Distributed Source Coding using Abelian Group Codes: Extracting Performance from Structure

Dinesh Krithivasan and S. Sandeep Pradhan ,
Department of Electrical Engineering and Computer Science,
University of Michigan, Ann Arbor, MI 48109, USA
email: dineshk@umich.edu, pradhanv@eecs.umich.edu

***Abstract*— In this work, we consider a distributed source coding problem with a joint distortion criterion depending on the sources and the reconstruction. This includes as a special case the problem of computing a function of the sources to within some distortion and also the classic Slepian-Wolf problem [12], Berger-Tung problem [5], Wyner-Ziv problem [4], Yeung-Berger problem [6] and the Ahlswede-Korner-Wyner problem [3], [13]. While the prevalent trend in information theory has been to prove achievability results using Shannon's random coding arguments, using structured random codes offer rate gains over unstructured random codes for many problems. Motivated by this, we present a new achievable rate-distortion region (an inner bound to the performance limit) for this problem for discrete memoryless sources based on "good" structured random nested codes built over abelian groups. We demonstrate rate gains for this problem over traditional coding schemes using random unstructured codes. For certain sources and distortion functions, the new rate region is strictly bigger than the Berger-Tung rate region, which has been the best known achievable rate region for this problem till now. Further, there is no known unstructured random coding scheme that achieves these rate gains. Achievable performance limits for single-user source coding using abelian group codes are also obtained as parts of the proof of the main coding theorem. As a corollary, we also prove that nested linear codes achieve the Shannon rate-distortion bound in the single-user setting. Note that while group codes retain some structure, they are more general than linear codes which can only be built over finite fields which are known to exist only for certain sizes.**

I. Introduction

The problem of distributed source coding involves a set of encoders which observe different correlated components of a vector source and communicate their quantized observations to a central decoder through a rate-constrained noiseless communication link. The decoder is interested in reconstructing these observations or some function of them to within some distortion as measured by a fidelity criterion. The goal is to obtain a computable single-letter characterization of the performance limits measured by the rates of transmission and the distortions achieved. Such a formulation finds wide applications in many areas of communications such as sensor networks and distributed computing.

Most existing works that address this problem use the canonical encoding strategy of vector quantization followed by random binning. The best known inner bound to the performance limit that uses this approach is the Berger-Tung [5] inner bound. It has been shown in the literature that this is optimal in several cases. The work of Korner and Marton [1], however, is an exception and looks at a special case of the problem involving a pair of doubly symmetric binary sources and near lossless reconstruction of the sample-wise logical XOR function of the source sequences. They considered an encoding strategy where the first operation is an identity transformation. For the second operation, they consider random structured binning of the spaces of source sequences and show optimality. Further, the binning of two spaces is done in a "correlated" fashion using a binary linear code.

In the present paper, we build on this work, and present a new achievable rate region for the general distributed source coding problem and demonstrate an encoding scheme that achieves this rate region by using random coding on structured code ensembles. Our approach relies on the use of nested group codes for encoding. The binning operation of the encoders are done in a "correlated" manner as dictated by these structured codes. This use of "structured quantization followed by correlated binning" is in contrast to the more prevalent "quantization using random codes followed by independent binning" in distributed source coding. This approach unifies all the known results in distributed source coding such as the Slepian-Wolf problem [12], Korner-Marton problem [1], Wyner-Ahlswede-Korner problem [3], [13], Wyner-Ziv problem [4], Yeung-Berger problem [6] and Berger-Tung problem [5], under a single framework while recovering their respective rate regions. Moreover, this approach performs strictly better than the standard Berger-Tung based approach for certain source distributions. As a corollary, we show that nested linear codes can achieve the Shannon rate-distortion function in the single source point-to-point setting. A similar correlated binning strategy for reconstructing linear functions of jointly Gaussian sources with mean squared error criterion was presented in [9]. The present work develops a similar framework based on group codes. This rate region is developed using the following two new ideas. First, we use the fact that any abelian group is isomorphic to the direct sum of primary cyclic groups to enable the decomposition of the source into its constituent "digits" which are then encoded sequentially. Second, we show that, although group codes may not approach the Shannon rate-distortion function in a single source point-

This work was supported by NSF grant (CAREER) CCF-0448115.

to-point setting, it is possible to construct non-trivial group codes which contain a code that approaches it. Using these two ideas, we provide an all-group-code solution to the problem and characterize an inner bound to the performance limit using single-letter information quantities.

