Homologous Codes for Multiple Access Channels

Pinar Sen and Young-Han Kim
Department of Electrical and Computer Engineering
University of California, San Diego
Email: {psen, yhk}@ucsd.edu

***Abstract*—Building on recent development by Padakandla and Pradhan, and by Lim, Feng, Pastore, Nazer, and Gastpar, this paper studies the potential of structured coding as a complete replacement for random coding in network information theory. The roles of two techniques used in nested coset coding to generate nonuniform codewords, namely, shaping and channel transformation, are clarified and illustrated via the simple example of the two-sender multiple access channel. While individually deficient, the optimal combination of shaping and channel transformation is shown to achieve the same performance as traditional random codes for this channel model, which opens up new possibilities of utilizing nested coset codes with the same generator matrix for a broader class of applications.**

I. Introduction

Random independently and identically distributed (i.i.d.) code ensembles play a fundamental role in network information theory, with most existing coding schemes built on them; see, for example, [1]. As shown by the classical example by Körner and Marton [2], however, using the same code at multiple users can achieve strictly better performance for some communication problems. Recent studies illustrate the benefit of such *structured coding* for computing linear combinations in [3]–[5], for the interference channels in [6]–[9], and for the multiple access channels with state information in [10]. Consequently, there has been a flurry of research activities on structured coding in network information theory, facilitated in part by several standalone workshops and tutorials at major conferences by leading researchers.

Most of the existing results are based on lattice codes or linear codes on finite alphabets. Recently, Padakandla and Pradhan [10] brought a new dimension to the arsenal of structured coding by developing nested coset codes. In their nested coset coding scheme, a coset code of a rate higher than the target is first generated randomly. A codeword of a desired property (such as type or joint type) is then selected from a subset (a coset of a subcode). This construction is reminiscent of the multicoding scheme in Gelfand–Pinsker coding for channels with state and Marton coding for broadcast channels. But in a sense, nested coset coding is more fundamental in that the scheme at its core is relevant even for single-user communication. By a careful combination of individual and common parts of coset codes, the proposed coding scheme in [10] achieves rates for multiple access channels (MACs) with state beyond what can be achieved by existing random or structured coding schemes. The analysis of the scheme is performed by packing and covering lemmas developed again in [10] that parallel such lemmas for random coding in [1].

Recently, structured coding based on random nested coset codes was further streamlined by Lim, Feng, Pastore, Nazer, and Gastpar [5]. With the primary motivation of communicating linear combinations of codewords over a multiple access channel (as in compute–forward [3]), they augmented the original nested coset coding scheme in [10] by the channel transformation technique by Gallager [11, Sec. 6.2] and developed new analysis tools when multiple senders use nested coset codes with a common generator matrix. The resulting achievable rate region, when adapted to the Gaussian case, improves upon the previous result for compute–forward [3].

In both [10] and [5], however, structured coding of nested coset codes is reserved for rather niche communication scenarios of adapting multiple codewords to a common channel state or computing sums of codewords, and even in these limited cases, as a complement to random coding. The coding scheme in [10] uses superposition of codewords with individual and common generator matrices. A similar coding scheme in [9] for three-user interference channels again uses a combination of random coding (for decoding messages) and structured coding (for decoding functions) of nested coset codes, this time with a more explicit superposition coding architecture. There is also some indication that the benefit of computation can be realized to the full extend only in special cases for which desired linear combinations and channel structures are matched [12]. In the same vein, the aforementioned rate region for computing in [5] turns out to be strictly smaller than the typical capacity region, when computation is specialized to communication. Apparently, structured coding, even based on the promising new technique of nested coset codes, can only play a complementary role to random coding.

This paper aims to show that at least for simple communication networks, the opposite is true, and that structured coding can completely replace random coding. In particular, we show that nested coset codes of the same generator matrix (termed *homologous codes*), which was thought to be good only for recovering linear combinations, can achieve the same rates as random coding for the task of communicating individual codewords over MACs. For simplicity of exposition, we focus on two-sender MACs, but the same technique can be generalized to more complicated channel models. Our finding relies on the identification of *shaping* and *channel*

978-1-5090-4096-4/17/$31.00 ©2017 IEEE

transformation, both of which are used to improve upon conventional coset codes by allowing nonuniform codewords, as key components to supplant random coding. Achievable rates of each technique are characterized, which, inter alia, tightens the previous analysis in [5].

