On the Achievable Rates of Sources having a Group Alphabet in a Distributed Source Coding Setting

K. Vinodh, V. Lalitha, N. Prakash, P. Vijay Kumar
Dept. of ECE
Indian Institute of Science
Bangalore - 560012, India
Email: {kvinodh, lalitha, prakashn, vijay}@ece.iisc.ernet.in.

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

***Abstract*—We consider the problem of compression via homomorphic encoding of a source having a group alphabet. This is motivated by the problem of distributed function computation, where it is known that if one is only interested in computing a function of several sources, then one can at times improve upon the compression rate required by the Slepian-Wolf bound. The functions of interest are those which could be represented by the binary operation in the group.**

We first consider the case when the source alphabet is the cyclic Abelian group, Z_{p^r}. In this scenario, we show that the set of achievable rates provided by Krithivasan and Pradhan [1], is indeed the best possible. In addition to that, we provide a simpler proof of their achievability result. In the case of a general Abelian group, an improved achievable rate region is presented than what was obtained by Krithivasan and Pradhan.

We then consider the case when the source alphabet is a non-Abelian group. We show that if all the source symbols have non-zero probability and the center of the group is trivial, then it is impossible to compress such a source if one employs a homomorphic encoder.

Finally, we present certain non-homomorphic encoders, which also are suitable in the context of function computation over non-Abelian group sources and provide rate regions achieved by these encoders.

I. Introduction

Let X_1 and X_2 be two non-collocated sources having the same finite alphabet $\mathcal{X}$ and joint distribution $P_{X_1X_2}$ and let the receiver be interested in computing the function, $f(X_1, X_2)$. Using Slepian-Wolf compression [2], one can achieve lossless compression at a sum rate $H(X_1, X_2)$. Now, consider the case when the function can be embedded within a group, i.e., it is possible to associate with every element in the source alphabet, an element in a finite group G such that $f(x_1, x_2) = g \circ h$, where $g, h \in G$ and where multiplication is carried out in the group G. The use of homomorphic encoders permits one to compress the function $f(x_1, x_2)$ by compressing the individual sources. A homomorphic encoder is an encoder employing a mapping ϕ where ϕ is a group homomorphism, i.e., $\phi(g \circ h) = \phi(g) \circ \phi(h)$. Thus, by compressing g, h using separate homomorphic encoders ϕ at the two sources and having the receiver compute the product $\phi(g) \circ \phi(h)$, we have in effect achieved distributed compression of the function $f(x_1, x_2)$. Note that for greatest efficiency the homomorphic encoder ϕ is chosen based on the distribution of $f(X_1, X_2)$. For a large class of groups, we can achieve a sum rate, that for certain distributions, improves upon the Slepian-Wolf bound, by using such a homomorphic encoder [1]. We begin with a few examples.

1) Modulo two sum of sources [3]: Let the alphabet $\mathcal{X} = \{0, 1\}$ and let the function that needs to be computed be $f(x_1, x_2) = (x_1 + x_2) \mod 2$. The function in this case is naturally embedded in the group $G = \mathbb{Z}_2$, the set of integers modulo two. Assume the sources to have joint distribution given by $P(0, 0) = P(1, 1) = p/2, P(0, 1) = P(1, 0) = (1-p)/2,\ 0 < p < 1/2$. In this case, the sum rate required using Slepian-Wolf encoding would equal $H(X_1, X_2) = 1 + h(p)$. But if the compression is done homomorphically, then the required sum rate equals $2h(p)$ which is less than $H(X_1, X_2)$ for $0 < p < \frac{1}{2}$. It is shown in [3] that this sum rate is indeed optimal for the given source distribution.

2) Modulo four sum of sources: Let $\mathcal{X} = \{0, 1, 2, 3\}$ and $f(x_1, x_2) = (x_1 + x_2) \mod 4$. Though the function could be naturally embedded in the group $\mathbb{Z}_4$, we will now show how to embed the function f in the group $\mathbb{Z}_3 \times \mathbb{Z}_2$ which at times leads to better sum rates than the natural embedding. Let $x_1, x_2 \in \mathbb{Z}_4$. Then x_1 and x_2 can be written as $x_1 = \alpha + 2\beta$ and $x_2 = \gamma + 2\delta$, where $\alpha, \beta, \gamma, \delta \in \{0, 1\}$. Then, $(x_1 + x_2) \mod 4$ could be recovered from $(\alpha + \gamma) \mod 3$ and $(\beta + \delta) \mod 2$, which could be embedded in $\mathbb{Z}_3$ and $\mathbb{Z}_2$ respectively. Thus, $f(x_1, x_2)$ can be embedded in $\mathbb{Z}_3 \times \mathbb{Z}_2$.

3) Product of matrices over a finite field: Consider the case where the alphabet $\mathcal{X} = GL_2(\mathbb{F}_q)$, the set of 2×2 invertible matrices over the finite field $\mathbb{F}_q$. Let $f(x_1, x_2) = x_1x_2$, matrix multiplication over $\mathbb{F}_q$. In this example also, the function is naturally embedded in the non-Abelian group $G = GL_2(\mathbb{F}_q)$. Even here, many distributions exists in which homomorphic encoding improves upon Slepian-Wolf encoding.

4) Average of two sources: Let the source alphabet $\mathcal{X} = \{0, \ldots, M\}$ and the function of interest is the average of 2 sources, i.e., $f(x_1, x_2) = \frac{1}{2}(x_1 + x_2)$. Here f could be embedded in the group $\mathbb{Z}_q$, where q is a prime greater than $2M$. For example, let $\mathcal{X} = \{0, 1\}$ and $f(x_1, x_2) = (x_1 + x_2)/2$. The function $g(x_1, x_2) = 2f(x_1, x_2)$ can be embedded into

$\mathbb{Z}_3$. The receiver first recovers $g(x_1, x_2)$ and divide it by a factor of 2 to obtain $f(x_1, x_2)$.

Notation: $X^n = (X_1, \ldots, X_n)$ will denote an $n-$length random vector, while boldface $\mathbf{x}$ will denote its realization.

II. System Model For Homomorphic Compression

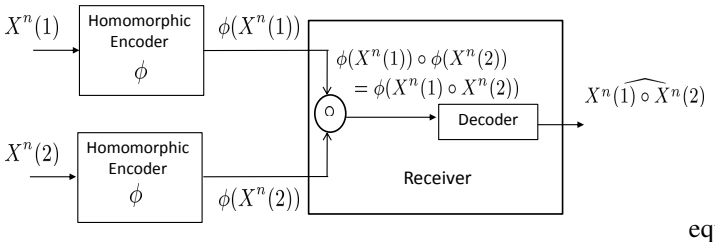


Fig. 1. System model for function computation

We consider a distributed compression problem (See Fig 1) involving two correlated but memoryless sources and a receiver that is only interested in computing a function of the two sources, in a lossless manner. We assume further that homomorphic encoders are employed, unless stated otherwise. Though the system model will be described for two sources, it can be directly extended to any number of sources. The source alphabet is assumed to be a finite group $(G, \circ)$, where $\circ$ denotes the binary operation in the group. Let $X^n(i)$ denote the random variables corresponding to an $n-$length output sequence of the i^{th} source, $i = 1, 2$. The sequence $(X^n(1), X^n(2))$ is assumed to be i.i.d $\sim P_{X(1)X(2)}$. The function that needs to be computed at the receiver is $X^n = X^n(1) \circ X^n(2)$, in which the multiplication is carried out component wise in the group G.

Encoder : Since we restrict our attention to homomorphic encoders, encoding of both sources is carried out using the group homomorphism $\phi^{(n)}$,

$$\phi^{(n)} : G^n \quad \longrightarrow \quad \bar{G} \ , \tag{1}$$

where $\bar{G}$ denotes the codomain of the homomorphism. For example, $\bar{G}$ could be G^k, where $k = \alpha n, 0 \leq \alpha \leq 1$. Here α may be viewed as a crude measure of the amount of compression taking place for large n. Let $\phi^{(n)}(X^n(1))$ and $\phi^{(n)}(X^n(2))$ denote the output of the two encoders.