The paper is organized as follows. In Section II, we define the problem formally and present known results for the problem. In Section III, we present an overview of the properties of groups in general and cyclic groups in particular that shall be used later on. In Section IV, we define the various concepts used in the rest of the paper. In Section V, we present our coding scheme and present an achievable rate region for the problem defined in Section II. Section VI contains the various corollaries of the theorem presented in Section V. In Section VII, we demonstrate the application of our coding theorem to various problems. We conclude the paper with some comments in Section VIII.

A brief overview of the notation used in the paper is given below. Random variables are denoted by capital letters such as X, Y etc. The alphabet over which a discrete random variable X takes values will be indicated by $\mathcal{X}$. The cardinality of a discrete set $\mathcal{X}$ is denoted by $|\mathcal{X}|$. For a random variable X with distribution $p_X(\cdot)$, the set of all n-length strongly ϵ-typical sequences are denoted by $A_\epsilon^n(X)$ [10]. For a pair of jointly distributed random variables X, Y with distribution $p_{X,Y}(\cdot,\cdot)$, the set of all n-length y^n-sequences jointly ϵ-typical with a given x^n sequence is denoted by the set $A_\epsilon^n(x^n)$.

II. Problem Definition and Known Results

Consider a pair of discrete random variables (X, Y) with joint distribution $p_{XY}(\cdot,\cdot)$. Let the alphabets of the random variables X and Y be $\mathcal{X}$ and $\mathcal{Y}$ respectively. The source sequence (X^n, Y^n) is independent over time and has the product distribution $Pr((X^n, Y^n) = (x^n, y^n)) = \prod_{i=1}^n p_{XY}(x_i, y_i)$. We consider the following distributed source coding problem. The two components of the source are observed by two encoders which do not communicate with each other. Each encoder communicates a compressed version of its input through a noiseless channel to a joint decoder. The decoder is interested in reconstructing the sources with respect to a general fidelity criterion. Let $\hat{\mathcal{Z}}$ denote the reconstruction alphabet, and the fidelity criterion is characterized by a mapping: $d : \mathcal{X} \times \mathcal{Y} \times \hat{\mathcal{Z}} \to \mathbb{R}^+$. We restrict our attention to additive distortion measures.

In this work, we will concentrate on the above distributed source coding problem (with one distortion constraint), and provide an information-theoretic inner bound to the optimal rate-distortion region. One such inner bound can be obtained based on the Berger-Tung coding scheme [5] as follows. Let $\mathcal{P}$ denote the family of pair of conditional probabilities $(P_{U|X}, P_{V|Y})$ defined on $\mathcal{X} \times \mathcal{U}$ and $\mathcal{Y} \times \mathcal{V}$, where U and V are finite sets. For any $(P_{U|X}, P_{V|Y}) \in \mathcal{P}$, let the induced joint distribution be $P_{XYUV} = P_{XY} P_{U|X} P_{V|Y}$. U, V play the role of auxiliary random variables. Define $G\colon \mathcal{U} \times \mathcal{V} \to \hat{\mathcal{Z}}$ as that function of U, V that gives the optimal reconstruction $\hat{Z}$ with respect to the distortion measure $d(\cdot,\cdot,\cdot)$. With these definitions, an achievable rate region for this problem is presented below.

Fact 1: For a given source (X, Y) and distortion $d(\cdot,\cdot,\cdot)$ define the region $\mathcal{RD}_{BT}$ as

$$\mathcal{RD}_{BT} \triangleq \bigcup_{(P_{U|X}, P_{V|Y}) \in \mathcal{P}} \Big\{ R_1 \geq I(X;U|V), \; R_2 \geq I(Y;V|U), R_1 + R_2 \geq I(XY;UV), \; D \geq \mathbb{E}d(X, Y, G(U, V)) \Big\} \quad (1)$$

Then any $(R_1, R_2, D) \in \mathcal{RD}_{BT}^*$ is achievable where * denotes convex closure[1].