The rest of the paper is organized as follows. Section II defines nested coset codes and homologous codes. Section III discusses the running examples of binary adder and binary erasure multiple access channels. The main results are presented in Section IV.

We adapt the notation in [1], [13]. The set of integers $\{1, 2, \ldots, n\}$ is denoted by $[1 : n]$. For a length-n sequence $x^n \in \mathcal{X}^n$, we define its type as $\pi(x|x^n) = |\{i\colon x_i = x\}|/n$ for $x \in \mathcal{X}$. For $\epsilon \in (0, 1)$, $\mathcal{T}_\epsilon^{(n)}(X) = \{x^n\colon |p(x) - \pi(x|x^n)| \le \epsilon p(x),\ x \in \mathcal{X}\}$. A length-$n$ vector of all zeros (ones) is denoted by $\mathbf{0}_n$ ($\mathbf{1}_n$), where the subscript is omitted when it is clear in the context. An $m \times n$ matrix of all zeros is denoted by $O_{m\times n}$. The $n \times n$ identity matrix is denoted by I_n.

II. Homologous Codes

A *nested coset* code was first proposed in [10]. Defined on a finite field $\mathbb{F}_q$ of order q, an $(n, k, \hat{k})$ nested coset code is defined by a $(k + \hat{k}) \times n$ generator matrix G, a length-n dithering vector (coset leader) d^n, and a shaping function $l : \mathbb{F}_q^k \to \mathbb{F}_q^{\hat{k}}$. Let

$$x^n(m, l) = [m\ \ l]\, G + d^n, \quad m \in \mathbb{F}_q^k,\ l \in \mathbb{F}_q^{\hat{k}}. \tag{1}$$

Each message $m \in \mathbb{F}_q^k$ is then assigned a codeword $x^n(m, l(m))$, where $l(m)$ is the specified shaping function. A standard *coset* code can be seen as a special case of a nested coset code with $\hat{k} = 0$ (no shaping). Specializing even further, we recover a *linear code* as a nested coset code with $\hat{k} = 0$ and $d^n = \mathbf{0}_n$.

Introduced in [10], a *random* nested coset code is an ensemble of nested coset codes that are constructed via a random generator matrix G and a random dithering vector D^n to emulate the behavior of a random (nonlinear) code ensemble drawn from a specified pmf $p(x)$ on $\mathbb{F}_q$. Each element of G and D^n is i.i.d. $\mathrm{Unif}(\mathbb{F}_q)$. Given the realizations of G and D^n, $x^n(m, l)$ for $m \in \mathbb{F}_q^k,\ l \in \mathbb{F}_q^{\hat{k}}$ is defined as in (1). For shaping, we use the joint typicality encoding in [10]; see [14] for a similar technique. Let $p(x)$ be the desired pmf and $\epsilon' > 0$. For each message $m \in \mathbb{F}_q^k$, choose an $l \in \mathbb{F}_q^{\hat{k}}$ such that $x^n(m, l) \in \mathcal{T}_{\epsilon'}^n(X)$. If there are more than one such l, choose one of them at random; if there is none, choose one in $\mathbb{F}_q^{\hat{k}}$.

As shown in [5], [10], random nested coset code ensembles can achieve the capacity of a discrete memoryless channel $p(y|x)$. When the input alphabet $\mathcal{X}$ is not isomorphic to a finite field, the channel can be transformed into a virtual channel $p(y|u)$ with equal capacity via an appropriately chosen auxiliary input U and symbol-by-symbol mapping $X = \varphi(U)$ [11]. This result can be extended to the Gaussian channel [5] (via a quantization argument) and to multiple access channels [10]. In particular, for the 2-sender discrete memoryless (DM) MAC $p(y|x_1, x_2)$ and input pmfs $p(x_1)$ and $p(x_2)$, each sender can use a random nested coset code ensemble (with individual generator matrices G_1 and G_2) to achieve the pentagonal region $\mathscr{R}_{\mathrm{MAC}}(X_1,X_2)$ characterized by

$$\begin{aligned} R_1 &\le I(X_1; Y|X_2), \\ R_2 &\le I(X_2; Y|X_1), \\ R_1 + R_2 &\le I(X_1, X_2; Y). \end{aligned} \tag{2}$$

