How to Compute Modulo Prime-Power Sums

Mohsen Heidari
EECS Department
University of Michigan
Ann Arbor,USA
Email: mohsenhd@umich.edu

S. Sandeep Pradhan
EECS Department
University of Michigan
Ann Arbor,USA
Email: pradhanv@umich.edu

***Abstract*—The problem of computing modulo prime-power sums is investigated in distributed source coding as well as computation over Multiple-Access Channel (MAC). We build upon the previous group coding schemes and present a new multi-level group coding strategy. Using the new coding scheme, we derived achievable rates for both settings and show that strict improvements can be obtained.**

I. Introduction

EVER since the seminal paper by Korner and Marton in 1979, structured codes played a key role in the study of asymptotic performance of multi-terminal communications [1]-[5]. In all of these works, algebraic structure of the codes is exploited to derive new bounds on the asymptotic performance limits of communication. These bounds are strictly better than those derived using unstructured codes. Most of these works concentrate on linear codes built on finite fields. Despite the aforementioned benefits, the algebraic structure imposed by linear codes has certain restrictions. Finite fields exist only when the alphabet size is a prime power. Even when the existence is not an issue, in certain problems, weaker algebraic structures such as groups have better properties, [6]. Group codes are a type of structured codes that are closed under the group operation. These codes have been studied in [6]-[9] for point-to-point (PtP) communication problems. Under specific constraints in multi-terminal settings, compared to linear codes, the structure of group codes matches better with that of the channel or source. This results in achieving lower transmission rates in certain distributed source coding problems [10] and higher transmission rates for certain broadcast channels [2].

When the underlying group is not a field, there are non trivial subgroups. Since group codes are closed under the group addition, these subgroups put a penalty on the transmission rates. Based on this observation, in our earlier attempt, we introduced a class of structured codes called transversal group codes [11]. These codes are built over cyclic groups. In contrast to group codes, they are not closed under the group addition. This allows the transversal group codes to compensate for the penalty put by subgroups and achieve higher/lower transmission rates in channel/source coding problems. In particular, these codes extend the asymptotic rate region achievable in distributed source coding as well as computation over MAC.

In this paper, we extend the notion of transversal group codes and introduce a new class of codes over groups called Multi-Level Group Codes (MLGC). These codes are constructed by taking subsets of group codes. We restrict ourselves to cyclic groups and provide a construction of the subsets. We first study some basic properties of MLGC and derive a packing and a covering bound for such codes. These bounds indicate that the PtP channel capacity and optimal rate-distortion function is achievable using MLGC. Next, we use these results to explore the applications of MLGC in multi-terminal communication problems. We derive achievable rates using MLGC for certain distributed source coding and computation over MAC problems. We show, through some examples, that these codes give better achievable rates for both settings. Due to space limitation in this paper, some proofs have been omitted; a more complete version can be found in [12].

The rest of this paper is organized as follows: Section II provides the preliminaries and notations. In Section III we propose MLGC and investigate some of their properties. In Section IV and Section V, we discuss the applications of MLGC in computation over MAC and distributed source coding, respectively. Section VI concludes the paper.

II. Preliminaries

Notations: We denote (i) vectors using lowercase bold letters such as $\mathbf{b}, \mathbf{u}$, (ii) matrices using uppercase bold letters such as $\mathbf{A}$, (iii) random variables using capital letters such as X, Y, (iv) numbers, realizations of random variables and elements of sets using lower case letters such as a, x. Calligraphic letters such as $\mathcal{C}$ and $\mathcal{U}$ are used to represent sets. For shorthand, we denote the set $\{1, 2, \ldots, m\}$ by $[1 : m]$.

Groups: A group is a set equipped with a binary operation denoted by "+". The focus of this paper is on the cyclic groups. Given a prime power p^r, the group of integers modulo p^r is denoted by $\mathbb{Z}_{p^r}$, where the underlying set is $\{0, 1, \cdots, p^r - 1\}$ and the addition is modulo-p^r. For $s \in \{0, 1, \cdots, r\}$, define

$$G_s = p^s \mathbb{Z}_{p^r} = \{0, p^s, 2p^s, \cdots, (p^{r-s} - 1)p^s\},$$

and $T_s = \{0, 1, \cdots, p^s - 1\}$. Note, G_s is a subset of $\mathbb{Z}_{p^r}$ that is closed under the modulo-p^r addition. Given G_s and T_s, each element a of $\mathbb{Z}_{p^r}$ can be represented uniquely as a sum $a = t + g$, where $g \in G_s$ and $t \in T_s$. We denote such t by $[a]_s$.

