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 group codes and present a new class of codes called Quasi Group Codes (QGC). A QGC is a subset of a group code. These codes are not closed under the group addition. We investigate some properties of QGC's, and provide a packing and a covering bound. Next, we use these bounds to derived achievable rates for distributed source coding as well as computation over MAC. We show that strict improvements over the previously known schemes can be obtained using QGC's.**

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 nontrivial 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 Quasi Group Codes (QGC). 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 QGC's 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 QGC's. Next, we use these results to explore the applications of QGC's in multi-terminal communication problems. We derive achievable rates using QGC's 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 QGC's and investigate some of their properties. In Section IV and Section V, we discuss the applications of QGC's in distributed source coding and computation over MAC, respectively. Section VI concludes the paper.

II. Preliminaries

A. Notations

We denote (i) vectors using lowercase bold letters such as $\mathbf{b}, \mathbf{u}$, (ii) matrices using uppercase bold letters such as $\mathbf{G}$, (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 $\{1, 2, \dots, m\}$ by $[1:m]$.

B. Definitions

A group is a set equipped with a binary operation denoted by "+". 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

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

and $T_s = \{0, 1, \cdots, p^s - 1\}$. For example, $H_0 = \mathbb{Z}_{p^r}, T_0 = \{0\}$, whereas $H_r = \{0\}, T_r = \mathbb{Z}_{p^r}$. Note, H_s is a subset of $\mathbb{Z}_{p^r}$ that is closed under the modulo-p^r addition. Given H_s and T_s, each element a of $\mathbb{Z}_{p^r}$ can be represented uniquely as

This work was supported by NSF grant CCF-1111061 and CCF-1422284.

978-1-5090-1806-2/16/$31.00 ©2016 IEEE

a sum $a = t + h$, where $h \in H_s$ 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 a positive integer n, denote $\mathbb{Z}_{p^r}^n = \bigotimes_{i=1}^n \mathbb{Z}_{p^r}$. Note $\mathbb{Z}_{p^r}^n$ is a group, whose addition is element-wise and its underlying set is $\{0, 1, \ldots, p^r - 1\}^n$.

Definition 1 (Shifted Group Codes). *Consider positive integers n, k, where $k \leq n$. An (n, k)-shifted group code over $\mathbb{Z}_{p^r}$ is defined as*

$$\mathcal{C} = \{\mathbf{u}\mathbf{G} + \mathbf{b} : \mathbf{u} \in \mathbb{Z}_{p^r}^k\}, \tag{1}$$

where $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ and $\mathbf{G}$ is a $k \times n$ matrix with elements in $\mathbb{Z}_{p^r}$.

Suppose the elements of $\mathbf{G}$ and b are chosen randomly and uniformly over $\mathbb{Z}_{p^r}$. Then with probability one, the rate of the shifted group code corresponding to $\mathbf{G}$ and $\mathbf{b}$ is $R = \frac{1}{n} \log_2 |\mathcal{C}| = \frac{k}{n} \log_2 p$. Shifted group codes, in general, are defined over arbitrary groups. Sahebi, *et al,* [9], characterized the ensemble of all group codes over finite commutative groups.

Definition 2 (Transversal Group Codes). *Consider non-negative integers $n, k_1, k_2, \ldots, k_r$. An $(n, k_1, k_2, \ldots, k_r)$-transversal group code over $\mathbb{Z}_{p^r}$ is defined as*

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

where $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ and $\mathbf{G}_s$ is a $k_s \times n$ matrix with elements in $\mathbb{Z}_{p^r}$.

Suppose that the elements of $\mathbf{G}_s$ and $\mathbf{b}$ are selected randomly and uniformly over $\mathbb{Z}_{p^r}$. Then, for large enough n, with probability close to one, the rate of this code equals

$$R = \frac{1}{n} \log_2 |\mathcal{C}| = \sum_{s=1}^{r} \frac{k_s}{n} \log_2 |T_s| = \sum_{s=1}^{r} \frac{k_s}{n} \log_2 p^s$$

Performance limits of transversal codes for point-to-point as well as certain multi-terminal problems are investigated in [11].