Thus, heterologous codes (= with different generators) can emulate the performance of typically nonlinear random code ensembles for MACs. (In fact, by controlling the structure of G_1 and G_2 more carefully, they can achieve larger rates than random codes for channels with state [10]).

We now consider nested coset codes with closer structural relationship. A collection of $(n, k_j, \hat{k}_j)$ nested coset codes, $j = 1, 2, \ldots, N$, is called as *homologous codes* if they share a common generator matrix G (but have individual dithering sequences and shaping functions). Since $k_j + \hat{k}_j$ may differ, we use zero padding, i.e., instead of (1), we have

$$x_j^n(m_j, l_j) = [m_j\ l_j\ \mathbf{0}_{\kappa-(k_j+\hat{k}_j)}]G + d_j^n,$$

where $\kappa = \max_j(k_j + \hat{k}_j)$. In biological analogy, even though homologous codes are constructed from the same generator matrix, the actual "shape" of the codes can be quite different due to individual shaping functions. *Random* homologous codes are generated by a common generator matrix G and dithering vectors $D_1^n, D_2^n, \ldots, D_N^n$ of i.i.d. $\mathrm{Unif}(\mathbb{F}_q)$ entries, and shaping functions that find an l_j such that

$$x_j^n(m_j, l_j) \in \mathcal{T}_{\epsilon'}^n(X_j), \quad j = 1, 2, \ldots, N,$$

for given pmfs $p(x_1), p(x_2), \ldots, p(x_N)$.

Due to the use of a common generator matrix, homologous codes can achieve high rates when the goal of communication is to recover linear combination of codewords. For a 2-sender DM-MAC, an achievable rate region is characterized in [5] for recovering linear combinations of codewords from random homologous code ensembles. When recovering both messages, however, this achievable rate region is in general smaller than the pentagonal region in (2). This raises the question of whether random homologous codes are useful only for communicating the sum of the messages and fundamentally deficient compared to heterologous ones in communicating the messages themselves.

III. Motivating Examples

We present two simple examples that illustrate the performance of homologous codes and motivate our main result.

Example 1 (Binary adder MAC): Let $Y = X_1 \oplus X_2$, where $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y} = \{0, 1\}$ and the addition operation $\oplus$ is over $\mathbb{F}_2$. The capacity region of this channel is achieved by random coding with i.i.d. $\mathrm{Bern}(1/2)$ inputs X_1 and X_2, and is depicted in Fig. 1a. No linear or coset codes of the same generator matrix, however, can achieve this region. For example, if $R_1 = R_2$, the message pair (m_1, m_2) results in the same output as the message pair (m_2, m_1). Following a similar argument, it can be shown that coset codes of the same generator matrix

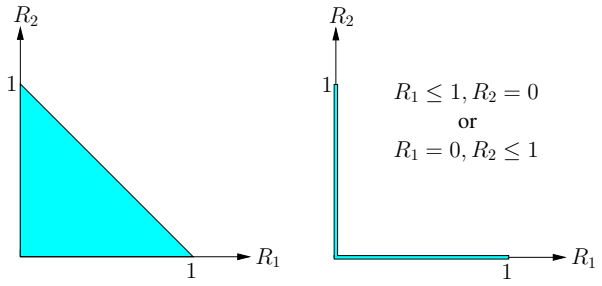

Fig. 1: (a) The capacity region and (b) an achievable rate region of the binary adder MAC.