For any elements $a, b \in \mathbb{Z}_{p^r}$, we define the multiplication $a \cdot b$ by adding a with itself b times. Given the group $\mathbb{Z}_{p^r}$ a positive integer n, we construct a larger group denoted by $\mathbb{Z}_{p^r}^n = \bigotimes_{i=1}^n \mathbb{Z}_{p^r}$, whose addition is element-wise.

Group Codes: Let $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ and consider a $k \times n$ matrix $\mathbf{A}$ with elements in $\mathbb{Z}_{p^r}$, where $k \leq n$. A group code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ with length n is defined by

$$\mathcal{C} = \{\mathbf{uA} + \mathbf{b} : \mathbf{u} \in \mathbb{Z}_{p^r}^k\}.$$

Group codes, in general, are defined over any group G. Sahebi, *et al,* [9], characterized the ensemble of all group codes over commutative groups.

Transversal Group Codes: Select $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ and for each $s \in [1 : r]$, let $\mathbf{A}_s$ be a $k_s \times n$ matrix with elements in $\mathbb{Z}_{p^r}$. A transversal group code over $\mathbb{Z}_{p^r}$ with length n is defined as

$$\mathcal{C} = \{\sum_{s=1}^{r} \mathbf{u}_s \mathbf{A}_s + \mathbf{b} : \mathbf{u}_s \in T_s^{k_s}, s \in [1 : r]\}.$$

A. Computation Over MAC

Consider a two user MAC whose input alphabets at each terminal form a group G and its output alphabet is denoted by $\mathcal{Y}$.

Definition 1 (Codes for computation over MAC)**.** *A (θ_1, θ_2)-code for computation over the above MAC consists of two encoding functions and one decoding function. The encoding functions are denoted by $f_i : [1 : \theta_i] \to G^n$, for $i = 1, 2$ and the decoding function is a map $g : \mathcal{Y}^n \to G^n$.*

Definition 2 (Achievable Rate)**.** *(R_1, R_2) is said to be achievable if for any $\epsilon > 0$, there exist a (θ_1, θ_2)-code such that*

$$P\{g(Y^n) \neq f_1(m_1) + f_2(m_2)\} \leq \epsilon, \quad R_i \leq \frac{1}{n} \log \theta_i,$$

holds for all $m_i \in [1 : \theta_i], i = 1, 2$.

III. Multi-Level Group Codes

In this section, we propose *Multi-level group* codes that are built upon group codes. It is known that a linear code over a field $\mathbb{F}_p$ is a subspace of $\mathbb{F}_p^n$. This code can also be viewed as the image of a linear transformation from $\mathbb{F}_p^k$ into $\mathbb{F}_p^n$. Similarly, as described in Section II, a group code over $\mathbb{Z}_{p^r}$, can be viewed as the image of a map from $\mathbb{Z}_{p^r}^k$ into $\mathbb{Z}_{p^r}^n$. Such map is denoted as $\phi(\mathbf{u}) = \mathbf{uA} + \mathbf{b}$, where $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ and $\mathbf{A}$ is a matrix with elements belonging to $\mathbb{Z}_{p^r}$. The idea to create MLGC is to restrict the domain of this map to a subset of $\mathbb{Z}_{p^r}^k$. We first discuss this idea for a special case, then we describe a specific construction of this subset.

Suppose U is a random variable over $\mathbb{Z}_{p^r}$. For some small $\epsilon > 0$, let $\mathcal{U} = A_\epsilon^{(k)}(U)$. Consider a $k \times n$ matrix $\mathbf{A}$ with elements in $\mathbb{Z}_{p^r}$ and let

$$\mathcal{C} = \{\mathbf{uA} + \mathbf{b} : \mathbf{u} \in \mathcal{U}\},$$

where $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ is an arbitrary translation. Note if U is uniform over $\mathbb{Z}_{p^r}$, then $\mathcal{C}$ will be a group code.