Proof: Follows from the analysis of the Berger-Tung problem [5] in a straightforward way. ∎

III. Groups - An Introduction

In this section, we present an overview of some properties of groups that are used later. We refer the reader to [11] for more details. We shall deal exclusively with abelian groups and hence the additive notation will be used for the group operation. The group operation of the group G is denoted by $+_G$. Similarly, the identity element of group G is denoted by e_G. The additive inverse of $a \in G$ is denoted by $-a$. The subscripts are omitted when the group in question is clear from the context. If H is a subgroup of the group G, it is denoted by $H < G$. The direct sum of two groups G_1 and G_2 is denoted by $G_1 \oplus G_2$. The direct sum of a group G with itself n times is denoted by G^n.

It is assumed that the reader has familiarity with the concepts of group homomorphisms, cyclic groups and cosets. We present the following well known fact about abelian groups.

Fact 2: Let G be a finite abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be $n = \prod_{i=1}^k p_i^{e_i}$. Then $G \cong A_1 \oplus A_2 \cdots \oplus A_k$ where $|A_i| = p_i^{e_i}$. Further, for each $A_i, 1 \leq i \leq k$ with $|A_i| = p_i^{e_i}$, we have $A_i \cong \mathbb{Z}_{p_i^{h_1}} \oplus \mathbb{Z}_{p_i^{h_2}} \cdots \oplus \mathbb{Z}_{p_i^{h_t}}$ where $h_1 \geq h_2 \cdots \geq h_t$ and $\sum_{j=1}^t h_j = e_i$. This decomposition of A_i into direct sum of primary cyclic groups is called the invariant factor decomposition of A_i. Putting these decompositions together, we get a decomposition of an arbitrary abelian group G into a direct sum of possibly repeated primary cyclic groups. Further, this decomposition of G is unique,i.e., if $G \cong B_1 \oplus B_2 \ldots B_m$ with $|B_i| = p_i^{e_i}$ for all i, then $B_i \cong A_i$ and B_i and A_i have the same invariant factors.

Proof: See [11], Section 5.2, Theorem 5. ∎

For example, Fact 2 implies that any abelian group of order 8 is isomorphic to either $\mathbb{Z}_8$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ or to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ where $\oplus$ denotes the direct sum of groups. Thus, we first consider the coding theorems only for the primary cyclic groups $\mathbb{Z}_{p^r}$. Results obtained for such groups are then extended to hold for arbitrary abelian groups through this decomposition.

[1]The cardinalities of U and V can be bounded using Caratheodary theorem [10].

The group $\mathbb{Z}_m$ is a commutative ring with the addition operation being addition modulo-m and the multiplication operation being multiplication modulo-m. This multiplicative structure is also exploited in the proofs. The group operation in $\mathbb{Z}_m^n$ is denoted by $u_1^n + u_2^n$. Addition of u_1^n with itself k times is denoted by ku_1^n. The multiplication operation between elements x and y of the underlying ring $\mathbb{Z}_m$ is denoted by xy. The group operation in the group $\mathbb{Z}_m$ is often explicitly denoted by $\oplus_m$. We shall build our codebooks as kernels of homomorphisms from $\mathbb{Z}_{p^r}^n$ to $\mathbb{Z}_{p^r}^k$. The proofs exploit the known fact that there exists a bijection between the set of all homomorphisms from the group $\mathbb{Z}_{p^r}^n$ to $\mathbb{Z}_{p^r}^k$ and the set of all $k \times n$ matrices with elements taking values from the group $\mathbb{Z}_{p^r}$.

IV. Definitions

When a random variable X takes value over the group $\mathbb{Z}_{p^r}$, we need to ensure that it doesn't just take values in some proper subgroup of $\mathbb{Z}_{p^r}$. This leads us to the concept of a non-redundant distribution over a group.

Definition 1: A random variable X with $\mathcal{X} = \mathbb{Z}_{p^r}$ or its distribution P_X is said to be non-redundant if $P_X(x) > 0$ for at least one symbol $x \in \mathbb{Z}_{p^r} \backslash p\mathbb{Z}_{p^r}$.