Receiver : Since the function of interest corresponds to the multiplication of two elements in the group, the first step taken by the receiver is to multiply the outputs of the two encoders to obtain

$$\begin{aligned} \phi^{(n)}(X^n(1)) \circ \phi^{(n)}(X^n(2)) &\overset{(a)}{=} \phi^{(n)}(X^n(1) \circ X^n(2)) \\ &= \phi^{(n)}(X^n), \end{aligned} \tag{2}$$

where (a) follows since $\phi^{(n)}$ is a homomorphism. The input to the decoder is $\phi^{(n)}(X^n)$ and let $\hat{X}^n$ denote its output. Let $P_e^{(n)}$ denote the probability of error, averaged over all source symbols i.e., $P_e^{(n)} = P(X^n \neq \hat{X}^n)$.

The multiplication taking place in the receiver allows one to consider an equivalent system model (see Fig. 2), wherein a discrete memoryless source (DMS), with the alphabet G, produces the product $X^n(1) \circ X^n(2) = X^n$, i.i.d. $\sim P_X$ where

$$P_X(x) = \sum_{x(1), x(2) : x(1) \circ x(2) = x} P_{X(1)X(2)}(x(1), x(2)). \tag{3}$$

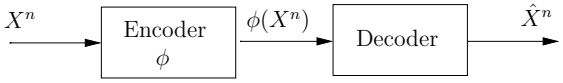


Fig. 2. Equivalent single source system model

Since the probability of error in recovering X^n in the equivalent model is the same as the probability of error in computing the product function $X^n(1) \circ X^n(2)$ in the original model, it suffices to consider homomorphic encoding of the single source X. Hence, from now on we will work with this equivalent system model.

Rate: The rate of the encoder $\phi^{(n)}$ (in bits per symbol) is given by

$$R^{(n)} \quad = \quad \frac{\log_2 |\text{Im}(\phi^{(n)})|}{n} \ , \tag{4}$$

where $\text{Im}(\phi^{(n)})$ denotes the image of the map $\phi^{(n)}$.

Achievability A rate R is said to be achievable, if for any $\delta > 0, \ \epsilon > 0$, there exists a sequence of homomorphisms $\{\phi^{(n)}\}$ such that for every sufficiently large n, $R^{(n)} < R + \delta$ and $P_e^{(n)} \leq \epsilon$. The *achievable rate region* is the closure of set of all achievable rates.

It follows from our definition of rates that if R is achievable for the source X in the equivalent system model, then the rate pair (R, R) is achievable in the original system model.

III. Compression of Abelian groups

The *Primary Decomposition Theorem* [4] states that any finite Abelian group G is isomorphic to the direct product of primary cyclic groups, i.e., $G \ \cong \ \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_\ell^{r_\ell}}$,where p_i is prime, $r_i \geq 1, \ 1 \leq i \leq \ell$. Hence, without loss of generality, we will assume that G has this structure. In [1] a homomorphic coding scheme is presented for any Abelian group. In this section, we first show that when $\ell = 1$, i.e., $G = \mathbb{Z}_{p^r}$, the rate region of the coding scheme presented in [1] is indeed the best possible. We will then go on to present a new homomorphic coding scheme for Abelian groups for the case $\ell > 1$ and show that its rate region improves upon the rate region of the scheme in [1].

A. Abelian groups of the form $\mathbb{Z}_{p^r}$ ($\ell = 1$)

Here, the source alphabet G, is assumed to be the finite cyclic group $\mathbb{Z}_{p^r}$, where p is a prime and $r > 0$. The binary operation $\circ$ will be denoted by $+$. The groups, $p^i\mathbb{Z}_{p^r}, 0 \leq i \leq r$, form the additive subgroups of $\mathbb{Z}_{p^r}$. The subgroup $p^i\mathbb{Z}_{p^r}$ is isomorphic to $\mathbb{Z}_{p^{r-i}}$. The quotient group $\mathbb{Z}_{p^r}/p^i\mathbb{Z}_{p^r}$, comprised of the cosets of $p^i\mathbb{Z}_{p^r}$ in $\mathbb{Z}_{p^r}$, is isomorphic to $\mathbb{Z}_{p^i}$ and hence, we will identify $\mathbb{Z}_{p^i}$ with the coset representatives

of $\mathbb{Z}_{p^r}/p^i\mathbb{Z}_{p^r}$. Define $[X]_i = X \bmod p^i$ and let $P_{[X]_i}$ denote the induced distribution on $[X]_i$. For example, if the group is $\mathbb{Z}_4$, then $[X]_1 \sim (P_X(0)+P_X(2), P_X(1)+P_X(3))$. Note that X and $[X]_i$ are jointly distributed according to

$$P_{X,[X]_i}(x,y) = \begin{cases} P_X(x) & \text{if } y = x \bmod p^i, \\ 0 & \text{else.} \end{cases} \quad (5)$$

Let $\psi_i^{(n)}$ be the restriction of $\phi^{(n)}$ to the subgroup $p^i\mathbb{Z}_{p^r}^n$, i.e.,

$$\psi_i^{(n)} = \phi^{(n)}|_{p^i\mathbb{Z}_{p^r}^n} : p^i\mathbb{Z}_{p^r}^n \longrightarrow \bar{G} , \quad (6)$$

We also define

$$R_{\psi_i}^{(n)} \triangleq \frac{\log\left|\mathrm{Im}(\psi_i^{(n)})\right|}{n} . \quad (7)$$

From now on, wherever unambiguous, we will shall use ϕ, ψ_i and P_e in place of $\phi^{(n)}, \psi_i^{(n)}$ and $P_e^{(n)}$ respectively.

Theorem 1: For the source X drawn i.i.d. $\sim P_X$ and whose alphabet is $\mathbb{Z}_{p^r}$, the *achievable rate region* under homomorphic encoding is given by

$$R \geq \max_{0\leq i<r} \left(\frac{r}{r-i}\right)(H(X) - H([X]_i)) . \quad (8)$$

The achievability of the above theorem is shown in [1] (See Section 7.1) by a random averaging argument over the set of all homomorphisms of the form

$$\phi : \mathbb{Z}_{p^r}^n \longrightarrow \mathbb{Z}_{p^r}^k . \quad (9)$$

We provide a proof of the converse. We begin with a few lemmas.

Lemma 2:

$$H(X|[X]_i) = H(X) - H([X]_i) . \quad (10)$$

Proof: The proof follows from noting that

$$H(X) = H(X,[X]_i) = H([X]_i) + H(X|[X]_i) . \quad (11)$$

□

In light of the above lemma, the *achievable rate region* in Theorem 1 can be rewritten in the form

$$R \geq \max_{0\leq i<r} \left(\frac{r}{r-i}\right) H(X|[X]_i) . \quad (12)$$

This simple observation, nevertheless, turns out to be an important ingredient in our proof of Theorem 1. Henceforth, we will use (12) in place of (8) to indicate the *achievable rate region* of Theorem 1.

Lemma 3: Let $\phi : \mathbb{Z}_{p^r}^n \longrightarrow \bar{G}$ be a homomorphism. Then there exists a second homomorphism $\bar{\phi} : \mathbb{Z}_{p^r}^n \longrightarrow \mathbb{Z}_{p^r}^k$, for some $k > 0$, such that $\mathrm{Ker}(\phi) = \mathrm{Ker}(\bar{\phi})$.

Proof: See Appendix A. □

Since the kernel of a homomorphic encoder determines both its rate as well as the probability of error, we replace the codomain $\bar{G}$ in (1) by $\mathbb{Z}_{p^r}^k$.