Next, we propose a more general construction of $\mathcal{U}$. Consider positive integers $m, k_i, i \in [1 : m]$. For each i, let $\mathbf{A}_i$ be a $k_i \times n$ matrix with elements in $\mathbb{Z}_{p^r}$. Consider the map $\phi(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m) = \sum_{i=1}^m \mathbf{u}_i \mathbf{A}_i + \mathbf{b}$. Suppose $U_1, U_2, \cdots, U_m$ are independent random variables over $\mathbb{Z}_{p^r}$. For a small $\epsilon > 0$, define the MLGC code as

$$\mathcal{C} = \{\phi(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m) \mid \mathbf{u}_i \in A_\epsilon^{(k_i)}(U_i), i \in [1 : m]\}. \quad (1)$$

Note, we consider $\mathcal{U}$ as a Cartesian product of the typical sets of U_i, i.e.,

$$\mathcal{U} = \bigotimes_{i=1}^{m} A_\epsilon^{(k_i)}(U_i).$$

We restrict ourselves to this construction of $\mathcal{U}$, due to tractability in analyzing the performance of the code.

Definition 3. *An $(n, m, k_1, k_2, \ldots, k_m)$ MLGC over $\mathbb{Z}_{p^r}$ is characterized by a translation $\mathbf{b} \in \mathbb{Z}_{p^r}^n$, random variables U_i over $\mathbb{Z}_{p^r}$ and $k_i \times n$ matrices $\mathbf{A}_i$, where $i \in [1 : m]$.*

Remark 1. Any group code and transversal group code over $\mathbb{Z}_{p^r}$ is a multi-level group code.

Fix $n, m, k_1, k_2, \ldots, k_m$ and random variables $U_i, i \in [1 : m]$. We create an ensemble by taking the collection of all $(n, k_1, k_2, \ldots, k_m)$ multi-level group codes with random variables U_i, for all matrices $\mathbf{A}_i$ and translations $\mathbf{b}$. A random codebook $\mathcal{C}$, from this ensemble, is chosen by selecting the elements of $\mathbf{A}_i, i \in [1 : m]$ and $\mathbf{b}$ randomly and uniformly from $\mathbb{Z}_{p^r}$. For large enough n, with probability one the rate of this code is

$$R = \frac{1}{n} \log_2 |\mathcal{C}| \approx \sum_{i=1}^{m} \frac{k_i}{n} H(U_i).$$

Note, we have assumed that the map induced by $\mathbf{b}$ and the matrices $\mathbf{A}_i$ is injective. This conditions is satisfied with high probability if

$$\sum_{i=1}^{m} \frac{k_i}{n} H(U_i | [U_i]_s) \leq (r - s) \log_2 p, \text{ for } 0 \leq s \leq r - 1.$$

In the next subsection, we discuss the properties of multi-level group codes and derive a packing and a covering bound for these codes.

A. Properties of Multi-Level Group Codes

When the underlying group is $\mathbb{Z}_{p^r}$ for $r \geq 2$, there are several nontrivial subgroups. These subgroups cause a penalty on the rate of a group code. This results in lower transmission rates in channel coding and higher transmission rates in source coding. However, when the structure of the group codes match with that of a multi-terminal channel/source coding problem, higher/lower transmission rates are obtained. One reason is that as group codes are closed under the addition, $|\mathcal{C} + \mathcal{C}|$ is small. This brings about higher transmission rates in multi-terminal channel coding where the sum of two transmitted codewords are decoded.

Transversal group codes remove the penalty for the subgroups by paying the price for larger $|\mathcal{C} + \mathcal{C}|$. multi-level group codes, on the other hand, balance the trade off between the penalty for subgroups and $|\mathcal{C} + \mathcal{C}|$. This results in a more flexible algebraic structure to match better with the structure of the channel or source. The following lemma shows such tradeoff.

Lemma 1. *Suppose $\mathcal{C}$ and $\mathcal{C}'$ are two $(n, m, k_1, \ldots, k_m)$ MLGC with random variables U_i and $U_i', i \in [1 : m]$, respectively. If $\mathcal{C}$ and $\mathcal{C}'$ have identical matrices and translation with elements chosen randomly and uniformly from $\mathbb{Z}_{p^r}$, then with probability one the followings hold:*

1) $\mathcal{C} + l\mathcal{C}'$ is a $(n, m, k_1, \ldots, k_m)$ multi-level group code with random variable $U_i + lU_i'$,

2) $\max\{|\mathcal{C}|, |l\mathcal{C}'|\} \le |\mathcal{C} + l\mathcal{C}'| \le \min\{p^{rn}, |\mathcal{C}| \cdot |l\mathcal{C}'| - 1\}$,

where $l \in \mathbb{Z}_{p^r}$ is an arbitrary element.