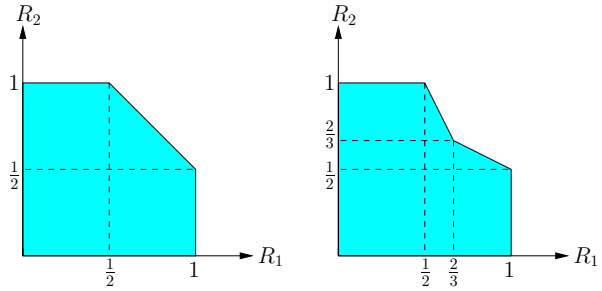

Fig. 2: (a) The capacity region and (b) an achievable rate region of the binary erasure MAC.

can only achieve the rate region depicted in Fig. 1b. By using *nested* coset codes with proper shaping, however, the capacity region can be achieved. Suppose that $m_1, m_2, l_1, l_2 \in \mathbb{F}_2^{n/2}$ and consider

$$\begin{aligned} x_1^n(m_1, l_1(m_1)) &= [m_1 \; l_1(m_1)] = [m_1 \;\; \mathbf{0} \;], \\ x_2^n(m_2, l_2(m_2)) &= [m_2 \; l_2(m_2)] = [m_2 \; m_2]. \end{aligned} \tag{3}$$

This pair of $(n, n/2, 0)$ and $(n, n/2, n/2)$ homologous code with the same generator matrix $I_{n\times n}$ and trivial shaping functions can communicate m_1 and m_2 without any error. It is easy to generalize this construction to asymmetric rates.

The next example has the underlying channel structure that is not fully compatible with the algebraic structure of codes.

Example 2 (Binary erasure MAC): Let $Y = X_1 + X_2$, where $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$, $\mathcal{Y} = \{0, 1, 2\}$, and the addition operation $+$ is over $\mathbb{R}$. The capacity region of the channel is achieved by random coding with i.i.d. $\mathrm{Bern}(1/2)$ inputs X_1 and X_2, and is depicted in Fig. 2a. In contrast, it can be shown that no pair of coset codes with the same generator matrix can achieve the rate pair $(1/2 + \epsilon, 1/2 + \epsilon)$ for $\epsilon > 0$. This limitation of coset codes can be once again overcome by nested coset codes. Let $A_{k\times n}$ be a generator matrix of a linear code of rate $R = k/n < 1/2$ for the *point-to-point* binary erasure channel of erasure probability $1/2$. Then, the following pair of linear codes (with zero padding) can achieve the rate pair $(R, 1)$: $x_1^n(m_1) = [m_1 \, \mathbf{0}_{n(1-R)}]\, B$ and $x_2^n(m_2) = m_2\, B$, where $B = \left[A^T \; (A^\perp)^T\right]^T$, A^T is the transpose of matrix A, and $A^\perp$ is an $(n-k)\times n$ matrix whose rows are orthogonal to the rows of A. We now construct homologous $(2n, n+k, 0)$ and $(2n, n+k, n-k)$ nested coset codes with the generator matrix

$$G = \left[\begin{array}{c|c} B & O_{n\times n} \\ \hline O_{k\times n} & B \\ A^\perp & \end{array}\right]. \tag{4}$$

Then it can be shown that the first and second halves of codewords are reliably communicated at rates $(R, 1)$ and $(1, R)$, which combined together can be arbitrarily close to $(3/4, 3/4)$. A similar argument can be extended to the entire capacity region.

The constructions of nested coset codes in (3) and (4) emulate time division and time sharing, respectively, in disguise. Consequently, these codes do not scale to more complicated problems (such as interference channels) in a satisfactory manner. As discussed shortly, however, most (random) homologous codes are sufficient to achieve the capacity region, provided that they are constructed according to appropriate distributions.

IV. Achievable Rate Regions of Random Homologous Codes

We now investigate the performance of random homologous code ensembles defined in Section II. Following the standard terminology in network information theory, we say that a rate pair (R_1, R_2) is *achievable* if there exists a sequence of codes of a fixed rate pair (R_1, R_2) indexed by the block length n such that the average probability of error $P_e^{(n)}$ tends to 0 as $n \to \infty$. Specializing further, we say that (R_1, R_2) is *achievable by random homologous codes* if there exists a sequence of random $(n, nR_1, n\hat{R}_1)$ and $(n, nR_2, n\hat{R}_2)$ homologous code ensembles (cf. Section II) such that $\lim_{n\to\infty} \mathsf{E}[P_e^{(n)}] = 0$, where the expectation is taken with respect to the randomness in the common generator matrix and individual dithering sequences.