Consider a two user MAC whose input alphabets at each terminal is $\mathbb{Z}_{p^r}$ and its output alphabet is denoted by $\mathcal{Y}$.

Definition 3 (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 $f_i : [1 : \theta_i] \to \mathbb{Z}_{p^r}^n$, for $i = 1, 2$ and the decoding function is a map $g : \mathcal{Y}^n \to \mathbb{Z}_{p^r}^n$.*

Definition 4 (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*

$$P\{g(Y^n) \neq f_1(M_1) + f_2(M_2)\} \leq \epsilon, \quad R_i \leq \frac{1}{n} \log \theta_i,$$

where M_1 and M_2 are independent random variables and $p(M_i = m_i) = \frac{1}{\theta_i}$ for all $m_i \in [1 : \theta_i], i = 1, 2$.

III. Quasi Group Codes

In this section, we propose a new class of codes called *quasi group* codes.

Note that a linear code over a field $\mathbb{F}_p$ is defined as 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, a shifted group code over $\mathbb{Z}_{p^r}$ (as in Definition 1) is the image of an *addition-preserving* map from $\mathbb{Z}_{p^r}^k$ into $\mathbb{Z}_{p^r}^n$. This map is denoted by $\phi(\mathbf{u}) = \mathbf{u}\mathbf{G} + \mathbf{b}$, where $\mathbf{b} \in \mathbb{Z}_{p^r}^n$ and $\mathbf{G}$ is a $k \times n$ matrix whose elements are in $\mathbb{Z}_{p^r}$.

The idea to construct a QGC is to consider only a subset of a shifted group code. This can be done by restricting the domain of ϕ to a subset $\mathcal{U}$ of $\mathbb{Z}_{p^r}^k$. Therefore, a QGC is defined by

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

where $\mathcal{U}$ is an arbitrary subset of $\mathbb{Z}_{p^r}^k$. For a general subset $\mathcal{U}$, the codebook $\mathcal{C}$ is not necessary closed under the addition. However, it possesses certain algebraic structures. Note that it is difficult to analyze the performance of QGC for a general $\mathcal{U}$. In what follows, we present a special construction of $\mathcal{U}$ that is suitable for tractability in analyzing the performance of the code.

Let U be a random variable over $\mathbb{Z}_{p^r}$ and set $\mathcal{U} = A_\epsilon^{(k)}(U)$. In this case, by changing the PMF of U, one can create different sets $\mathcal{U}$. For example, if U is uniform over $\mathbb{Z}_{p^r}$, then $\mathcal{U} = \mathbb{Z}_{p^r}^k$, and $\mathcal{C}$ will become a shifted group code.

Next, we provide a more general construction of $\mathcal{U}$. Fix m, and consider positive integers $k_i, i \in [1 : m]$. For each i, let $\mathbf{G}_i$ be a $k_i \times n$ matrix with elements in $\mathbb{Z}_{p^r}$. Suppose $U_1, U_2, \cdots, U_m$ are independent random variables over $\mathbb{Z}_{p^r}$. As a codebook define

$$\mathcal{C} = \{\sum_{i=1}^{m} \mathbf{u}_i \mathbf{G}_i + \mathbf{b} \mid \mathbf{u}_i \in A_\epsilon^{(k_i)}(U_i), i \in [1 : m]\}, \tag{2}$$

where $\mathbf{b} \in \mathbb{Z}_{p^r}^n$. Note, in this case, we consider $\mathcal{U}$ as a Cartesian product of the typical sets of U_i, i.e., $\mathcal{U} = \bigotimes_{i=1}^m A_\epsilon^{(k_i)}(U_i)$.

Definition 5. *An $(n, m, k_1, k_2, \ldots, k_m)$ QGC over $\mathbb{Z}_{p^r}$ is defined as in (2) and 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 $\mathbf{G}_i$, where $i \in [1 : m]$.*

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

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

$$R = \frac{1}{n} \log_2 |\mathcal{C}| \approx \min\{\log_2 p^r, \sum_{i=1}^{m} \frac{k_i}{n} H(U_i)\}. \tag{3}$$

Remark 2. Let $\mathcal{C}$ be a randomly selected QGC as in the above. In contrast to linear codes, codewords of $\mathcal{C}$ are not pairwise independent.