It follows from this definition that $x^n \in A_\epsilon^n(X)$ contains at least one $x \in \mathbb{Z}_{p^r} \backslash p\mathbb{Z}_{p^r}$ if X is non-redundant. Such sequences are called non-redundant sequences. A redundant random variable taking values over $\mathbb{Z}_{p^r}$ can be made non-redundant by a suitable relabeling of the symbols. Also, note that a redundant random variable over $\mathbb{Z}_{p^r}$ is non-redundant when viewed as taking values over $\mathbb{Z}_{p^{r-i}}$ for some $0 < i \leq r$. Our coding scheme involves good nested group codes for source and channel coding and the notion of embedding the optimal reconstruction function in a suitable abelian group. These concepts are made precise in the following series of definitions.

Definition 2: A bivariate function $G\colon \mathcal{U} \times \mathcal{V} \to \mathcal{G}$ is said to be embeddable in an abelian group A with respect to the distribution $p_{UV}(u, v)$ on $\mathcal{U} \times \mathcal{V}$ if there exists injective functions $S_U^{(A)}\colon \mathcal{U} \to A, S_V^{(A)}\colon \mathcal{V} \to A$ and a surjective function $S_G^{(A)}\colon A \to \mathcal{G}$ such that for all $(u, v) \in \mathcal{U} \times \mathcal{V}$ with $p_{UV}(u, v) > 0$, we have

$$S_G^{(A)}(S_U^{(A)}(u) +_A S_V^{(A)}(v)) = G(u, v) \tag{2}$$

If $G(U, V)$ is indeed embeddable in the abelian group A, it is denoted as $G(U, V) \subset A$ with respect to the distribution $p_{UV}(u, v)$. Define the mapped random variables $\bar{U} = S_U^{(A)}(U)$ and $\bar{V} = S_V^{(A)}(V)$. Their dependence on A is suppressed and the group in question will be clear from the context.

Suppose the function $G(U, V) \subset A$ with respect to p_{UV}. We encode the function $G(U, V)$ sequentially by treating the sources as vector valued over the cyclic groups whose direct sum is isomorphic to A. This alternative representation of the sources is made precise in the following definition.

Definition 3: Suppose the function $G(U, V) \subset A$ with respect to p_{UV}. Let A be isomorphic to $\oplus_{i=1}^k \mathbb{Z}_{p_i^{e_i}}$ where $p_1 \leq \cdots \leq p_k$ are primes and e_i are positive integers. Then, it follows from Fact 2 that there exists a bijection $S_A\colon A \to \mathbb{Z}_{p_1^{e_1}} \times \ldots \mathbb{Z}_{p_k^{e_k}}$. Let $\tilde{U} = S_A(\bar{U}), \tilde{V} = S_A(\bar{V})$. Let $\tilde{U} = (\tilde{U}_1, \ldots, \tilde{U}_k)$ be the vector representation of $\tilde{U}$. The random variables $\tilde{U}_i$ are called the digits of $\tilde{U}$. A similar decomposition holds for $\tilde{V}$. Define $\tilde{Z} = (\tilde{Z}_1, \ldots, \tilde{Z}_k)$ where $\tilde{Z}_i \triangleq \tilde{U}_i \oplus_{p_i^{e_i}} \tilde{V}_i$. It follows that $S_A^{-1}(\tilde{Z}) = \bar{U} +_A \bar{V}$.

Our encoding operation proceeds thus: we reconstruct the function $G(U, V)$ by first embedding it in some abelian group A and then reconstructing $\bar{U} +_A \bar{V}$ which we accomplish sequentially by reconstructing $\tilde{U}_i \oplus_{p_i^{e_i}} \tilde{V}_i$ one digit at a time. While reconstructing the ith digit, the decoder has as side information the previously reconstructed $(i-1)$ digits. This digit decomposition approach requires that we build codes over the primary cyclic groups $\mathbb{Z}_{p^r}$ which are "good" for various coding purposes. We define the concepts of group codes and what it means for group codes to be "good" in the following series of definitions.