We take a gradual approach to presenting the main result and first discuss the key technical ingredients of the proof one by one. Throughout information measures are in log base q.

A. Shaping

Symbols in random coset codes are uniformly drawn over $\mathbb{F}_q$. By proper shaping via joint typically encoding, random homologous code ensembles emulate the statistical behavior of a random code ensemble while maintaining a common algebraic structure across users.

We describe the achievable rate region for the finite field input DM-MAC $p(y|x_1, x_2)$, $\mathcal{X}_1 = \mathcal{X}_2 = \mathbb{F}_q$, by random homologous code ensembles. For given pmfs $p(x_1)$ and $p(x_2)$, we refer to the rate region in (2) as $\mathscr{R}_{\mathrm{MAC}}(X_1, X_2)$, and define $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$ as the set of rate pairs (R_1, R_2) such that

$$R_1 < \max\{I(X_1; Y),\, H(X_1) - H(X_2) + I(X_2; Y)\}, \tag{5}$$

or

$$R_2 < \max\{I(X_2; Y),\, H(X_2) - H(X_1) + I(X_1; Y)\}. \tag{6}$$

Proposition 1: A rate pair (R_1, R_2) is achievable for the finite field input DM-MAC $p(y|x_1, x_2)$ by random homologous codes if

$$(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(X_1, X_2) \cap \mathscr{R}_{\text{L}}(X_1, X_2)$$

for some input pmfs $p(x_1)$ and $p(x_2)$.

Proof sketch: Our proof steps follow [5, Sec. VI] essentially line by line, except the analysis of one error event. Fix $p(x_1)$ and $p(x_2)$. Let $\epsilon' > 0$. We use random homologous code ensembles via typicality encoding (cf. Section II) constructed with the pmfs $p(x_1)$ and $p(x_2)$, and parameter ϵ'. The decoder finds a unique pair of $(\hat{m}_1, \hat{m}_2)$ such that $(x_1^n(\hat{m}_1, l_1), x_2^n(\hat{m}_2, l_2), y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y)$ for some (l_1, l_2), where $\epsilon > \epsilon'$. Assume that $(M_1, M_2) = (\mathbf{0}, \mathbf{0})$ is transmitted and $(L_1, L_2) = (\mathbf{0}, \mathbf{0})$ is chosen by the shaping functions. We bound the probability of error $\mathsf{P}(\mathcal{E})$ averaged over codebooks. As in [5], the decoder makes an error only if one or more of the following occur:

$$\begin{aligned}
\mathcal{E}_1 &= \{X_j^n(\mathbf{0}, l_j) \notin \mathcal{T}_{\epsilon'}^{(n)} \text{ for all } l_j,\ j = 1 \text{ or } 2\},\\
\mathcal{E}_2 &= \{(X_1^n(\mathbf{0}, \mathbf{0}), X_2^n(\mathbf{0}, \mathbf{0}), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\},\\
\mathcal{E}_{34} &= \{(X_1^n(m_1, l_1), X_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some}\\
&\quad (m_1, l_1) \neq (\mathbf{0}, \mathbf{0}) \text{ or some } (m_2, l_2) \neq (\mathbf{0}, \mathbf{0}) \text{ but not both}\},\\
\mathcal{E}_5 &= \{(X_1^n(m_1, l_1), X_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some}\\
&\quad (m_1, l_1) \neq (\mathbf{0}, \mathbf{0}), (m_2, l_2) \neq (\mathbf{0}, \mathbf{0}) \text{ linearly independent}\},\\
\mathcal{E}_6 &= \{(X_1^n(m_1, l_1), X_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some}\\
&\quad (m_1, l_1) \neq (\mathbf{0}, \mathbf{0}), (m_2, l_2) \neq (\mathbf{0}, \mathbf{0}) \text{ linearly dependent}\}.
\end{aligned}$$

Thus, $\mathsf{P}(\mathcal{E}) \le \mathsf{P}(\mathcal{E}_1) + \sum_{k \neq 1} \mathsf{P}(\mathcal{E}_k \cap \mathcal{E}_1^c)$. By [5], the first four terms can be controlled by appropriate constraints on the rates. Improving upon [5], the last term is controlled by the following rate constraints, the proof of which is omitted.