The next lemma is central to our proof of the converse.

Lemma 4: Let $\phi : \mathbb{Z}_{p^r}^n \longrightarrow \mathbb{Z}_{p^r}^k$ be a group homomorphism. Let $\psi_i,\ 0 \leq i < r$, be restriction of ϕ to the subgroup $p^i\mathbb{Z}_{p^r}^n$. Then,

$$\log|\mathrm{Im}(\psi_i)| \leq \left(\frac{r-i}{r}\right)\log|\mathrm{Im}(\phi)|,\ 0 \leq i < r. \quad (13)$$

Proof: The proof essentially uses linear algebra over rings. See Appendix B for details. □

Remark 1: It should be noted that every group homomorphism $\phi : \mathbb{Z}_{p^r}^n \longrightarrow \mathbb{Z}_{p^r}^k$ is also a module homomorphism, when $\mathbb{Z}_{p^r}^n$ is considered as a module over $\mathbb{Z}_{p^r}$. In this context, it is worth noting that the result in Lemma 4 is not necessarily true in the case of vector space homomorphisms. For example, let $\phi : \mathbb{F}_{p^r}^n \longrightarrow \mathbb{F}_{p^r}^k$ be a vector space homomorphism, where $\mathbb{F}_{p^r}$ is a finite field of p^r elements and r is even. Let $\mathbb{F}_{p^s},\ s = \frac{r}{2}$ be a subfield of $\mathbb{F}_{p^r}$. Let ψ be the restriction of ϕ to $\mathbb{F}_{p^s}^n$. Let A be the matrix $[I_k\ \gamma I_k]$ where $\gamma \in \mathbb{F}_{p^r}\backslash\mathbb{F}_{p^s}$ and let ϕ be the homomorphism whose matrix is A. Then, it is not hard to verify that $|\mathrm{Im}(\phi)| = |\mathrm{Im}(\psi)| = p^{rk}$.

Proof of Theorem 1

As noted above, it is sufficient to prove the converse. The proof of the converse follows by contradiction. Suppose,

$$R < \max_{0\leq i<r} \left(\frac{r}{r-i}\right) H(X|[X]_i) . \quad (14)$$

is achievable. This implies that there exists a sequence of maps $\{\phi^{(n)} : \mathbb{Z}_{p^r}^n \longrightarrow \mathbb{Z}_{p^r}^k\}$, and decoders $\{D^n\}$, such that for some i, say i_0, for every sufficiently large n,

$$R^{(n)} < \left(\frac{r}{r-i_0}\right) H(X|[X]_{i_0}) , \quad (15)$$

and $P_e^n \to 0$. Consider now, the restriction of $\phi^{(n)}$ to the subgroup $p^{i_0}\mathbb{Z}_{p^r}^n$, i.e., $\psi_{i_0}^{(n)}$. Then, from Lemma 4 and our definition of rates we have,

$$R_{\psi_{i_0}}^{(n)} \leq \left(\frac{r-i_0}{r}\right) R^{(n)} . \quad (16)$$

Substituting (15) in (16), we get

$$R_{\psi_{i_0}}^{(n)} < H(X|[X]_{i_0}) . \quad (17)$$

We will now show that this is not possible. Consider a second system, as shown in Fig. 3. In this system, $X^n - [X]_{i_0}^n$ is encoded with the map $\psi_{i_0}^{(n)}$ and $[X]_{i_0}^n$ is given as the side information to the receiver. The receiver first reconstructs $\phi^{(n)}(X^n)$ and uses the decoder D^n to decode X^n from $\phi(X^n)$ and hence, this system has the same error performance as the original system. Thus, this system recovers X^n with arbitrarily low probability of error at a rate less than $H(X|[X]_{i_0})$. However, for any system with X as the input to its encoder and $[X]_{i_0}$ as side information at its decoder, any achievable rate has to be at least equal to $H(X|[X]_{i_0})$, which contradicts the existence of the new system and hence (14).

□

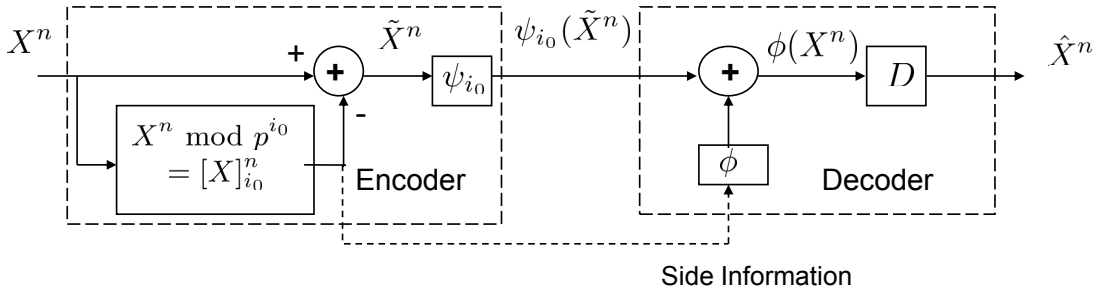


Fig. 3. An alternate system that aids in the proof of Theorem 1

B. Abelian groups of the form $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_l^{r_\ell}}$

So far, we have been focusing on the compression of the Abelian group $\mathbb{Z}_{p^r}$. In this section, we provide achievable rates for the Abelian group $G = \mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_l^{r_\ell}}$. For simplicity, we restrict the discussion to the case when the group has only two components, i.e. groups of the form $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}}$. Let $X = (X^{(1)}, X^{(2)})$ be a random variable on G, distributed according to $P_X = P_{X^{(1)}X^{(2)}}$. Also let $[X^{(1)}]_i = X^{(1)} \bmod p_1^i,\ 0 \leq i \leq r_1$ and $[X^{(2)}]_j = X^{(2)} \bmod p_2^j,\ 0 \leq j \leq r_2$. We first briefly describe a homomorphic achievable scheme (which we term scheme $\mathcal{A}$) presented in [1]. Let ϕ_1 and ϕ_2 be homomorphisms on $\mathbb{Z}^n_{p_1^{r_1}}$ and $\mathbb{Z}^n_{p_2^{r_2}}$, respectively, i.e.,

$$\phi_1 : \mathbb{Z}^n_{p_1^{r_1}} \to \mathbb{Z}^{k_1}_{p_1^{r_1}} \quad , \quad \phi_2 : \mathbb{Z}^n_{p_2^{r_2}} \to \mathbb{Z}^{k_2}_{p_2^{r_2}}. \tag{18}$$

From ϕ_1 and ϕ_2, we construct the homomorphic encoder, ϕ, as

$$\begin{aligned} \phi : \mathbb{Z}^n_{p_1^{r_1}} \times \mathbb{Z}^n_{p_2^{r_2}} &\longrightarrow \mathbb{Z}^{k_1}_{p_1^{r_1}} \times \mathbb{Z}^{k_2}_{p_2^{r_2}} \\ (\mathbf{x}^{(1)}, \mathbf{x}^{(2)}) &\rightsquigarrow (\phi_1(\mathbf{x}^{(1)}), \phi_2(\mathbf{x}^{(2)})). \end{aligned} \tag{19}$$

The decoder is assumed to be a successive reconstruction decoder which first decodes $X^{(1)}$ from $\phi_1(\mathbf{x}^{(1)})$ and then decodes $X^{(2)}$ from $\phi_2(\mathbf{x}^{(2)})$, assuming that $X^{(1)}$ has already been successfully decoded. Let R_i be the rate required to encode $X^{(i)},\ i = 1, 2$. The rate region of this scheme is given by

$$\begin{aligned} \mathcal{R}_A &= \{ \quad R_1 + R_2, \\ R_1 &\geq \max_{0 \leq i < r_1} \left(\frac{r_1}{r_1 - i} \right) H(X^{(1)} | [X^{(1)}]_i), \\ R_2 &\geq \max_{0 \leq j < r_2} \left(\frac{r_2}{r_2 - j} \right) H(X^{(2)} | [X^{(2)}]_j, X^{(1)}) \Big\}. \end{aligned} \tag{20}$$

The rate region $\mathcal{R}_A$ can be shown to be achieved by reworking Theorem 1, to take into account the presence of side information at the decoder. The performance of this scheme certainly depends on the order in which the components are decoded and hence, one to needs to further optimize over all possible orderings to obtain the best achievable rate. The rate region for the best ordering is same as (20) with appropriate changes in the constraints. Note that if every component had a field structure, i.e. if $r_j = 1,\ \forall j$, this scheme is indeed optimal and the rate region is invariant to the order of decoding. This is due to the fact that if one decodes $X^{(1)}$ first, the rates $R_1 = H(X^{(1)})$ and $R_2 = H(X^{(2)}|X^{(1)})$ are achievable, whereas if one decodes $X^{(2)}$ first, $R_2 = H(X^{(2)})$ and $R_1 = H(X^{(1)}|X^{(2)})$ are achievable. In both cases $R_1 + R_2 = H(X^{(1)}, X^{(2)})$.