We use a different notation to simplify (3). Let $k = \sum_{i=1}^m k_i$. Denote $q_i = \frac{k_i}{k}$. Since $q_i \geq 0$ and $\sum_i q_i = 1$, we can define a random variable Q with $P(Q = i) = q_i$. Define a random variable U with the conditional distribution

$P(U=a|Q=i)=P(U_i=a)$ for all $a\in\mathbb{Z}_{p^r}, i\in[1:m]$. Therefore, (3) is simplified to

$$R\approx\min\{\log_2 p^r, \frac{k}{n}H(U|Q)\}. \tag{4}$$

A. Unionized Quasi Group Codes

Note that a randomly generated QGC 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 Quasi Group Codes (UQGC).

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

$$\mathcal{C}_{out}=\bigcup_{j\in[1:l]}(\mathcal{C}_{in}+t(j)) \tag{5}$$

Definition 6. *Let $\mathcal{C}_{in}$ be an $(n,m,k_1,\dots,k_m)$ QGC. An $(n,m,l,k_1,k_2,\dots,k_m)$ UQGC over $\mathbb{Z}_{p^r}$ is defined as in (5) and is characterized by $\mathcal{C}_{in}$ as the inner code and a mapping $t:[1:l]\rightarrow\mathbb{Z}_{p^r}^n$.*

B. Properties of Quasi Group Codes

It is known that if $\mathcal{C}$ is a random unstructured codebook, then $|\mathcal{C}+\mathcal{C}|\approx|\mathcal{C}|^2$ with high probability. Group codes on the other hand are closed under the addition, which means $|\mathcal{C}+\mathcal{C}|=|\mathcal{C}|$. Comparing to unstructured codes, when the structure of the group codes matches with that of a multi-terminal channel/source coding problem, higher/lower transmission rates are obtained. However, in certain problems, the structure of the group codes is too restrictive. More precisely, 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.

Quasi group codes balance the trade-off between the structure of the group codes and that of the unstructured codes. More precisely, when $\mathcal{C}$ is a QGC, then $|\mathcal{C}+\mathcal{C}|$ is a number between $|\mathcal{C}|$ and $|\mathcal{C}|^2$. This results in a more flexible algebraic structure to match better with the structure of the channel or source. This trade-off is shown more precisely in the following lemma.

Lemma 1. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two $(n,m,k_1,\dots,k_m)$ QGC with random variables U_i and $U'_i, i\in[1:m]$, respectively. Suppose $\mathcal{C}$ and $\mathcal{C}'$ have identical matrices and translation with elements chosen randomly and uniformly over $\mathbb{Z}_{p^r}$. Then for large enough n, with probability one, the followings hold:*

1) *$\mathcal{C}+a\mathcal{C}'$ is a $(n,m,k_1,\dots,k_m)$ QGC with random variables $U_i+aU'_i$,*
2) *$\max\{|\mathcal{C}|,|a\mathcal{C}'|\}\leq|\mathcal{C}+a\mathcal{C}'|\leq\min\{p^{rn},|\mathcal{C}|\cdot|a\mathcal{C}'|\}$,*

where $a\in\mathbb{Z}_{p^r}$ is arbitrary.

In what follows, we derive a packing and a covering bound for a QGC with matrices and translation chosen randomly and uniformly. Fix a PMF $p(x,y)$, and suppose an ϵ-typical sequence $\mathbf{y}$ is given with respect to the marginal distribution $p(y)$. Consider the set of all codewords that are jointly typical with $\mathbf{y}$ with respect to $p(x,y)$. In the packing lemma, we characterize the conditions in which the probability of this set is small. This implies the existence of a "good-channel" code which is also a QGC. In the covering lemma, we derive the conditions for which, with high probability, there exists at least one such codeword. In this case a "good-source" code exists which is also a QGC. These conditions are provided in the next two lemmas.