Lemma 1: The probability $P(\mathcal{E}_6 \cap \mathcal{E}_1^c)$ can be bounded by two different expressions:

$$\begin{aligned}
\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) &\le (q-1) q^{n(\hat{R}_1 + \hat{R}_2 + \min\{R_1 + \hat{R}_1, R_2 + \hat{R}_2, \})}\\
&\quad \cdot q^{n(H(X_1) + H(X_2) + H(X_2|Y) - 3 + \delta(\epsilon))},\\
\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) &\le (q-1) q^{n(\hat{R}_1 + \hat{R}_2 + \min\{R_1 + \hat{R}_1, R_2 + \hat{R}_2, \})}\\
&\quad \cdot q^{n(H(X_1) + H(X_2) + H(X_1|Y) - 3 + \delta(\epsilon))}.
\end{aligned}$$

Combining Lemma 1 with the rate constraints in [5], we have the achievability of the rate pairs (R_1, R_2) such that $R_1 < I(X_1; Y|X_2)$, $R_2 < I(X_2; Y|X_1)$, $R_1 + R_2 < I(X_1, X_2; Y)$, and

$$\begin{aligned}
&\min\{R_1 - H(X_1),\ R_2 - H(X_2)\}\\
&\qquad < -\min\{H(X_1|Y),\ H(X_2|Y)\},
\end{aligned}$$

which can be shown to be equivalent to the stated condition in the proposition. ∎

When specialized to the binary adder MAC, the achievable rate region in Proposition 1 (over all input pmfs) coincides with the capacity region. For the binary erasure MAC, (5) and (6) are reduced to $R_1 < I(X_1; Y)$ and $R_2 < I(X_2; Y)$, respectively. Hence, the rate region can be computed easily and shown to be *strictly smaller* than the capacity region, as sketched in Fig. 2b. In particular, the largest achievable symmetric rate is $2/3$.

B. Channel Transformation

Instead of using a nested coset code and choosing an appropriate shaping function, there is a simpler way of achieving the performance of nonuniformly distributed codes. Following the basic idea in [11, Sec. 6.2], we can simply transform the channel $p(y|x_1, x_2)$ into a *virtual channel* with finite field inputs

$$p(y|u_1, u_2) = p_{Y|X_1, X_2}(y|\varphi_1(u_1), \varphi_2(u_2)) \tag{7}$$

for some symbol-by-symbol mappings $\varphi_1 : \mathbb{F}_q \to \mathcal{X}_1$ and $\varphi_2 : \mathbb{F}_q \to \mathcal{X}_2$, as illustrated in Fig. 3. Note that this transformation can be applied to any DM-MAC $p(y|x_1, x_2)$ of arbitrary (not necessarily finite field) input alphabets.

We now consider a pair of random coset codes of the same generator matrix for the virtual channel, which is equivalent to random homologous codes with $\hat{R}_1 = \hat{R}_2 = 0$. Following the similar (yet simpler) steps in the proof of achievability in Proposition 1, we can establish the following.

Proposition 2: A rate pair (R_1, R_2) is achievable for a DM-MAC $p(y|x_1, x_2)$ by random coset codes in $\mathbb{F}_q$ with the same generator matrix, if

$$(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(U_1, U_2) \cap \mathscr{R}_{\text{L}}(U_1, U_2),$$

where $\mathscr{R}_{\text{MAC}}(U_1, U_2)$ is defined as in (2) for the virtual channel $p(y|u_1, u_2)$ in (7) and for the inputs U_1 and U_2 drawn independently according to $\text{Unif}(\mathbb{F}_q)$, and $\mathscr{R}_{\text{L}}(U_1, U_2)$ is the set of (R_1, R_2) such that

$$\min(R_1, R_2) < \max\{I(U_1; Y),\ I(U_2; Y)\}. \tag{8}$$

Note that (8) is equivalent to (5) and (6) since U_1 and U_2 are uniform on $\mathbb{F}_q$. The same region can be achieved by random *linear* codes as well.