Definition 4: Let A be a finite abelian group. A group code $\mathcal{C}$ of blocklength n over the group A is a subset of A^n which is closed under the group addition operation, i.e., $\mathcal{C} \subset A^n$ is such that if $c_1^n, c_2^n \in \mathcal{C}$, then so does $c_1^n +_{A^n} c_2^n$. Recall that the kernel $\ker(\phi)$ of a homomorphism $\phi\colon A^n \to A^k$ is a subgroup of A^n. We use this fact to build group codes. As mentioned earlier, we build codes over the primary cyclic group $\mathbb{Z}_{p^r}$. In this case, every group code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n$ has associated with it a $k \times n$ matrix H with entries in $\mathbb{Z}_{p^r}$ which completely defines the group code as $\mathcal{C} \triangleq \{x^n \in \mathbb{Z}_{p^r}^n\colon Hx^n = 0^k\}$. Here, the multiplication and addition are carried out modulo-p^r. H is called the parity-check matrix of the code $\mathcal{C}$. We employ nested group codes in our coding scheme. In distributed source coding problems, we often need one of the components of a nested code to be a good source code while the other one to be a good channel code. We shall now define nested group codes and the notions of "goodness" used to classify a group code as a good source or channel code.

Definition 5: A nested group code $(\mathcal{C}_1, \mathcal{C}_2)$ is a pair of group codes such that every codeword in the codebook $\mathcal{C}_2$ is also a codeword in $\mathcal{C}_1$, i.e., $\mathcal{C}_2 < \mathcal{C}_1$. Their associated parity check matrices are the $k_1 \times n$ matrix H_1 and the $k_2 \times n$ matrix H_2. They are related to each other as $H_1 = J \cdot H_2$ for some $k_1 \times k_2$ matrix J.

The code $\mathcal{C}_1$ is called the fine group code while $\mathcal{C}_2$ is called the coarse group code. When nested group codes are used in distributed source coding, typically the coset leaders of $\mathcal{C}_2$ in $\mathcal{C}_1$ are employed as codewords. In such a case, the rate of the nested group code would be $n^{-1}(k_2 - k_1) \log p^r$ bits.

We define the notion of "goodness" associated with a group code below. To be precise, these notions are defined for a family of group codes indexed by the blocklength n. However, for the sake of notational convenience, this indexing is not made explicit.

Definition 6: Let P_{XU} be a distribution over $\mathcal{X} \times \mathcal{U}$ such that the marginal P_U is a non-redundant distribution over $\mathbb{Z}_{p^r}$ for some prime power p^r. For a given group code $\mathcal{C}$

over $\mathcal{U}$ and a given $\epsilon > 0$, let the set $A_\epsilon(\mathcal{C})$ be defined as

$$A_\epsilon(\mathcal{C}) \triangleq \{x^n \colon \exists u^n \in \mathcal{C} \text{ such that } (x^n, u^n) \in A_\epsilon^{(n)}(X,U)\}. \tag{3}$$

The group code $\mathcal{C}$ over $\mathcal{U}$ is called a good source code for the triple $(\mathcal{X},\mathcal{U},P_{XU})$ if for all$\epsilon > 0$, we have $P_X^n(A_\epsilon(\mathcal{C})) \geq 1-\epsilon$ for all sufficiently large n.

Note that, a group code which is a good source code in this sense may not be a good source code in the usual Shannon sense. Rather, such a group code contains a subset which is a good source code in the Shannon sense for the source P_X with forward test channel $P_{U|X}$.

Definition 7: Let P_{ZS} be a distribution over $\mathcal{Z}\times\mathcal{S}$ such that the marginal P_Z is a non-redundant distribution over $\mathbb{Z}_{p^r}$ for some prime power p^r. For a given group code $\mathcal{C}$ over $\mathcal{Z}$ and a given $\epsilon > 0$, define the set $B_\epsilon(\mathcal{C})$ as follows:

$$B_\epsilon(\mathcal{C}) \triangleq \{(z^n, s^n) \colon \exists \tilde{z}^n \text{ such that } (\tilde{z}^n, s^n) \in A_\epsilon^{(n)}(Z,S) \text{ and } H\tilde{z}^n = Hz^n\}. \tag{4}$$

Here, H is the $k(n)\times n$ parity check matrix associated with the group code $\mathcal{C}$. The group code $\mathcal{C}$ is called a good channel code for the triple $(\mathcal{Z},\mathcal{S},P_{ZS})$ if for all $\epsilon > 0$, we have $P_{ZS}^n(B_\epsilon(\mathcal{C})) \leq \epsilon$ for all sufficiently large n. Associated with such a good group channel code would be a decoding function $\psi : \mathbb{Z}_{p^r}^k \times \mathcal{S}^n \to \mathbb{Z}_{p^r}^n$ such that $P(\psi(Hz^n, s^n) = z^n) \geq 1-\epsilon$.