Proof: The complete proof is given in [12]. ■

In what follows, we prove a covering and a packing bound for multi-level group codes. These bounds are useful in analyzing the asymptotic performance of MLGC's.

Lemma 2 (Packing)**.** *Let $\mathcal{C}$ be a $(n, m, k_1, k_2, \ldots, k_m)$ MLGC with translation $\mathbf{b}$, random variables U_i and matrices $\mathbf{A}_i$, $i \in [1 : m]$. Let $(X, Y) \sim p(x, y)$, where X takes values from $\mathbb{Z}_{p^r}$. Suppose the elements of $\mathbf{A}_i$ and $\mathbf{b}$ are chosen randomly and uniformly from $\mathbb{Z}_{p^r}$. Then for an arbitrary sequence $\mathbf{y}$,*

$$P\{(\mathbf{x}, \mathbf{y}) \in A_\epsilon^{(n)}(X, Y) \text{ for some } \mathbf{x} \in \mathcal{C}\} \to 0, \text{ as } n \to \infty,$$

if

$$R \le \min_{0 \le s \le r-1} \frac{\sum_{i=1}^m k_i H(U_i)}{\sum_{i=1}^m k_i H(U_i|[U_i]_s)} \big(\log_2 p^{r-s} - H(X|Y[X]_s) \big). \quad (2)$$

Proof: For the proof refer to [12] ■

Lemma 3 (Covering)**.** *Let $\mathcal{C}$ be a $(n, m, k_1, k_2, \ldots, k_m)$ MLGC with translation $\mathbf{b}$, random variables U_i and matrices $\mathbf{A}_i$, $i \in [1 : m]$. Let $(X, \hat{X}) \sim p(x, \hat{x})$, where $\hat{X}$ is uniform over $\mathbb{Z}_{p^r}$. Suppose the elements of $\mathbf{A}_i$ and $\mathbf{b}$ are chosen randomly and uniformly from $\mathbb{Z}_{p^r}$. Then for any $\mathbf{x} \in A_\epsilon^{(n)}(X)$,*

$$P\{(\mathbf{x}, \hat{\mathbf{x}}) \in A_\epsilon^{(n)}(X, \hat{X}) \text{ for some } \hat{\mathbf{x}} \in \mathcal{C}\} \to 1, \text{ as } n \to \infty,$$

if

$$R \ge \max_{1 \le s \le r} \frac{\sum_{i=1}^m k_i H(U_i)}{\sum_{i=1}^m k_i H([U_i]_s)} \big(\log_2 p^s - H([\hat{X}]_s|X) \big). \quad (3)$$

Proof: The proof is given in [12]. ■

Remark 2. MLGC codes achieve the symmetric channel capacity and symmetric rate-distortion function. To see this, set $m = 1$ and U_1 uniform over $\{0, 1\}$.

Lemma 1, 2 and Lemma 3 provide a tool to derive inner bounds for achievable rates using multi-level group codes in multi-terminal channel coding and source coding. In the next two sections, we study applications of multi-level group codes in distributed source coding and computation over MAC. We will show that multi-level group code improves upon previously known schemes. But, before that let us describe another ensemble of codes based on multi-level group codes.

B. Unionized Multi-Level Group Codes

Note that a randomly generated MLGC has uniform distribution over the group $\mathbb{Z}_{p^r}$. However, in many communication setups we require application of codes with non-uniform distributions. In the case of group codes, this problem is resolved by constructing a group code first, then the union of different shifts of this group code is considered as the codebook. In other words, a large codebook is binned, where the bins themselves are required to possess a group structure [9]. This new codebook is called a unionized group code. Dual to this codebook construction method, we design a new ensemble of codes. The new codes are called Unionized Multi-Level Group Codes (UMLGC).