Let $\mathcal{C}$ be a $(n,m,k_1,k_2,\dots,k_m)$ QGC with random variables U_i. Suppose the generator matrices and the translation vector of $\mathcal{C}$ are chosen randomly and uniformly over $\mathbb{Z}_{p^r}$. Index codewords of $\mathcal{C}$ by $\theta\in[1:|\mathcal{C}|]$. By $\mathbf{c}(\theta)$ denote the θth codeword of $\mathcal{C}$. Define random variables Q and U as in (4), i.e., $P(Q=i)=\frac{k_i}{\sum_i k_i}$ and $P(U=a|Q=i)=P(U_i=a)$, for all $a\in\mathbb{Z}_{p^r}, i\in[1:m]$. Let $\mathcal{C}_{out}$ be a $(n,l,m,k_1,\dots,k_m)$ UQGC with $l=2^{nR_{bin}}$, $\mathcal{C}$ as an inner code and a map $t:[1:2^{nR_{bin}}]\rightarrow\mathbb{Z}_{p^r}^n$ which is selected randomly and uniformly. We use these notations in the following lemmas.

Lemma 2 (Packing)**.** *Let $(X,Y)\sim p(x,y)$, where X takes values over $\mathbb{Z}_{p^r}$. Fix $\theta\in[1:|\mathcal{C}|]$. Let $\tilde{\mathbf{Y}}^n$ be a random sequence distributed according to $\prod_{i=1}^n p(\tilde{y}_i|c_i(\theta))$. Suppose, conditioned on $\mathbf{c}(\theta)$, $\tilde{\mathbf{Y}}^n$ is independent of any other codewords in $\mathcal{C}$. Then, as $n\rightarrow\infty$, $P\{\exists\mathbf{x}\in\mathcal{C}:(\mathbf{x},\tilde{\mathbf{Y}}^n)\in A_\epsilon^{(n)}(X,Y),\mathbf{x}\neq\mathbf{c}(\theta)\}$ is arbitrary close to zero, if*

$$R<\min_{0\leq s\leq r-1}\frac{H(U|Q)}{H(U|Q,[U]_s)}\big(\log_2 p^{r-s}-H(X|Y[X]_s)\big). \tag{6}$$

Lemma 3 (Covering)**.** *Let $(X,\hat{X})\sim p(x,\hat{x})$, where $\hat{X}$ is uniform over $\mathbb{Z}_{p^r}$. Let $\mathbf{X}^n$ be a random sequence distributed according to $\prod_{i=1}^n p(x_i)$. Then, as $n\rightarrow\infty$, $P\{\exists\hat{\mathbf{x}}\in\mathcal{C}_{out}:(\mathbf{X}^n,\hat{\mathbf{x}})\in A_\epsilon^{(n)}(X,\hat{X})\}$ is arbitrary close to one, if*

$$R_{bin}+\frac{H([U]_s|Q)}{H(U|Q)}R>\log_2 p^s-H([\hat{X}]_s|X) \tag{7}$$

holds for $1\leq s\leq r$.

Remark 3. Using QGC's the symmetric channel capacity and symmetric rate-distortion function are achievable. To see this, set $R_{bin}=0, m=1$ and U_1 uniform over $\{0,1\}$.

0One application of these lemmas is in PtP source coding and channel coding using quasi group codes.

Lemma 4. *Using UQGC's, the PtP channel capacity and rate-distortion function is achievable for any channel and source with finite alphabet size.*

The proof of the above lemmas are provided in [12]. Lemma 1, 2 and Lemma 3 provide a tool to derive inner bounds for achievable rates using quasi group codes in multi-terminal channel coding and source coding problem. In the next two sections, we study applications of quasi group codes in distributed source coding as well as computation over MAC.

IV. Distributed Source Coding

In this section, we consider a special distributed source coding problem. Suppose X_1 and X_2 are sources over $\mathbb{Z}_{p^r}$ with joint PMF $p(x_1, x_2)$. The jth encoder compresses X_j and sends it to a central decoder. The decoder wishes to reconstruct $X_1 + X_2$ losslessly.