1) An Improved Rate Region: We now present a second homomorphic scheme (termed scheme $\mathcal{B}$) which improves upon the rate region of scheme $\mathcal{A}$. We use the same encoder structure given by (19) in Scheme $\mathcal{B}$. The receiver jointly decodes $(\mathbf{x}^{(1)}, \mathbf{x}^{(2)})$ from $(\phi_1(\mathbf{x}^{(1)}), \phi_2(\mathbf{x}^{(2)}))$.

Theorem 5: Consider a source $X = (X^{(1)}, X^{(2)})$ drawn i.i.d $\sim P_X = P_{X^{(1)}X^{(2)}}$ and whose alphabet is $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}}$. Then using homomorphisms for compression, the set of rates given by

$$\begin{aligned} \mathcal{R}_B \quad = \quad & \Bigg\{ \bar{R}_1 + \bar{R}_2 \Bigg| \frac{r_1 - i}{r_1} \bar{R}_1 + \frac{r_2 - j}{r_2} \bar{R}_2 \geq H\left(X | [X]_{ij}\right), \\ & 0 \leq i \leq r_1, 0 \leq j \leq r_2 \Bigg\} \end{aligned} \tag{21}$$

is achievable, where $[X]_{ij} = ([X^{(1)}]_i, [X^{(2)}]_j)$. If $p_1 \neq p_2$, then $\mathcal{R}_\mathcal{B}$ is precisely the *achievable rate region*.

Proof: Please see Appendix C for a proof of the achievability. We omit the proof of converse. □

2) Comparison of Rate Regions, $\mathcal{R}_A$ and $\mathcal{R}_B$: We now show that $\mathcal{R}_A \subsetneq \mathcal{R}_B$. Let $R = R_1 + R_2 \in \mathcal{R}_A$ where R_1 and R_2 satisfy the constraints in (20). Combining the two constraints, we get

$$\left(\frac{r_1 - i}{r_1} \right) R_1 + \left(\frac{r_2 - j}{r_2} \right) R_2 \tag{22}$$

$$\geq H(X^{(1)} | [X^{(1)}]_i) + H(X^{(2)} | [X^{(2)}]_j, X^{(1)}) \tag{23}$$

$$\geq H(X | [X]_{ij}), \quad \forall\ 0 \leq i \leq r_1,\ 0 \leq j \leq r_2, \tag{24}$$

which implies $R \in \mathcal{R}_B$ and hence $\mathcal{R}_A \subseteq \mathcal{R}_B$. Note that this containment is true independent of the ordering of the components of the group, G.

In order to show that $\mathcal{R}_A \subsetneq \mathcal{R}_B$, consider the example where $G = \mathbb{Z}_3 \times \mathbb{Z}_4$ with the distribution

$$P_{X^{(1)}, X^{(2)}} = \begin{bmatrix} 0.1342 & 0.0687 & 0.0645 & 0.0628 \\ 0.0327 & 0.1260 & 0.0026 & 0.0870 \\ 0.0858 & 0.1077 & 0.1161 & 0.1119 \end{bmatrix},$$

where $X^{(1)}$ and $X^{(2)}$ are random variables over alphabets $\mathbb{Z}_3$ and $\mathbb{Z}_4$, respectively. Using scheme $\mathcal{A}$, the best sum rate is achieved by first decoding $X^{(2)}$ and then decoding $X^{(1)}$. In this case, $R_2 = 1.9798$, $R_1 = 1.4133$ and $R_A = R_1 + R_2 = 3.3931$. Using scheme $\mathcal{B}$, it can be seen after some calculations that $\bar{R}_1 = 1.4885$ and $\bar{R}_2 = 1.9028$ satisfy all the constraints in (21) of Theorem 5. Thus the sum rate achieved in this case is $R_B = \bar{R}_1 + \bar{R}_2 = 3.3913 < R_A$, which proves $\mathcal{R}_A \subsetneq \mathcal{R}_B$. In fact, as noted in Theorem 5 whenever $p_1 \neq p_2$, $\mathcal{R}_B$ is indeed the *achievable rate region*.

The improvement in the homomorphic compression rates directly translates to improvement in achievable sum rates in function computation, under the original system model in Fig 1.

IV. Compression of non-Abelian groups

Unlike in the case of Abelian groups, it is not at all clear that any homomorphic compression is possible in the case of a general non-Abelian group. We say compression is possible if a rate less than $\log_2|G|$ is achievable. We begin with an investigation into the possibility of compression under a homomorphic encoder ϕ. We obtain two necessary conditions for compression to be possible:

1) the map ϕ when restricted to any finite set of input co-ordinates must represent an isomorphism of groups and
2) the compression rate must satisfy the lower bound:

$$R \geq \log_2 \frac{|G|}{|\mathcal{Z}(G)|}. \tag{25}$$

It follows from the second condition that homomorphic source compression is not possible in the case of non-Abelian groups G having a trivial center $\mathcal{Z}(G)$. For the case when the group does possess a non-trivial center $\mathcal{Z}(G)$, we divide the discussion into two cases. In the first case, the group G is assumed to be the direct product $G = P \times Q$ of an Abelian group P and a non-Abelian group Q. Here we show that compression is indeed possible using a homomorphic encoder. In the second case, when such a decomposition is not possible, we show how one can achieve compression by making use of an encoder that is "almost" homomorphic. Both these compression techniques, though will be discussed only in the context of two sources, can be extended to any finite number of sources. Finally, we give a third compression strategy, also non-homomorphic, which is applicable only for a two source setting, but provides compression even when $\mathcal{Z}(G)$ is trivial.

We begin by describing certain properties of the homomorphic encoder.

A. Properties of the encoder

Consider the homomorphic encoder described in (1). Let ϕ_i be the restriction of ϕ to the i^{th} copy of G, i.e.

$$\phi_i = \phi|_{1\times\ldots\times G_i\times\ldots\times 1}\colon G_i \twoheadrightarrow \bar{G}_i, \tag{26}$$

with $\bar{G}_i = \text{Im}(\phi_i)$ and $G_i = G,\ \forall i$. Then for any $\mathbf{y} \in G^n$, we have

$$\phi(\mathbf{y}) = \prod_{i=1}^{n} \phi(y(i)). \tag{27}$$

Property 1: $\forall i, j, i \neq j,\ \bar{G}_i, \bar{G}_j$ commute element-wise; i.e. $\bar{g}_i \circ \bar{g}_j = \bar{g}_j \circ \bar{g}_i,\ \bar{g}_i \in \bar{G}_i,\ \bar{g}_j \in \bar{G}_j$. This follows from the fact that the groups $1 \times \ldots \times G_i \times \ldots \times 1$ and $1 \times \ldots \times G_j \times \ldots \times 1$ commute element-wise and hence the same holds for their homomorphic images.