A UMLGC consists of an inner code and an outer code. Suppose $\mathcal{C}_{in}$ is a $(n, m, k_1, \ldots, k_m)$ MLGC with translation $\mathbf{b}$, random variables U_i and matrices $\mathbf{A}_i, i \in [1 : m]$. We use $\mathcal{C}_{in}$ as the inner code. Given a positive integer l, consider a map $t : [1 : l] \to \mathbb{Z}_{p^r}^n$. Define the outer code as

$$\mathcal{C}_{out} = \bigcup_{j \in [1:l]} (\mathcal{C}_{in} + t(j))$$

Definition 4. *An $(n, m, l, k_1, k_2, \ldots, k_m)$ UMLGC over $\mathbb{Z}_{p^r}$ is characterized by a mapping $t : [1 : l] \to \mathbb{Z}_{p^r}^n$, a translation $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ and $k_i \times n$ matrices $\mathbf{A}_i, i \in [1 : m]$ with elements in $\mathbb{Z}_{p^r}$.*

One application of UMLGC is in PtP source coding and channel coding.

Lemma 4. *UMLGC achieve the PtP channel capacity and rate-distortion function for any channel and source with finite alphabet size.*

Proof: The proof follows from Remark 2 and is provided in [12]. ■

IV. Distributed Source Coding

We study a two-user distributed source coding and derive an achievable region. Suppose X_1 and X_2 are sources over $\mathbb{Z}_{p^r}$ with joint PMF $p(x_1, x_2)$. The jth encoder compress X_j and sends it to a central decoder. The decoder wishes to reconstruct $X_1 + X_2$ losslessly. We propose a coding scheme using unionized multi-level group codes and derive an achievable region. Then we show that this region strictly extends the previously know achievable regions.

Definition 5. *A pair (R_1, R_2) belongs to $\mathcal{R}_s$, if there exist $m \in \mathbb{N}$, $q_i \in \mathbb{Q}$ and random variables $V_i, V_i', i \in [1 : m]$ over $\mathbb{Z}_{p^r}$, such that*

$$R_1 + \sum_{i=1}^m q_i H(V_i) = r \log_2 p, \quad R_2 + \sum_{i=1}^m q_i H(V_i') = r \log_2 p,$$

where 1) $q_i > 0$, 2) $V_i, V_i', i \in [1 : m]$ are mutually independent, 3) For any $s \in [0 : r - 1]$

$$\sum_{i=1}^m q_i H(W_i|[W_i]_s) \le r \log_2 p - H(X|[X]_s),$$

where $W_i = V_i + V_i'$, $X = X_1 + X_2$.

Theorem 1. *$\mathcal{R}_s$ is achievable for lossless reconstruction of $X_1 + X_2$, where X_1 and X_2 are a pair of sources over the group $\mathbb{Z}_{p^r}$.*

Outline of the proof: Consider any pair of rates $(R_1, R_2) \in \mathcal{R}_s$. Let $m, q_i, V_i, V_i', i \in [1 : m]$ are as in Definition 5 and correspond to (R_1, R_2). Assume $q_i = k_i/n$, where k_i and n are positive integers. For each i, generate a $k_i \times n$ matrix $\mathbf{A}_i$ whose elements are chosen randomly and uniformly from $\mathbb{Z}_{p^r}$. Select $\mathbf{b}, \mathbf{b}' \in \mathbb{Z}_{p^r}^n$ randomly and uniformly. Let $t : [1 : 2^{nR_1}] \to \mathbb{Z}_{p^r}^n$ and $t' : [1 : 2^{nR_2}] \to \mathbb{Z}_{p^r}^n$ be two maps selected randomly.

Codebook Generation: We use three UMLGC, one for each encoder and one for the decoder. We first build the inner codes. Let $\mathcal{C}_{in}$ and $\mathcal{C}_{in}'$ be two $(n, m, k_1, \ldots, k_m)$ multi-level group codes with identical matrices $\mathbf{A}_i$. Let $\mathbf{b}$ and $V_i, i \in [1 : m]$ be the corresponding translation and random variables of $\mathcal{C}_{in}$, respectively. Assign $\mathbf{b}'$ and $V_i', i \in [1 : m]$ as the translation and random variables associated with $\mathcal{C}_{in}'$. Define $\mathcal{C}_{in,d} = \mathcal{C}_{in} + \mathcal{C}_{in}'$.