We use UQGC's to propose a coding strategy for this problem. We use two UQGC's with identical matrices, one for each encoder. As discussed in Subsection III-A, each UQGC consists of an inner code and an outer code. We select an outer code that is also a "good-source" code. Consider the codebook created by the sum of the two inner codes. Since, the decoder wishes to reconstruct only $X_1 + X_2$, we select the inner codes such that this codebook is also a "good-channel" code. In the following theorem, we characterize an achievable rate region for the above problem using UQGC's.

Theorem 1. *Suppose X_1 and X_2 are a pair of sources over the group $\mathbb{Z}_{p^r}$. Lossless reconstruction of $X_1 + X_2$ is possible, if the following holds*

$$R_i \geq \log_2 p^r - \frac{H(W_i|Q)}{H(W|[W]_s Q)}(\log_2 p^{(r-s)} - H(X|[X]_s)), \tag{8}$$

where, $i = 1, 2$, $0 \leq s \leq r-1$, $W = W_1 + W_2$ with probability one and the Markov chain $W_1 - Q - W_2$ holds.

Remark 4. One can bound the cardinality of Q by $|\mathcal{Q}| \leq r$. This implies that a UQGC with at most r layers is enough to achieve the above bounds.

Outline of the proof: Fix positive integers $n, m, k_1, \ldots, k_m$. Let $\mathcal{C}_{1,in}$ and $\mathcal{C}_{2,in}$ be two $(n, m, k_1, \ldots, k_m)$ QGC's (as in Definition 5) with identical matrices and translation, but with independent random variables. Suppose that the elements of the matrices and translation corresponding to $\mathcal{C}_{1,in}$ and $\mathcal{C}_{2,in}$ are selected randomly and uniformly from $\mathbb{Z}_{p^r}$. Let $t_1 : [1 : 2^{nR_1}] \rightarrow \mathbb{Z}_{p^r}^n$ and $t_2 : [1 : 2^{nR_2}] \rightarrow \mathbb{Z}_{p^r}^n$ be two maps selected randomly uniformly and independently of other random variables.

Codebook Generation: We use two UQGC's, one for each encoder. The codebook for the first encoder is a $(n, m, l_1, k_1, \ldots, k_m)$ UQGC with $l_1 = 2^{nR_1}$, the inner code $\mathcal{C}_{1,in}$ and the mapping t_1. For the second encoder use a $(n, m, l_2, k_1, \ldots, k_m)$ UQGC with $l_2 = 2^{nR_2}$, the inner code $\mathcal{C}_{2,in}$ and the mapping t_2. For the decoder, we use $\mathcal{C}_{1,in} + \mathcal{C}_{2,in}$ as a codebook.

Encoding: Given a typical sequence $\mathbf{x}_1 \in A_\epsilon^n(X_1)$, encoder 1 first finds $i \in [1 : 2^{nR_1}]$ and $\mathbf{c}_1 \in \mathcal{C}_{1,in}$ such that $\mathbf{x}_1 = \mathbf{c}_1 + t_1(i)$; then it sends i. If no such i is 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 $\mathbf{c}_2 \in \mathcal{C}_{2,in}$ such that $\mathbf{x}_2 = \mathbf{c}_2 + t_2(j)$ and sends j. If no such j is found, an error event E_2 will be declared. If more than one indices were found at each encoder, select one randomly.

Decoding: The decoder wishes to reconstruct $\mathbf{x}_1 + \mathbf{x}_2$. Assume there is no encoding error. Upon receiving i and j, the decoder first calculates $t_1(i)$ and $t_2(j)$. Then it finds $\tilde{\mathbf{c}} \in \mathcal{C}_{1,in} + \mathcal{C}_{2,in}$ such that $\tilde{\mathbf{c}} + t_1(i) + t_2(j) \in A_\epsilon^{(n)}(X_1 + X_2)$. If such $\tilde{\mathbf{c}}$ is found, then $\tilde{\mathbf{c}} + t_1(i) + t_2(j)$ is declared as a reconstruction of $\mathbf{x}_1 + \mathbf{x}_2$. An error event E_d occurs, if no unique $\tilde{\mathbf{c}}$ was found.