Proposition 2 was stated for a fixed channel transformation specified by a given pair of symbol-by-symbol mappings $\varphi(u_1)$ and $\varphi(u_2)$ on a finite field $\mathbb{F}_q$. We now consider all such channel transformations, which results in a simpler achievable rate region.

Corollary 1: A rate pair (R_1, R_2) is achievable for the DM-MAC $p(y|x_1, x_2)$ by random coset codes in some finite field with the same generator matrix, if

$$(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(X_1, X_2) \cap \mathscr{R}'_{\text{L}}(X_1, X_2)$$

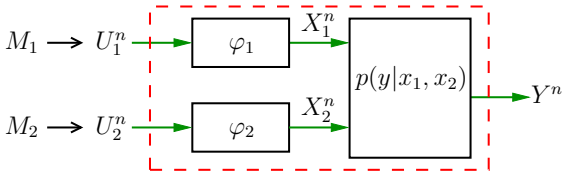

Fig. 3: The transformed DM-MAC $p(y|u_1, u_2)$ with virtual inputs U_1 and U_2.

for some input pmfs $p(x_1)$ and $p(x_2)$, where $\mathscr{R}'_{\mathrm{L}}(X_1, X_2)$ is the set of (R_1, R_2) such that

$$\min(R_1, R_2) < \max\{I(X_1;Y),\, I(X_2;Y)\}. \tag{9}$$

Proof: First suppose that $p(x_1)$ and $p(x_2)$ are of the form

$$i/p^m \tag{10}$$

for some prime p and $i, m \in \mathbb{Z}^+$ for all x_1 and x_2. Then there exist $\varphi_1(u_1)$ and $\varphi_2(u_2)$ on $\mathbb{F}_q$ such that $X_j \stackrel{d}{=} \varphi_j(U_j)$ with $U_j \sim \mathrm{Unif}(\mathbb{F}_q)$, where $q = p^m$. Hence, we can transform the channel $p(y|x_1, x_2)$ into a virtual channel $p(y|u_1, u_2)$ and achieve the rate region in Proposition 2. Now, since $(U_1, U_2) \to (X_1, X_2) \to Y$ form a Markov chain and (U_1, X_1) and (U_2, X_2) are independent, $\mathscr{R}_{\mathrm{L}}(U_1, U_2)$ in Proposition 2 can be simplified as $\mathscr{R}'_{\mathrm{L}}(X_1, X_2)$. Finally, the earlier restrictions on the input pmfs can be removed since the set of pmfs of the form (10) is dense. This completes the proof. ■

For the binary adder MAC, the achievable rate region in the corollary can be shown to be equivalent to the capacity region. This does not contradict the fact that no coset code on the *binary field* can achieve a positive symmetric rate pair, since channel transformation allows the use of linear (or coset) codes over larger finite fields. For the binary erasure MAC, this channel transformation technique achieves the same rate region (Fig. 2b) as the shaping technique (Proposition 1), although $\mathscr{R}'_{\mathrm{L}}(X_1, X_2)$ is in general larger than $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$ for fixed pmfs $p(x_1)$ and $p(x_2)$.

C. Combination

As shown for the binary erasure MAC example, shaping (with homologous codes) and channel transformation (with coset codes of the same generator matrix) seemingly cannot achieve the capacity region. Channel transformation was combined with shaping in [5] to convert code alphabets from finite fields to general sets (even real numbers). In contrast, we utilize channel transformation mappings as optimization parameters and show that the optimal combination of these two techniques can achieve the pentagonal region $\mathscr{R}_{\mathrm{MAC}}(X_1, X_2)$ for any $p(x_1)$ and $p(x_2)$ while maintaining the inherent algebraic structure of the code. Consider the virtual channel in (7) and random homologous codes for this channel. Then, Proposition 1 implies the following.