Let the outer code for the first and the second encoder be denoted by $\mathcal{C}_{out}$ and $\mathcal{C}_{out}'$, respectively. These two codebooks are given as follows:

$$\mathcal{C}_{out} = \bigcup_{j \in [1:2^{nR_1}]} (\mathcal{C}_{in} + t(j)),$$
$$\mathcal{C}_{out}' = \bigcup_{j' \in [1:2^{nR_2}]} (\mathcal{C}'_{in} + t'(j')).$$

Encoding: Given a typical sequence $\mathbf{x}_1 \in A_\epsilon^n(X_1)$, encoder 1 first finds $j \in [1 : 2^{nR_1}]$ and $\mathbf{c} \in \mathcal{C}_{in}$ such that $\mathbf{x}_1 = \mathbf{c} + t(j)$; then it sends j. If no such j was found, an error event E_1 will be declared.

Similarly, upon receiving $\mathbf{x}_2 \in A_\epsilon^n(X_2)$, the second encoder finds $j' \in [1 : 2^{nR_2}]$ and $\mathbf{c}' \in \mathcal{C}'_{in}$ such that $\mathbf{x}_2 = \mathbf{c}' + t'(j)$ and sends j'. If no such j' was found, an error event E_2 will be declared. If more than one index were found at each encoder, select one randomly.

Decoding: Assume there is no encoding error. The decoder wishes to reconstruct $\mathbf{x}_1 + \mathbf{x}_2$. Upon receiving j and j', the decoder takes $t(j)$ and $t'(j')$; then finds $\mathbf{c}_d \in \mathcal{C}_{in,d}$ such that $\mathbf{c}_d + t(j) + t'(j') \in A_\epsilon^{(n)}(X_1 + X_2)$. If such $\mathbf{c}_d$ is found, then $\tilde{\mathbf{z}} = \mathbf{c}_d + t(j) + t'(j')$ is declared as a reconstruction of $\mathbf{x}_1 + \mathbf{x}_2$. An error event E_d occurs if $\tilde{\mathbf{z}} \neq \mathbf{x}_1 + \mathbf{x}_2$.

We show in [12] that for large enough n the probability of $E_1 \cup E_2 \cup E_d$ approaches zero. ∎

Remark 3. When X_1 and X_2 are distributed over the field $\mathbb{Z}_p$, $\mathcal{R}_s$ is equivalent to

$$R_j \geq H(X_1 + X_2).$$

This is the achievable rate region using linear codes.

In general, $\mathcal{R}_s$ extends the achievable regions using linear codes, group codes and transversal group codes. We show, through an example, that this extension is strict.

Example 1. We consider a distributed source coding problem in which X_1 and X_2 are sources over $\mathbb{Z}_4$ and lossless reconstruction of $X_1 + X_2$ is required at the decoder. Assume X_1 is uniform over $\mathbb{Z}_4$. X_2 is related to X_1 via $X_2 = N - X_1$, where N is independent of X_1. The distribution of N is given in Table I.

TABLE I. DISTRIBUTION OF N

N	0	1	2	3
P_N	$0.1\delta_N$	$0.9\delta_N$	$0.1(1-\delta_N)$	$0.9(1-\delta_N)$

It is known that group codes in this example outperform linear codes, [9]. The largest achievable region using group codes is

$$R_j \geq \max\{H(Z), 2H(Z|[Z]_1)\}, \quad j = 1, 2,$$

where $Z = X_1 + X_2$. We showed in [11] that transversal group codes outperform group codes and the following is achievable

$$R_j \geq \max\{H(Z), 1/2H(Z) + H(Z|[Z]_1)\}.$$

Using Theorem 1, an inner bound for $\mathcal{R}_s$ is obtained as

$$R_j \geq 2 - \min\{0.6(2 - H(Z)), 5.7(2 - 2H(Z|[Z]_1)\}.$$

This is verified by setting $m = 1$, $P(V_1 = 0) = P(V_1' = 0) = 0.95$ and $P(V_1 = 1) = P(V_1' = 1) = 0.05$.

Now, let $\delta_N = 0.6$. In this case, using group codes the rate $R_i \approx 1.94$ is achievable, using transveral group codes $R_i \approx 1.69$ is achievable and lastly UMLGC achieves $R_i \approx 1.67$.

V. COMPUTATION OVER MAC

Through a variation from the standard computation over MAC problems, in this section, we explore distributed computation of the inputs of a MAC. Consider a two-user MAC in which a central receiver wishes to compute the sum of the inputs the channel. Figure 1 depicts a schematic of this setup. Suppose the channel's inputs, X_1 and X_2, take values from $\mathbb{Z}_{p^r}$. Two distributed encoders map their messages to X_1^n and X_2^n. Upon receiving the channels output the decoder wishes to decode $X_1^n + X_2^n$ with no loss. Applications of this problem are in various multui-user communication setups such as interference and broadcast channels.