Using standard arguments for large enough n, we can ignored the event in which $\mathbf{x}_1$ and $\mathbf{x}_2$ are not typical. Note that the event E_i is the same as the interested event in Lemma 3, where $\hat{X} = X = X_i$ with probability one, $\mathcal{C}_{out} = \mathcal{C}_i$, $R_{bin} = R_i$, $\mathcal{C} = \mathcal{C}_{in,i}$ and $R = R_{in,i}, i = 1, 2$. Therefore, applying Lemma 3, $\mathcal{C}_1$ and $\mathcal{C}_2$ need to satisfy (7). Using Lemma 2, we can show that $P(E_d) \rightarrow 0$ as $n \rightarrow \infty$, if the bounds in (6) are satisfied with $Y = \emptyset, X = X_1 + X_2$ and $\mathcal{C} = \mathcal{C}_{1,in} + \mathcal{C}_{2,in}$. Using the above argument, and noting that the effective transmission rate of the ith encoder is R_i, we can derive the bounds in (8). The cardinality bound on $\mathcal{Q}$ and the complete proof are provided in [12]. ■

Since every linear code, group code and transversal group code is a QGC, their achievable rates are included in the rate region characterized in (8). We show, through the following example, that UQGC's improves upon the previously known schemes.

Example 1. 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	$0.1\delta_N$	$0.9\delta_N$	$0.1(1-\delta_N)$	$0.9(1-\delta_N)$

Using standard unstructured codes, the rates $R_1 + R_2 \geq H(X_1, X_2)$ are achievable. As is shown in [9], group codes in this example outperform linear codes. The largest achievable region using group codes is $R_j \geq \max\{H(Z), 2H(Z|[Z]_1)\}, \quad j = 1, 2$, where $Z = X_1 + X_2$. It is shown in [11] that using transversal group codes the rates

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

are achievable. An achievable rate region using UQGC's can be obtained from Theorem 1. Let Q be a trivial random variable and set $P(W_1 = 0) = P(W_2 = 0) = 0.95$ and $P(W_1 = 1) = P(W_2 = 1) = 0.05$. As a result one can verify that the following is achievable:

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

Let $\delta_N = 0.6$. In this case, using unstructured codes the rate $R_i \approx 1.72$ is achievable, using group codes $R_i \approx 1.94$ is achievable, using transversal group codes $R_i \approx 1.69$ is achievable. Whereas, $R_i \approx 1.67$ is achievable using UQGC's.

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. Figure 1 depicts an example of this problem. 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. The definition of a code for computation over MAC and an achievable rate are given in Definition 3 and 4, respectively. Applications of this problem are in various multi-user communication setups such as interference and broadcast channels.

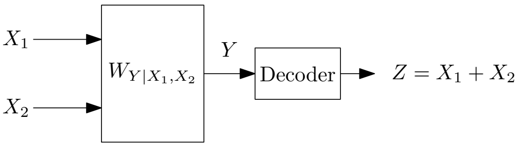

Fig. 1. Computation over a two-users MAC.

For the above setup, we use quasi group codes to derive an achievable rate region.

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

$$R_i \leq \frac{H(W_i|Q)}{H(W|[W]_s, Q)} I(X_1 + X_2; Y|[X_1 + X_2]_s), \qquad (9)$$

where $0 \leq s \leq r-1$, $i = 1, 2$, X_1 *and* X_2 *are independent and uniform over* $\mathbb{Z}_{p^r}$, $W = W_1 + W_2$, *and* $W_1 - Q - W_2$ *holds. Moreover, having* $|\mathcal{Q}| \leq r$ *is sufficient to achieve the above bounds.*

Outline of the proof:

Codebook Generation: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two $(n, m, k_1, k_2, \ldots, k_m)$ QGC with identical matrices and independent random variables. Suppose the translations are chosen randomly, independently and uniformly over $\mathbb{Z}_{p^r}^n$. Let the elements of the matrices be chosen randomly and uniformly over $\mathbb{Z}_{p^r}$. Index all the codewords in each codebooks.