Note that, as before, a group code which is a good channel code in this sense may not a good channel code in the usual Shannon sense. Rather, every coset of such a group code contains a subset which is a good channel code in the Shannon sense for the channel $P_{S|Z}$ with input distribution P_Z. This interpretation is valid only when S is a non-trivial random variable.

Lemma 1: For any triple $(\mathcal{Z},\mathcal{S},P_{ZS})$ of two finite sets and a distribution, with $|\mathcal{Z}| = p^r$ a prime power and P_Z non-redundant, there exists a sequence of group codes $\mathcal{C}$ that is a good channel code for the triple $(\mathcal{Z},\mathcal{S},P_{ZS})$ such that the dimensions of their associated $k(n)\times n$ parity check matrices satisfy

$$\lim_{n\to\infty}\frac{k(n)}{n}\log p^r = \max_{0\leq i<r}\left(\frac{r}{r-i}\right)(H(Z|S) - H([Z]_i|S)) \tag{5}$$

where $[Z]_i$ is a random variable taking values over the set of all distinct cosets of $p^i\mathbb{Z}_{p^r}$ in $\mathbb{Z}_{p^r}$. For example, if $\mathcal{Z} = \mathbb{Z}_8$, then $[Z]_2$ is a 4-ary random variable with symbol probabilities $(p_Z(0)+p_Z(4)), (p_Z(1)+p_Z(5)), (p_Z(2)+p_Z(6))$ and $(p_Z(3)+p_Z(7))$.

Note that $[Z]_0$ is a constant and $[Z]_r = Z$. When building codes over groups, each proper subgroup of the group contributes a term to the maximization in equation (5). Since the smaller the right hand side of equation (5), the better the channel code is, we incur a penalty by building codes over groups with large number of subgroups.

Lemma 2: For any triple $(\mathcal{X},\mathcal{U},P_{XU})$ of two finite sets and a distribution, with $|\mathcal{U}| = p^r$ a prime power and P_U non-redundant, there exists a sequence of group codes $\mathcal{C}$ that is a good source code for the triple $(\mathcal{X},\mathcal{U},P_{XU})$ such that the dimensions of their associated $k(n)\times n$ parity check matrices satisfy

$$\lim_{n\to\infty}\frac{k(n)}{n}\log p^r = \min_{\alpha\in\{1,r\}}\frac{r|H(U|X) - \log p^{r-\alpha}|^+}{\alpha} \tag{6}$$

where $|x|^+ = \max(x,0)$.

The proofs of these lemmas are omitted. Putting $r = 1$ in equations (5) and (6), we get the performance obtainable while using linear codes built over Galois fields.

Lemma 3: Let X, Y, S, U, V be five random variables where U and V take value over the group $\mathbb{Z}_{p^r}$ for some prime power p^r. Let $Z = U \oplus_{p^r} V$. Let $U \to X \to Y \to V$ form a Markov chain, and let $S \to (X,Y) \to (U,V)$ form a Markov chain. From the Markov chains, it follows that $H(U|X) \leq H(Z|S), H(V|Y) \leq H(Z|S)$. Without loss of generality, let $H(U|X) \leq H(V|Y) \leq H(Z|S)$. Then, there exists a pair of nested group codes $(\mathcal{C}_{11},\mathcal{C}_2)$ and $(\mathcal{C}_{12},\mathcal{C}_2)$ such that