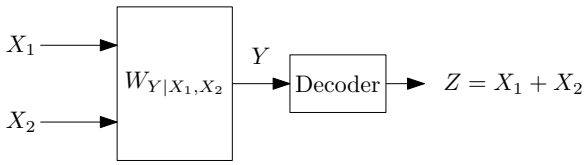

Fig. 1. The diagram of computation over MAC.

For the above setup, we use multi-level group codes to derive an achievable region which extends the previously known regions. Our scheme consists of two multi-level group codes, one for each encoder. We use identical matrices for each code but different translations and random variables. At the decoder, as a codebook, we consider the sum of the codebooks used at each encoder. Using the packing bound in Lemma 2 we show that the following set of rates is achievable.

Definition 6. *The pair (R_1, R_2) belongs to $\mathcal{R}_c$, if there exist $m \in \mathbb{N}, q_i \in \mathbb{Q}$ and random variables V_i and V_i', for $i \in [1 :$*

$m]$, *such that*

$$R_1 = \sum_{i=1}^{m} q_i H(V_i), \quad R_2 = \sum_{i=1}^{m} q_i H(V_i'),$$

where $q_i \geq 0$ *and 1)*$V_i, V_i', i \in [1 : m]$ *are mutually independent, , 2) for any* $s \in [0 : r-1]$,

$$\sum_{i=1}^{m} q_i H(W_i|[W_i]_s) \leq r \log_2 p - H(X|Y, [X]_s), \qquad (4)$$

where $W_i = V_i + V_i'$, $X = X_1 + X_2$ *and* X_1 *and* X_2 *are uniform over* $\mathbb{Z}_{p^r}$.

Theorem 2. *$\mathcal{R}_c$ is achievable for computation over any MAC with input-alphabets $\mathbb{Z}_{p^r}$.*

Outline of the proof: Consider a pair $(R_1, R_2) \in \mathcal{R}_c$. Suppose m and $q_i, V_i, V_i', i \in [1 : m]$ are as in Definition 6 and correspond to (R_1, R_2). We can find positive integers n and k_i such that for each i, $q_i = k_i/n$.

For each i, generate a $k_i \times n$ matrix $\mathbf{A}_i$ whose elements are chosen randomly and uniformly from $\mathbb{Z}_{p^r}$. Select $b, b' \in \mathbb{Z}_{p^r}^n$ randomly and uniformly.

Codebook Generation: Let $\mathcal{C}$ and $\mathcal{C}'$ be two $(n, m, k_1, k_2, \ldots, k_m)$ MLGC with identical matrices $\mathbf{A}_i$. Let the translation and random variables corresponding to $\mathcal{C}$ be b and $V_i, i \in [1 : m]$. Assign b' and $V_i', i \in [1 : m]$ as the translation and random variables associated with $\mathcal{C}'$. Lastly, set $\mathcal{C}_d = \mathcal{C} + \mathcal{C}'$. By Lemma 1, $\mathcal{C}_d$ is a MLGC with translation $b + b'$ and random variable $V_i + V_i'$. Index all the codwords in each codebooks $\mathcal{C}, \mathcal{C}'$ and $\mathcal{C}_d$.

Encoding: Encoder one upon receiving a message index θ sends the corresponding codeword in $\mathcal{C}$. The second encoder, similarly, upon receiving θ' sends the corresponding codeword in $\mathcal{C}'$. Suppose the output of encoder j is $x_j, j = 1, 2$.

Decoding: Upon receiving y from the channel, the decoder wishes to decode $x = x_1 + x_2$. It finds $\tilde{x} \in \mathcal{C}_d$ such that $\tilde{x}$ and y are jointly typical with respect to the distribution $P_{X_1+X_2,Y}$, where X_1 and X_2 are uniform over $\mathbb{Z}_{p^r}$. An error occurs if no unique $\tilde{x}$ is found.