Property 2: $\text{Im}(\phi) = \prod_{i=1}^{n} \bar{G}_{\pi(i)}$ where π is any permutation of $\{1, 2, \ldots, n\}$. This follows from (27) and Property 1.

Property 3: If $\mathcal{I}, \mathcal{J} \subseteq \{1, \ldots, n\}$ such that $\mathcal{I} \cap \mathcal{J}$ is the null set, then

$$\prod_{i\in\mathcal{I}} \bar{G}_i \bigcap \prod_{j\in\mathcal{J}} \bar{G}_j = \mathcal{Z}\left(\prod_{i\in\mathcal{I}} \bar{G}_i\right) \bigcap \mathcal{Z}\left(\prod_{j\in\mathcal{J}} \bar{G}_j\right). \tag{28}$$

This follows from Property 1.

B. Necessary conditions for compressibility

Theorem 6: Consider the subgroup K of G^n, where $K = 1 \times \ldots \times G_{i_1} \times \ldots \times G_{i_2} \times \ldots \times G_{i_r} \times \ldots \times 1$, with $1 \leq i_1 < i_2 < \ldots < i_r \leq n$. If r is finite, then for large n, the restriction of ϕ to K must necessarily be an isomorphism for compression to be possible assuming a homomorphic encoder if all the source symbols have non-zero probability.

Proof: We will prove the Theorem for the case when $r = 1$ and the case of a general finite r can be proved along similar lines. The proof proceeds via the method of contradiction. Without loss of generality, assume $K = G_1 \times 1 \times \ldots 1$. Let $\bar{G}_1 \triangleq \text{Im}(\phi|_K)$. Assume $\phi^{(n)}|_K$ is not an isomorphism; which implies $\exists b (\neq 1_G) \in G$ such that $\phi|_K(b) = 1_{\bar{G}_1}$. Consider the sequence $\mathbf{a} = [b \ \ 1_G^{n-1}]$. Clearly, $\mathbf{a} \in \text{Ker}(\phi)$. Let the order of $\mathbf{a}$ in G^n be m which is same as the order of b in G. Let G^n be partitioned into cosets $C_i, 1 \leq i \leq \frac{|G|^n}{m}(\text{say} M)$ of the subgroup $(1, \mathbf{a}, \mathbf{a}^2, \ldots, \mathbf{a}^{m-1})$. All sequences $(\mathbf{x_i}, \mathbf{x_i} \circ \mathbf{a}, \mathbf{x_i} \circ \mathbf{a}^2, \ldots, \mathbf{x_i} \circ \mathbf{a}^{m-1})$ in a particular coset C_i have the same image under ϕ. Thus any decoder can decode only to one of the sequences in a coset C_i. Let $\hat{\mathbf{x}}_i$ denote the sequence with the maximum probability in the coset C_i and let $S_n = \{\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2, \ldots, \hat{\mathbf{x}}_M\}$. Then, under any decoder, $P_e^{(n)} \geq P(S_n^c)$. Also, since the sequences $\mathbf{x}_i$ and $\mathbf{x}_i \circ \mathbf{a}^j$ differ in only position and all source symbols are assumed to have non-zero probability, we have $P(\mathbf{x}_i \circ \mathbf{a}^j) \geq q\ P(\hat{\mathbf{x}}_i), 1 \leq j \leq m$ where q is the ratio of the minimum to the maximum probability of the source symbols. Hence,

$$P(S_n^c) \geq \sum_{i=1}^{M} q(m-1)P(\hat{\mathbf{x}}_i) = \beta P(S_n) = \beta(1 - P(S_n^c)),$$

where $\beta = q(m-1)$ and is independent of n. Combining the above facts, we obtain

$$P_e^{(n)} \geq P(S_n^c) \quad \geq \quad \frac{\beta}{1+\beta} > 0 \tag{29}$$

□

By setting $r = 1$ in Theorem (6), we get $\bar{G}_i \cong G,\ 1 \leq i \leq n$. We will make use of this fact below, where we establish the necessity of second condition appearing in (25).

Theorem 7: For a group G with center $\mathcal{Z}(G)$, compression rates less than $\log_2 \frac{|G|}{|\mathcal{Z}(G)|}$ cannot be achieved using homomorphic encoders. Specifically, if $\mathcal{Z}(G) = \{1_G\}$, no compression is possible.

Proof: Consider the homomorphic encoder given in (1). From property 2, the rate of the encoder $\phi^{(n)}$ in (1) is given by

$$R^{(n)} = \frac{\log_2|\prod_{i=1}^n \bar{G}_i|}{n}. \tag{30}$$

Using the fact that for any two subgroups A and B of a finite group, $|AB| = (|A|\,|B|)/(|A \cap B|)$, the cardinality of the image, $\prod_{i=1}^n \bar{G}_i$, of $\phi^{(n)}$ can be lower bounded as follows.

$$\begin{aligned}
\left|\prod_{i=1}^n \bar{G}_i\right| &= \frac{\left|\bar{G}_1\right|\left|\prod_{i=2}^n \bar{G}_i\right|}{\left|\bar{G}_1 \cap \prod_{i=2}^n \bar{G}_i\right|} && (31)\\
&= \frac{\left|\bar{G}_1\right|\left|\prod_{i=2}^n \bar{G}_i\right|}{\left|\mathcal{Z}(\bar{G}_1) \cap \mathcal{Z}(\prod_{i=2}^n \bar{G}_i)\right|} && (32)\\
&\geq \frac{\left|\bar{G}_1\right|\left|\prod_{i=2}^n \bar{G}_i\right|}{\left|\mathcal{Z}(\bar{G}_1)\right|} && (33)\\
&= \frac{|G|\left|\prod_{i=2}^n \bar{G}_i\right|}{|\mathcal{Z}(G)|} && (34)\\
&\geq \frac{|G|^n}{|\mathcal{Z}(G)|^{n-1}}\ , && (35)
\end{aligned}$$

where (32) follows from Property 3, (34) follows since, for compression to be possible, Theorem 6 implies that $\bar{G}_i \cong G,\ \forall i$. Combining equation (30) and (35), we get

$$R^{(n)} \geq \log_2 \frac{|G|}{|\mathcal{Z}(G)|} + \frac{1}{n}\log_2|\mathcal{Z}(G)|, \tag{36}$$

from which, using the definition of achievability of rate R, it can be shown that no rate less than $\log \frac{|G|}{|\mathcal{Z}(G)|}$ is achievable. □

Theorem (7) rules out homomorphic compression of many of the commonly known non-Abelian groups such as the dihedral-group, D_{2m}, for m odd, the symmetric group S_m, for $m \geq 3$, and the alternating group, A_m, for $m \geq 4$, and all non-abelian simple groups, since all of the above groups have trivial centers. See [4] for a discussion on these groups.

C. Achievable rates for non-Abelian groups

As noted in the start of this section, we will consider the following three compression schemes.

Case 1 : Here in this case, we consider the compression of non-Abelian group G that can be decomposed as a direct product of a non-Abelian and an Abelian group i.e., say G is decomposable as $G \cong B \times A$, where B is non-Abelian and A is Abelian. The proposed scheme is simple. The non-Abelian components are transmitted as such, while the Abelian components are compressed as discussed in Section III. Then an achievable rate of compression for the group G is given by $R = R_1 + R_2$, where $R_1 \geq \log|B|$ and R_2 is the achievable rate corresponding to the Abelian group A.

