underline{U}\underline{V}X\underline{Y}} \in \\ \mathbb{D}_f(W_{\underline{Y}|X}, \kappa, \tau)}} \beta_f(p_{\underline{U}\underline{V}X\underline{Y}}) \right).$$

Theorem 3: For 3-DBC $(\mathcal{X}, \underline{\mathcal{Y}}, W_{\underline{Y}|X}, \kappa)$, $\beta_f(W_{\underline{Y}|X}, \kappa, \tau)$ is achievable, i.e., $\beta_f(W_{\underline{Y}|X}, \kappa, \tau) \subseteq \mathbb{C}(W_{\underline{Y}|X}, \kappa, \tau)$.

VII. Enlarging Marton's rate region using coset codes

The natural question that arises is whether the achievable rate region using coset codes contains Marton's rate region. It is our belief that coding techniques based on structured codes do not substitute their counterparts based on traditional unstructured independent codes, but enhance the same. Indeed, the technique proposed in [9] is strictly inferior to unstructured coding technique for certain source distributions.[9]

We therefore follow the approach of Ahlswede and Han [15, Section VI] to build upon Marton's rate region by gluing to it the coding technique proposed herein.[10] Indeed, a description of the resulting rate region is quite involved and we spare the reader of these details. The resulting coding technique will involve each user decode a univariate component of every other user's transmission particularly set apart for it, and furthermore decodes a bivariate component of the other two user's transmissions.[11] A mathematical characterization of the resulting achievable rate region can be derived using standard techniques. The reader is referred to [16, Section VII] for an illustration. For now, we conclude by stating that the resulting achievable rate region contains and strictly enlarges Marton's rate region for the general 3-DBC.

VIII. Concluding Remarks

Structured codes enable decoding of bivariate interference component more efficiently by containing range of the bivariate function. In this article, we only exploited this property of the simplest ensemble of structured codes - coset codes - that contain the interference to an affine space, leaving sufficient room for generalization using other algebraic structures. We therefore envision an achievable rate region involving a union over all algebraic objects pertaining to the several bivariate functions.

Acknowledgment

This work was supported by NSF grants CCF-0915619 and CCF-1116021.

References

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

[2] T. M. Cover, "Broadcast channels," *IEEE Trans. Inform. Theory*, vol. IT-18, no. 1, pp. 2–14, Jan. 1972.

[3] P. P. Bergmans, "Random coding theorems for the broadcast channels with degraded components," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 197–207, Mar. 1973.

[4] C. Nair and A. El Gamal, "The capacity region of a class of three-receiver broadcast channels with degraded message sets," *IEEE Trans. Inform. Theory*, vol. 55, no. 10, pp. 4479 –4493, oct. 2009.

[5] A. Gohari and V. Anantharam, "Evaluation of Marton's inner bound for the general broadcast channel," *IEEE Trans. Inform. Theory*, vol. 58, no. 2, pp. 608 –619, Feb. 2012.

[6] C. Nair and A. El Gamal, "An outer bound to the capacity region of the broadcast channel," *Information Theory, IEEE Transactions on*, vol. 53, no. 1, pp. 350–355, 2007.

[7] H. Weingarten, Y. Steinberg, and S. Shamai(Shitz), "The capacity region of the Gaussian MIMO broadcast channel," *IEEE Trans. Inform. Theory*, vol. 52, pp. 3936–3964, September 2006.

[8] M. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. 29, pp. 439–441, May 1983.

[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] D. Krithivasan and S. Pradhan, "Distributed source coding using abelian group codes: A new achievable rate-distortion region," *IEEE Trans. Inform. Theory*, vol. 57, no. 3, pp. 1495 –1519, march 2011.

[11] 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.

[12] A. Padakandla, A. Sahebi, and S. Pradhan, "A new achievable rate region for the 3-user discrete memoryless interference channel," in *2012 IEEE ISIT Proceedings*, july 2012, pp. 2256 –2260.

[13] A. Padakandla and S. Pradhan, "A new coding theorem for three user discrete memoryless broadcast channel," available at `http://arxiv.org/abs/1207.3146`.

[14] ——, "Nested linear codes achieve Marton's inner bound for general broadcast channels," in *2011 IEEE ISIT Proceedings*, 31 2011-aug. 5 2011, pp. 1554 –1558.

[15] 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.

[16] A. Padakandla and S. Pradhan, "Achievable rate region based on coset codes for multiple access channel with states," available at `http://arxiv.org/abs/1301.5655`.

[9] If X and Y are the distributed binary sources whose modulo-2 sum is to be reconstructed at the decoder, then Körner and Marton technique is strictly suboptimal if $H(X \oplus Y) > \frac{H(X,Y)}{2}$.

[10] This is akin to the use of superposition and binning in Marton's coding.

[11] An informed and inquisitive reader may begin to see a relationship emerge between the several layers of coding and common parts of a collection of random variables. Please refer to [13, Section VIII] for a discussion.