This is a packing problem for the effective channel $P_{Y|X_1+X_2}$. Denote the rate of $\mathcal{C}_d$ by R. Then by Lemma 2, the probability of error is small enough, if (2) holds for $U_i = V_i + V_i'$ and $X = X_1 + X_2$. This bound is equivalent to (4). Note that the rate of $\mathcal{C}$ and $\mathcal{C}'$ are R_1 and R_2, respectively. So (R_1, R_2) is achievable. ∎

Remark 4. Assume that the underlying group is $\mathbb{Z}_p$, i.e., the case where $r = 1$. Then $\mathcal{R}_c$ is simplified to

$$R_j \leq I(X_1 + X_2; Y), j = 1, 2,$$

where X_1 and X_2 are independent and uniform over $\mathbb{Z}_{p^r}$. It is known that this region is achievable by linear codes.

In what follows, we show by an example that $\mathcal{R}_c$ strictly extends the achievable region of unstructured codes, group codes and transversal group codes.

Example 2. Consider the following MAC:

$$Y = X_1 \oplus X_2 \oplus N,$$

where X_1 and X_2 are the channel inputs with alphabet $\mathbb{Z}_4$. N is independent of X_1 and X_2 with the distribution given in Table I, where $0 \leq \delta_N \leq 1$.

It is shown in [9] that the largest achievable region for group codes is

$$R_j \leq \min\{I(Z;Y), 2I(Z;Y|[Z]_1)\},$$

where $Z = X_1 + X_2$ and X_1 and X_2 are uniform over $\mathbb{Z}_4$. In [11], we showed transversal group codes achieve,

$$R_j \leq \min\{I(Z;Y), 0.5I(Z;Y) + I(Z;Y|[Z]_1)\}.$$

From Theorem 2, multi-level group codes achieve

$$R_j \leq \min\{0.6I(Z;Y), 5.7I(Z;Y|[Z]_1)\}.$$

Now, by setting $\delta_N = 0.6$, the rate $R_i \approx 0.06$ is achievable using group codes and $R_i \approx 0.31$ is achievable using transversal group codes. Whereas, $R_i \approx 0.33$ is achievable using MLGC.

VI. Conclusion

The problem of computing modulo prime-power was considered. A new layered ensemble of structured codes called MLGC was introduced. We investigated the performance limits of these codes in distributed source coding and computation over MAC. Achievablility results using these codes were provided for both settings. We showed that the application of MLGC for these problems results in improvements in terms of transmission rates.

References

[1] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources", IEEE Transactions on Information Theory, IT-25:219–221, Mar. 1979.

[2] A. Padakandla and S.S. Pradhan, "Achievable rate region for three user discrete broadcast channel based on coset codes," IEEE International Symposium on Information Theory Proceedings (ISIT), pp.1277-1281, July 2013.

[3] T. Philosof and R. Zamir, "On the loss of single-letter characterization: The dirty multiple access channel," IEEE Trans. Inform. Theory, vol. 55, pp. 2442-2454, June 2009.

[4] B. A. Nazer and M. Gastpar, "Computation over multiple-access channels", IEEE Transactions on Information Theory, Oct. 2007.

[5] A. Padakandla and S.S. Pradhan, "Computing sum of sources over an arbitrary multiple access channel," IEEE International Symposium on Information Theory Proceedings (ISIT), 2013 , pp.2144-2148, July 2013.

[6] H. A. Loeliger, "Signal sets matched to groups", IEEE Trans. Inform. Theory, vol. 37, no. 6, pp. 1675–1682, November 1991.

[7] H. A. Loeliger and T. Mittelholzer, "Convolutional codes over groups", IEEE Trans. Inform. Theory,vol. 42, no. 6, pp. 1660–1686, November 1996.

[8] G. Como and F. Fagnani, "The capacity of finite abelian group codes over symmetric memoryless channels", IEEE Transactions on Information Theory, 55(5):2037–2054, 2009.

[9] A.G. Sahebi, S.S. Pradhan, "Abelian Group Codes for Channel Coding and Source Coding," IEEE Transactions on Information Theory, vol.61, no.5, pp.2399-2414, May 2015.

[10] A. G Sahebi, and S.S Pradhan, "On distributed source coding using Abelian group codes," Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on , pp.2068,2074, 1-5 Oct. 2012

[11] M. Heidari, F. Shirani and S. Pradhan, " Beyond group capacity in multi-terminal communications", 2015

[12] M. Heidari, S.S. Pradhan, "How to Compute Modulo Prime-Power Sums," http://arxiv.org, 2016.