As an example, consider the distributed source compression scenario with two sources as in Figure 1. Let $G \cong B \times C_2$, where B is non-Abelian and C_2 is the cyclic group with two elements. The random variable $X_1 = (X_{1B}, X_{1C_2})$ and $X_2 = (X_{2B}, X_{2C_2})$. Let $X_{1B} \perp \{X_{1C_2}, X_{2B}, X_{2C_2}\}$ and $X_{2B} \perp \{X_{1C_2}, X_{1B}, X_{2C_2}\}$. Let both X_{1B} and X_{2B} be distributed as P_B. Let X_{1C_2} and X_{2C_2} be jointly distributed as in the first example of Section I; i.e. $P(0,0) = P(1,1) = p/2, P(0,1) = P(1,0) = (1-p)/2$. The function to be computed in the receiver is $y = x_1 \circ x_2 = (x_{1B}x_{2B}, x_{1C_2}x_{2C_2})$. The sum rate achieved using the above compression strategy is $2\log_2|B| + 2h(p)$. Slepian-Wolf coding for the same scenario would result in a sum rate $H(X_1, X_2) = 2H(P_B) + 1 + h(p)$. Clearly, if $2\log_2|B| + h(p) < 2H(P_B) + 1$, the distributed compression strategy using homomorphic encoders performs better than the Slepian-Wolf encoding method. Note that if P_B is uniformly distributed, this is always the case.

Case 2 : Here we show how compression is possible for any non-Abelian group possessing a non-trivial center (as opposed to requiring that it be the direct product of two groups one of which is Abelian). Let $Z = \mathcal{Z}(G)$, the center of G. Then $\mathcal{Z}(G^n) = Z^n$. Let ψ be a homomorphic encoder for the Abelian group Z^n. Consider the cosets of Z^n in G^n. Let $C = \{\mathbf{c}_1, \ldots, \mathbf{c}_r\}$ be the coset representatives. Let the output of the two sources be $\mathbf{x}_1$ and $\mathbf{x}_2$ and the function to be computed in the receiver be $\mathbf{y} = \mathbf{x}_1 \circ \mathbf{x}_2$. Let $\mathbf{x}_1 = \mathbf{c}_i \circ \mathbf{z}_1$ and $\mathbf{x}_2 = \mathbf{c}_j \circ \mathbf{z}_2,\ \mathbf{z}_1, \mathbf{z}_2 \in Z^n,\ \mathbf{c}_i, \mathbf{c}_j \in C$. The encoding operation at the two sources is then given by the map ϕ, where

$$\begin{aligned}
\text{encoder 1: } \phi : \mathbf{x}_1 &\longrightarrow (\mathbf{c}_i, \psi(\mathbf{z}_1)) && (37)\\
\text{encoder 2: } \phi : \mathbf{x}_2 &\longrightarrow (\mathbf{c}_j, \psi(\mathbf{z}_2)), && (38)
\end{aligned}$$

i.e. encoding takes place in two stages; in the first stage the coset representative is sent without compression and in the second stage the center component is compressed homomorphically. The receiver multiplies the outputs of the two encoders to get $(\mathbf{c}_i \circ \mathbf{c}_j, \psi(\mathbf{z}_1 \circ \mathbf{z}_2))$. The map ψ is chosen to allow reconstruction of $\mathbf{z}_1 \circ \mathbf{z}_2$ from $\psi(\mathbf{z}_1 \circ \mathbf{z}_2)$, using $\mathbf{c}_i, \mathbf{c}_j$ as side-information. The receiver finally recovers the function $\mathbf{y}$ as $\mathbf{y} = \mathbf{c}_i \circ \mathbf{c}_j \circ \mathbf{z}_1 \circ \mathbf{z}_2 = \mathbf{c}_i \circ \mathbf{z}_1 \circ \mathbf{c}_j \circ \mathbf{z}_2 = \mathbf{x}_1 \circ \mathbf{x}_2$, where the second equality follows since $\mathbf{z}_1, \mathbf{z}_2$ belong to the center of G^n. Note that the map ϕ is in general not a homomorphism. Yet the scheme allows for distributed function compression as with homomorphic encoders. The rate of compression can be calculated in a fashion as was done in Case 1.

Case 3*:* Here we give achievable rates for any non-Abelian group, in a two-source distributed coding setting. Let G be the source alphabet and let A be any Abelian subgroup of G. Such an Abelian subgroup always exists (for example, subgroup generated by a non-identity element). Let $\mathbf{x}_1$ and $\mathbf{x}_2$ be the source outputs and the function to be computed be $\mathbf{y}_1 = \mathbf{x}_1 \circ \mathbf{x}_2$. The first source represents $\mathbf{x}_1$ an element of left coset of A^n, while the second source represents its output

$\mathbf{x}_2$ as an element of the right coset of A^n. Let C be the set of coset representatives for both the left and right cosets. Let $\mathbf{x}_1 = \mathbf{c}_i \circ \mathbf{a}_1$ and $\mathbf{x}_2 = \mathbf{a}_2 \circ \mathbf{c}_j, \mathbf{a}_1, \mathbf{a}_2 \in A^n, \mathbf{c}_i, \mathbf{c}_j \in C$. Then encoders ϕ_1 and ϕ_2 at the two sources are described as

$$\begin{aligned} \text{encoder 1: } \phi_1 : \mathbf{x}_1 &\longrightarrow (\mathbf{c}_i, \psi(\mathbf{a}_1)) && (39)\\ \text{encoder 2: } \phi_2 : \mathbf{x}_2 &\longrightarrow (\psi(\mathbf{a}_2), \mathbf{c}_j), && (40) \end{aligned}$$

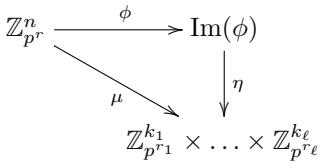
where ψ is a homomorphic encoder for A^n. Note that unlike in the previous two cases, the encoder is different for the two sources. The receiver can recover the product $\mathbf{a}_1 \circ \mathbf{a}_2$ from $\psi(\mathbf{a}_1 \circ \mathbf{a}_2)$ which in turn is obtained by multiplying $\psi(\mathbf{a}_1)$ and $\psi(\mathbf{a}_2)$. The function $\mathbf{y}$ is then calculated as $\mathbf{y} = \mathbf{c}_i \circ (\mathbf{a}_1 \circ \mathbf{a}_2) \circ \mathbf{c}_j$. The rate calculation can be carried out similar to as what was done in Case 1.

Appendix A
Proof of Lemma 3

Without loss of generality, we restrict the codomain of ϕ to $\mathrm{Im}(\phi)$. Since the domain of ϕ is Abelian, so is $\mathrm{Im}(\phi)$. Assuming $\mathrm{Im}(\phi)$ is non-trivial,

$$\mathrm{Im}(\phi) \cong \mathbb{Z}_{p_1^{r_1}}^{k_1} \times \ldots \times \mathbb{Z}_{p_\ell^{r_\ell}}^{k_\ell}, \tag{41}$$

where p_j is a prime, $r_j, k_j > 0,\ 1 \le j \le \ell$, for some $\ell > 0$. Now, since $\forall y \in \mathrm{Im}(\phi), p^r y = 0$, we should have $p_j = p,\ \forall j$, in the above equation. Let η denote the isomorphism in (41). Define $\mu \triangleq \eta \circ \phi$.