Encoding: Upon receiving a message index θ_j, encoder j sends the corresponding codeword in $\mathcal{C}_j$, where $j = 1, 2$. Suppose the output of encoder j is $\mathbf{x}_j, j = 1, 2$.

Decoding: Upon receiving $\mathbf{y}$ from the channel, the decoder wishes to decode $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$. It finds $\tilde{\mathbf{x}} \in \mathcal{C}_1 + \mathcal{C}_2$ such that $\tilde{\mathbf{x}}$ and $\mathbf{y}$ are jointly typical with respect to the distribution $P_{X_1+X_2,Y}$, where X_1 and X_2 are independent and uniform over $\mathbb{Z}_{p^r}$. An error event E is declared, if no unique $\tilde{\mathbf{x}}$ was found.

Note that by Lemma 1, $\mathcal{C}_1 + \mathcal{C}_2$ is a QGC. Using Lemma 2, we can show that $P(E) \to 0$ as $n \to \infty$, if the bounds in (6) hold, where $X = X_1 + X_2$ and $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. Multiply both sides of this bound by $\frac{\log|\mathcal{C}_i|}{\log|\mathcal{C}_1+\mathcal{C}_2|}$. This in turn implies (9), where $P(Q = q)$ is a rational number and $R_i = \frac{1}{n}\log|\mathcal{C}_i|$. The complete proof is provided in [12]. ■

We show, through the following example, that using QGC one can improve upon the previously known schemes.

Example 2. Consider the MAC described by $Y = X_1 \oplus X_2 \oplus N$, 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 $0 \leq \delta_N \leq 1$.

Using standard unstructured codes the rates satisfying $R_1 + R_2 \leq I(X_1 X_2; Y)$ are achievable. It is shown in [9] that the largest achievable region using group codes is $R_i \leq \min\{I(Z;Y), 2I(Z;Y|[Z]_1)\}$, where $Z = X_1 + X_2$ and X_1 and X_2 are uniform over $\mathbb{Z}_4$. It is shown in [11] that transversal group codes achieve

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

Using Theorem 2, QGC's achieve

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

This can be shown by setting Q to be a trivial random variable, $P(W_1 = 0) = P(W_2 = 0) = 0.95$ and $P(W_1 = 1) = P(W_2 = 1) = 0.05$.

Let $\delta_N = 0.6$. Then $R_i \approx 0.28$ is achievable using unstructured codes, $R_i \approx 0.06$ 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 QGC's.

VI. Conclusion

The problem of computing modulo prime-power was considered. A new layered ensemble of structured codes called QGC was introduced. We investigated the performance limits of these codes in distributed source coding and computation over MAC. Achievability results using these codes were provided for both settings. We showed that the application of QGC's 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 Trans. on Inf. 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 Inf. 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. on Inf. Theory, vol. 55, pp. 2442-2454, June 2009.

[4] B. Nazer and M. Gastpar, "Computation over multiple-access channels," IEEE Trans. on Inf. Theory, vol. 53, no. 10, pp. 3498-3516, Oct. 2007.

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

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

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

[8] G. Como and F. Fagnani, "The capacity of finite abelian group codes over symmetric memoryless channels", IEEE Trans. on Inf. Theory, vol. 55, no. 5, pp. 2037-2054, May 2009.

[9] A.G. Sahebi, S.S. Pradhan, "Abelian group codes for channel coding and source coding," IEEE Trans. on Inf. 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," 50th Annual Allerton Conf. on Communication, Control, and Computing (Allerton), pp. 2068-2074, Oct. 2012.

[11] M. Heidari, F. Shirani and S. S. Pradhan, "Beyond group capacity in multi-terminal communications," IEEE International Symposium on Inf. Theory (ISIT), Hong Kong, pp. 2081-2085, July 2015.

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