Proposition 3: A rate pair (R_1, R_2) is achievable for the DM-MAC $p(y|x_1, x_2)$ by random homologous codes in $\mathbb{F}_q$, if

$$(R_1, R_2) \in \mathscr{R}_{\mathrm{MAC}}(X_1, X_2) \cap \mathscr{R}_{\mathrm{L}}(U_1, U_2, X_1, X_2)$$

for some $p(u_1)$ and $p(u_2)$ on $\mathbb{F}_q$ and some mappings $x_1 = \varphi_1(u_1)$ and $x_2 = \varphi_2(u_2)$, where $\mathscr{R}_{\mathrm{L}}(U_1, U_2, X_1, X_2)$ is the set of rate pairs (R_1, R_2) such that

$$R_1 < \max\left[I(X_1;Y), H(U_1) - H(U_2) + I(X_2;Y)\right]$$

or

$$R_2 < \max\left[H(U_2) - H(U_1) + I(X_1;Y), I(X_2;Y)\right].$$

We are now ready to state the main technical result of this paper, which follows from Proposiition 3 by optimizing over all channel transformations.

Theorem 4.1: A rate pair (R_1, R_2) is achievable for the DM-MAC $p(y|x_1, x_2)$ by random homologous codes in some finite field, if $(R_1, R_2) \in \mathscr{R}_{\mathrm{MAC}}(X_1, X_2)$ for some $p(x_1), p(x_2)$.

Proof: Our argument is similar to that of Corollary 1, except that the choice of channel transformation needs more care. First suppose that $p(x_1)$ and $p(x_2)$ are of the form (10). We consider random homologous codes over $\mathbb{F}_q$ with $q = p^{2m}$. Choose U_1 and φ_1 such that U_1 and $\varphi_1(U_1) \stackrel{d}{=} X_1$ are one-to-one on the support of U_1 (this is always possible since $q \geq p^m$). Also choose $U_2 \sim \mathrm{Unif}(\mathbb{F}_q)$ and φ_2 such that $\varphi_2(U_2) \stackrel{d}{=} X_2$ (this is possible due to the form of $p(x_2)$). Then

$$\begin{aligned} H(U_2) - H(U_1) &\geq \log p^m \\ &\geq H(X_2) \geq I(X_1, X_2; Y) - 2I(X_1; Y), \end{aligned}$$

which implies that $\mathscr{R}_{\mathrm{MAC}}(X_1, X_2) \subseteq \mathscr{R}_{\mathrm{L}}(U_1, U_2, X_1, X_2)$. Finally, the restrictions on the input pmfs can be removed again by the denseness argument. ■

Acknowledgments

The work in this paper was supported in part by the Electronics and Telecommunications Research Institute through Grant 17ZF1100 from the Korean Ministry of Science, ICT, and Future Planning.

References

[1] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge: Cambridge University Press, 2011.
[2] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 219–221, 1979.
[3] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.
[4] Y. Song and N. Devroye, "Lattice codes for the Gaussian relay channel: Decode-and-forward and compress-and-forward," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4927–4948, August 2013.
[5] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar, "A joint typicality approach to algebraic network information theory," *CoRR*, vol. abs/1606.09548, 2016.
[6] A. Padakandla, A. G. Sahebi, and S. S. Pradhan, "A new achievable rate region for the 3-user discrete memoryless interference channel," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2012, pp. 2256–2260.
[7] V. Ntranos, V. R. Cadambe, B. Nazer, and G. Caire, "Integer-forcing interference alignment," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2013, pp. 574–578.
[8] O. Ordentlich, U. Erez, and B. Nazer, "The approximate sum capacity of the symmetric Gaussian K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3450–3482, 2014.
[9] A. Padakandla, A. G. Sahebi, and S. S. Pradhan, "An achievable rate region for the three-user interference channel based on coset codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1250–1279, March 2016.
[10] A. Padakandla and S. S. Pradhan, "Achievable rate region based on coset codes for multiple access channel with states," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2013, pp. 2641–2645.
[11] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.
[12] N. Karamchandani, U. Niesen, and S. Diggavi, "Computation over mismatched channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 666–677, April 2013.
[13] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.
[14] T. Gariby and U. Erez, "On general lattice quantization noise," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2008, pp. 2717–2721.