μ can be decomposed as $\mu = \mu_1 \times \ldots \times \mu_l$, where μ_j is the projection map

$$\mu_j : \mathbb{Z}_{p^r}^n \longrightarrow \mathbb{Z}_{p_j^{r_j}}^{k_j}, \tag{42}$$

with $1 \le j \le l$. Note that the map μ is onto and hence so are the projections, μ_js. This implies $r_j \le r,\ \forall j$. In this case, we have $\mathrm{Im}(\mu_j) \cong p^{r-r_j}\mathbb{Z}_{p^r}^{k_j} < \mathbb{Z}_{p^r}^{k_j}$. Let $\tilde{\mu_j} : \mathbb{Z}_{p^{r_j}}^{k_j} \hookrightarrow \mathbb{Z}_{p^r}^{k_j}$ be the corresponding isomorphic inclusion. Define a map $\tilde{\mu}$ as

$$\begin{aligned} \tilde{\mu} : \mathbb{Z}_{p^{r_1}}^{k_1} \times \ldots \times \mathbb{Z}_{p^{r_\ell}}^{k_\ell} &\longrightarrow \mathbb{Z}_{p^{r_1}}^{k_1+\ldots+k_\ell} && (43)\\ (x_1^{k_1}, \ldots, x_\ell^{k_\ell}) &\rightsquigarrow \left(\tilde{\mu}_1(x_1^{k_1}), \ldots, \tilde{\mu}_l(x_\ell^{k_\ell})\right) && (44) \end{aligned}$$

The desired map $\bar{\phi}$ is obtained as $\bar{\phi} \triangleq \tilde{\mu} \circ \mu : \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$, where $k = k_1 + \ldots + k_l$. To show that $\mathrm{Ker}(\phi) = \mathrm{Ker}(\bar{\phi})$, see that $\bar{\phi} = \tilde{\mu} \circ \eta \circ \phi$. Now, since both $\tilde{\mu}$ and η are $1-1$, we get $\mathrm{Ker}(\phi) = \mathrm{Ker}(\bar{\phi})$.

Appendix B
Proof of Lemma 4

Consider the homomorphism $\phi : \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$. Let A be the matrix corresponding to the homomorphism ϕ i.e., $\phi(\mathbf{x}) = A\mathbf{x}$ for every $\mathbf{x} \in \mathbb{Z}_{p^r}^n$. Note that the entries of A belong to $\mathbb{Z}_{p^r}$. It can be shown that $|\mathrm{Im}(\phi)|$ and $|\mathrm{Im}(\psi_i)|$ are invariant under elementary row and column operations on the matrix. Hence, we shall consider matrix A to be of the form,

$$\begin{bmatrix} I_{k_0} & & & & & \\ & pI_{k_1} & & & & \\ & & \ddots & & & 0_{k\times n-k} \\ & & & p^{r-1}I_{k_{r-1}} & & \\ & & & & 0_{k_r\times k_r} & \end{bmatrix}, \tag{45}$$

where $k = \sum_{j=0}^{r} k_j$ and I_ℓ denotes the identity matrix of size ℓ. Then we have,

$$\begin{aligned} |\mathrm{Im}(\phi)| &= (p^r)^{k_0} \ldots (p^{i+1})^{k_{r-i-1}} (p^i)^{k_{r-i}} \ldots p^{k_{r-1}} \\ |\mathrm{Im}(\psi_i)| &= (p^{r-i})^{k_0} \ldots (p)^{k_{r-i-1}} 1 \quad \ldots \quad 1\ . \end{aligned} \tag{46}$$

Taking logarithm on both sides and dividing the resulting terms we get

$$\frac{\log|\mathrm{Im}(\psi_i)|}{\log|\mathrm{Im}(\phi)|} = \left(\frac{r-i}{r}\right) \frac{\sum_{j=0}^{r-i-1} \frac{r-i-j}{r-i} k_j}{\sum_{j=0}^{r-i-1} \frac{r-j}{r} k_j + \sum_{j=r-i}^{r-1} \frac{r-j}{r} k_j}\ .$$

Since $\frac{r-i-j}{r-i} \le \frac{r-j}{r},\ 0 \le i < r$ we get,

$$\log|\mathrm{Im}(\psi_i)| \le \left(\frac{r-i}{r}\right) \log|\mathrm{Im}(\phi)|,\ 0 \le i < r. \tag{47}$$

Appendix C
Proof of Theorem 5

To enable us prove the above theorem, we introduce a few notations and definitions relating to the group $G = \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}}$, much like the way done in Section III-A for the group $\mathbb{Z}_{p^r}$. Consider the subgroup $H_{ij} = p_1^i\mathbb{Z}_{p_1^{r_1}} \times p_2^j\mathbb{Z}_{p_2^{r_2}}$ of G. Let G/H_{ij}, isomorphic to $K_{ij} = \mathbb{Z}_{p_1^i} \times \mathbb{Z}_{p_2^j}$, denote the cosets of H_{ij} in G. We will identify $\mathbb{Z}_{p_1^i} \times \mathbb{Z}_{p_2^j}$ with the coset representatives of G/H_{ij}. Let $y = (y^{(1)}, y^{(2)}) \in K_{ij}$ denote a coset representative. For the $n-$length vectors, we will identify K_{ij}^n with the coset representatives of the quotient group G^n/H_{ij}^n. A coset representative, $\mathbf{y} = (\mathbf{y}^{(1)}, \mathbf{y}^{(2)})$, is also a sequence of cosets of H_{ij} in G. Let $C_{\mathbf{y}}$ denote the coset $\mathbf{y} + H_{ij}$.

Let $P_{X,[X]_{ij}}$ denote the joint distribution of X and $[X]_{ij}$. By abuse of notation, we shall write $x \bmod p_{ij}$ in place of $(x^{(1)} \bmod p_1^i, x^{(2)} \bmod p_2^j)$. The distribution $P_{X,[X]_{ij}}$ is given by

$$P_{X,[X]_{ij}}(x,y) = \begin{cases} P_X(x) & \text{if } x \bmod p_{ij} = y \\ 0 & \text{else.} \end{cases} \tag{48}$$

Henceforth, we shall write $P(x,y)$ in place of $P_{X,[X]_{ij}}(x,y)$ and $P(x)$ in place of $P_X(x)$.

Let $A_\epsilon^n(X,[X]_{ij})$ denote the frequency typical set with respect to the distributions $P_{X,[X]_{ij}}$. We adopt the following definition of the typical set.

$$\begin{aligned} A_\epsilon^n(X,[X]_{ij}) = \Big\{(\mathbf{x},\mathbf{y}) : &\left|\frac{N(a,b|\mathbf{x},\mathbf{y})}{n} - P(a,b)\right| \\ &\le \epsilon P(a,b), \forall a \in G, b \in G/H_{ij}\Big\} \end{aligned} \tag{49}$$

where $N(a,b|\mathbf{x},\mathbf{y})$ denotes the number of joint occurrences of the symbols (a,b) in the sequences $(\mathbf{x},\mathbf{y})$. Let $A_\epsilon^n(X)$

and $A_\epsilon^n([X]_{ij})$ denote the typical sets with respect to the distributions P_X and $P_{[X]_{ij}}$, respectively. Also, let $A_\epsilon^n(X|\mathbf{y})$ denote the conditional typical set given $\mathbf{y}$.

A. A Few Useful Lemmas

Lemma 8: Consider a sequence $\mathbf{y} \in A_\epsilon^n([X]_{ij})$ and let $C_\mathbf{y} = \mathbf{y} + H_{ij}^n$. Then $A_\epsilon^n(X) \cap C_\mathbf{y} = A_\epsilon^n(X|\mathbf{y})$.

Proof: We only give a sketch of the proof. Consider a sequence $\mathbf{x}$ that is typical and belongs to the coset $C_\mathbf{y}$. Since $\mathbf{y} = \mathbf{x} \bmod p_{ij}$ is a deterministic function of $\mathbf{x}$, $\mathbf{y}$ occurs whenever $\mathbf{x}$ occurs i.e., $\mathbf{x}$ and $\mathbf{y}$ are jointly typical. Now, consider a sequence $\mathbf{x}$ that is jointly typical with $\mathbf{y}$, which means $\mathbf{x}$ is also typical. Also, since the cosets of H_{ij} are disjoint, $\mathbf{x}$ cannot be jointly typical with any $\mathbf{y}^{'} \neq \mathbf{y}$ and hence $\mathbf{x} \in C_\mathbf{y}$. □

Corollary 9: For any $\mathbf{x} \in A_\epsilon^n(X)$, we have

$$\left|A_\epsilon^n(X) \cap \mathbf{x} + H_{ij}^n\right| \leq 2^{nH(X|[X]_{ij})(1+\epsilon)} \quad (50)$$

Remark 2: We note that the above corollary also gives a simpler proof of Lemma 5 in [1], when specialized to case when $G = \mathbb{Z}_{p^r}$ and $H_{ij} = p^i\mathbb{Z}_{p^r}$.