- $\mathcal{C}_{11}$ is a good group source code for the triple $(\mathcal{X},\mathcal{U},P_{XU})$ with $\lim_{n\to\infty}\frac{k_{11}(n)}{n}\log p^r = \min_{\alpha\in\{1,r\}}(r/\alpha)|H(U|X) - \log p^{r-\alpha}|^+$.
- $\mathcal{C}_{12}$ is a good group source code for the triple $(\mathcal{Y},\mathcal{V},P_{YV})$ with $\lim_{n\to\infty}\frac{k_{12}(n)}{n}\log p^r = \min_{\alpha\in\{1,r\}}(r/\alpha)|H(V|Y) - \log p^{r-\alpha}|^+$.
- $\mathcal{C}_2$ is a good group channel code for the triple $(\mathcal{Z},\mathcal{S},P_{ZS})$ with $\lim_{n\to\infty}\frac{k_2(n)}{n}\log p^r = \max_{0\leq i<r}\left(\frac{r}{r-i}\right)(H(Z|S) - H([Z]_i|S))$.

The proof is omitted.

V. The Coding Theorem

We are given discrete random variables X and Y which are jointly distributed according to P_{XY}. Let $\mathcal{P}$ denote the family of pair of conditional probabilities $(P_{U|X}, P_{V|Y})$ defined on $\mathcal{X}\times\mathcal{U}$ and $\mathcal{Y}\times\mathcal{V}$, where $\mathcal{U}$ and $\mathcal{V}$ are finite sets, $|\mathcal{U}| = \alpha, |\mathcal{V}| = \beta$. For any $(P_{U|X}, P_{V|Y}) \in \mathcal{P}$, let the induced joint distribution be $P_{XYUV} = P_{XY}P_{U|X}P_{V|Y}$. U, V play the role of auxiliary random variables. Define $G\colon \mathcal{U}\times\mathcal{V} \to \hat{\mathcal{Z}}$ as that function of U,V that gives the optimal reconstruction $\hat{Z}$ with respect to the distortion measure $d(\cdot,\cdot,\cdot)$. Let $\mathcal{G}$ denote the image of $G(U,V)$. Let $\mathcal{T} = \{A\colon A \text{ is abelian}, |\mathcal{G}| \leq |A| \leq \alpha\beta, G(U,V) \subset A \text{ with respect to } P_{UV}\}$. It can be shown that the set $\mathcal{T}$ is non-empty, i.e., there always exists an abelian group $A \in \mathcal{T}$ in which any function $G(U,V)$ can be embedded. For any $A \in \mathcal{T}$, let A be isomorphic to $\oplus_{i=1}^k \mathbb{Z}_{p_i^{e_i}}$. Let $\tilde{U} = S_A(S_U^{(A)}(U))$ and $\tilde{V} = S_A(S_V^{(A)}(V))$ where the mappings are as defined in Definitions 2 and 3. Define $\tilde{Z} = (\tilde{Z}_1, \ldots, \tilde{Z}_k)$ where $\tilde{Z}_i = \tilde{U}_i \oplus \tilde{V}_i$ and the addition is done in the group to which the digits $\tilde{U}_i, \tilde{V}_i$ belong. Assume without loss of generality that the digits $\tilde{U}_i, \tilde{V}_i, \tilde{Z}_i, 1 \leq i \leq k$ are all non-redundant. If they are not, they can be made so by suitable relabeling of the symbols. Recall the definition of $[Z]_i$ from Lemma 1. The encoding operation of the X and Y encoders proceed in k steps with each step producing one digit of $\tilde{U}$ and $\tilde{V}$ respectively. Let $\pi_A\colon \{1,\ldots,k\} \to$

$\{1,\ldots,k\}$ be a permutation. The permutation π_A can be thought of as determining the order in which the digits get encoded and decoded. Let the set $\Pi_A(b), 1 \leq b \leq k$ be defined as $\Pi_A(b) = \{l\colon \pi_A(l) < b\}$. The set $\Pi_A(b)$ contains the indices of all the digits that get encoded before the bth stage. At the bth stage, let the digits $\tilde{U}_{\pi_A(b)}, \tilde{V}_{\pi_A(b)}$ take values over the group $\mathbb{Z}_{p_b}^{r_b}$. With these definitions, an achievable rate region for the problem is presented below.