Lemma 10: Let $\mathrm{Hom}(\mathbb{Z}_{p^r}^n, \mathbb{Z}_{p^r}^k)$ denote the set of all homomorphisms from $\mathbb{Z}_{p^r}^n$ to $\mathbb{Z}_{p^r}^k$. Then, for a homomorphism Φ randomly chosen from $\mathrm{Hom}(\mathbb{Z}_{p^r}^n, \mathbb{Z}_{p^r}^k)$, the probability that a given sequence $\mathbf{s} \in \mathbb{Z}_{p^r}^n$ belongs to $\mathrm{Ker}(\Phi)$ is given by,

$$P(\Phi(\mathbf{s}) = \mathbf{0}) = \begin{cases} p^{-(r-i)k} & \text{if } \mathbf{s} \in p^i\mathbb{Z}_{p^r}^n \backslash p^{i+1}\mathbb{Z}_{p^r}^n,\ 0 \leq i < r \\ 1 & \text{if } \mathbf{s} = \mathbf{0}. \end{cases} \quad (51)$$

Proof: See Lemma 4 in [1] □

B. Proof of Achievability

The achievability is proved by a random coding argument by averaging over the set of all homomorphisms, described in (19). Let $\Phi = (\Phi_1, \Phi_2)$ denote a randomly chosen map. Note that choosing Φ uniformly is same as choosing the component maps Φ_1, Φ_2 uniformly and independently. We define the component rates $R_1^{(n)}$ and $R_2^{(n)}$ as

$$R_1^{(n)} = \frac{\log_2 |\mathrm{Im}(\Phi_1^{(n)})|}{n}, \quad R_2^{(n)} = \frac{\log_2 |\mathrm{Im}(\Phi_2^{(n)})|}{n}. \quad (52)$$

Note that the rate of the encoder, $R^{(n)} = R_1^{(n)} + R_2^{(n)}$. The decoder is assumed to a typical set decoder. The decoder declares $\hat{\mathbf{x}}$ as the output if $\exists!\ \hat{\mathbf{x}} \in A_\epsilon^n(X)$ such that $\Phi(\hat{\mathbf{x}}) = \Phi(\mathbf{x})$; else the decoder declares an error. Let $D_{ij}^n = \left(p_1^i\mathbb{Z}_{p_1^{r_1}}^n \backslash p_1^{i+1}\mathbb{Z}_{p_1^{r_1}}^n\right) \times \left(p_2^j\mathbb{Z}_{p_2^{r_2}}^n \backslash p_2^{j+1}\mathbb{Z}_{p_2^{r_2}}^n\right)$. Also note that $D_{ij}^n \subset H_{ij}^n$. The probability of decoding error, P_e, averaged over all the $n-$length source sequences can then be upper bounded as

$$P_e^{(n)} \leq \sum_{\mathbf{x} \in A_\epsilon^n(X)} P_X(\mathbf{x}) P_{e|\mathbf{x}}^{(n)} + \epsilon, \quad (53)$$

where

$$\begin{aligned} P_{e|\mathbf{x}}^{(n)} &= P\left(\bigcup_{\substack{\tilde{\mathbf{x}} \in A_\epsilon^n(X) \\ \tilde{\mathbf{x}} \neq \mathbf{x}}} \Phi(\tilde{\mathbf{x}}) = \Phi(\mathbf{x})\right) \\ &\leq \sum_{\substack{\tilde{\mathbf{x}} \in A_\epsilon^n(X) \\ \tilde{\mathbf{x}} \neq \mathbf{x}}} P(\Phi(\tilde{\mathbf{x}}) = \Phi(\mathbf{x})) \\ &\overset{(a)}{=} \sum_{\substack{(\mathbf{s},\mathbf{t}) \in G^n, (\mathbf{s},\mathbf{t}) \neq (\mathbf{0},\mathbf{0}) \\ (\mathbf{s}+\mathbf{x}^{(1)}, \mathbf{t}+\mathbf{x}^{(2)}) \in A_\epsilon^n(X)}} P(\Phi_1(\mathbf{s}) = \mathbf{0}) P(\Phi_2(\mathbf{t}) = \mathbf{0}) \\ &= \sum_{\substack{0 \leq i \leq r_1 \\ 0 \leq j \leq r_2 \\ (i,j) \neq (r_1,r_2)}} \sum_{\substack{(\mathbf{s},\mathbf{t}) \in D_{ij}^n \\ (\mathbf{s}+\mathbf{x}^{(1)}, \mathbf{t}+\mathbf{x}^{(2)}) \in A_\epsilon^n(X)}} P(\Phi_1(\mathbf{s}) = \mathbf{0}) P(\Phi_2(\mathbf{t}) = \mathbf{0}) \\ &\overset{(b)}{\leq} \sum_{\substack{0 \leq i \leq r_1 \\ 0 \leq j \leq r_2 \\ (i,j) \neq (r_1,r_2)}} |A_\epsilon^n(X) \cap (\mathbf{s} + \mathbf{x}^{(1)}, \mathbf{t} + \mathbf{x}^{(2)}) + H_{ij}^n| \\ &\qquad \times p_1^{-(r_1-i)k_1} p_2^{-(r_2-j)k_2} \\ &\overset{(c)}{\leq} \sum_{\substack{0 \leq i \leq r_1 \\ 0 \leq j \leq r_2 \\ (i,j) \neq (r_1,r_2)}} 2^{nH(X|[X]_{ij})(1+\epsilon)} p_1^{-(r_1-i)k_1} p_2^{-(r_2-j)k_2}, \end{aligned}$$

where in (a), the probabilities split since Φ_1 and Φ_2 are picked independently. (b) and (c) follows from Lemma 10 and Corollary 9, respectively. Now, since ϵ can be made arbitrarily small, as long as

$$\left(\frac{r_1 - i}{r_1}\right)\frac{k_1}{n}\log p_1^{r_1} + \left(\frac{r_2 - j}{r_2}\right)\frac{k_2}{n}\log p_2^{r_2} > H(X|[X]_{ij}),$$

$P_e^{(n)}$ in (53) can be made arbitrarily small for every sufficiently large n. Combining this with the fact that

$$R_l^{(n)} \leq \frac{k_l}{n}\log p_l^{r_l},\ l \in \{1, 2\}, \quad (54)$$

it can be shown that any rate $R = \bar{R}_1 + \bar{R}_2$ such that

$$\left(\frac{r_1 - i}{r_1}\right)\bar{R}_1 + \left(\frac{r_2 - j}{r_2}\right)\bar{R}_2 > H(X|[X]_{ij}) \quad 0 \leq i \leq r_1, 0 \leq j \leq r_2, \quad (55)$$

is achievable. This completes the proof of achievability. □

ACKNOWLEDGMENT

This research is supported by the DRDO-IISc Program on Advanced Research in Mathematical Engineering and Microsoft Corporation and Microsoft Research India under the Microsoft Research India PhD Fellowship Award.

REFERENCES

[1] D. Krithivasan and S. Pradhan, "Distributed Source Coding using Abelian Group Codes," *Available: arxiv: 0808.2659v1[cs.IT]*.

[2] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *Information Theory, IEEE Transactions on*, vol. 19, no. 4, pp. 471–480, Jul 1973.

[3] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources (corresp.)," *Information Theory, IEEE Transactions on*, vol. 25, no. 2, pp. 219–221, Mar 1979.

[4] T.W. Hungerford, *Abstract Algebra: An Introduction*. Saunders College Publishing, 1997.