Theorem 1: For a given source (X,Y), define the region $\mathcal{RD}_{in}$ as

$$\bigcup_{\substack{(P_{U|X},P_{V|Y})\in\mathcal{P}\\ A\in\mathcal{T},\pi_A}} \Bigg\{ (R_1,R_2,D)\colon R_i \geq \sum_{b=1}^{k} \min\left(R_{ib}^{(1)}, R_{ib}^{(2)}\right) \text{ for } i=1,2, D \geq \mathbb{E}d(X,Y,G(U,V)) \Bigg\} \tag{7}$$

where

$$R_{1b}^{(1)} > \Bigg[\max_{0\leq i<r_b}\left(\frac{r_b}{r_b-i}\right)\Big(H(\tilde{Z}_{\pi_A(b)} \mid \tilde{Z}_{\Pi_A(b)}) - H([\tilde{Z}_{\pi_A(b)}]_i|\tilde{Z}_{\Pi_A(b)})\Big)\Bigg] - \left(\min_{\alpha\in\{1,r_b\}} \frac{r_b|H(\tilde{U}_{\pi_A(b)} \mid X,\tilde{U}_{\Pi_A(b)}) - \log p_b^{r_b-\alpha}|^+}{\alpha}\right) \tag{8}$$

and

$$R_{1b}^{(2)} > \Bigg[\max_{0\leq i<r_b}\left(\frac{r_b}{r_b-i}\right)\Big(H(\tilde{U}_{\pi_A(b)} \mid \tilde{Z}_{\Pi_A(b)}) - H([\tilde{U}_{\pi_A(b)}]_i \mid \tilde{Z}_{\Pi_A(b)})\Big)\Bigg] - \left(\min_{\alpha\in\{1,r_b\}} \frac{r_b|H(\tilde{U}_{\pi_A(b)} \mid X,\tilde{U}_{\Pi_A(b)}) - \log p_b^{r_b-\alpha}|^+}{\alpha}\right) \tag{9}$$

Then any $(R_1,R_2,D) \in \mathcal{RD}_{in}^*$ is achievable where * denotes convex closure.

Proof: A very brief sketch of the proof ideas is presented here. The encoding proceeds in k stages with the bth stage encoding the digits $\tilde{U}_{\pi_A(b)}, \tilde{V}_{\pi_A(b)}$ in order to produce the digit $\tilde{Z}_{\pi_A(b)}$. For this, the decoder has side information $\tilde{Z}_{\Pi_A(b)}$. Let $\tilde{U}_{\pi_A(b)}, \tilde{V}_{\pi_A(b)}$ take values over the group $\mathbb{Z}_{p^b}^{r_b}$. The encoders have two encoding options available at the bth stage. They can either encode the digits $\tilde{U}_{\pi_A(b)}$ and $\tilde{V}_{\pi_A(b)}$ directly or encode in such a way that the decoder is able to reconstruct $\tilde{Z}_{\pi_A(b)}$ directly. We present a coding scheme to achieve the latter corresponding to the rates $R_{ib}^{(1)}, i=1,2$.

We shall use a pair of nested group codes $(\mathcal{C}_{11b},\mathcal{C}_{2b})$ and $(\mathcal{C}_{12b},\mathcal{C}_{2b})$ to encode $\tilde{Z}_{\pi_A(b)}$. Let the corresponding parity check matrices of these codes be H_{11b}, H_{12b} and H_{2b} respectively. Let the dimensionality of these matrices be $k_{11b}\times n$, $k_{12b}\times n$ and $k_{2b}\times n$ respectively. These codebooks are all over the group $\mathbb{Z}_{p^b}^{r_b}$. We need C_{11b} to be a good source code for the triple $(\mathcal{X}\times\tilde{\mathcal{U}}_{\Pi_A(b)},\tilde{\mathcal{U}}_{\pi_A(b)},P_{X\tilde{U}_{\Pi_A(b)}\tilde{U}_{\pi_A(b)}})$, $\mathcal{C}_{12b}$ to be a good source code for the triple $(\mathcal{Y}\times\tilde{\mathcal{V}}_{\Pi_A(b)},\tilde{\mathcal{V}}_{\pi_A(b)},P_{Y\tilde{V}_{\Pi_A(b)}\tilde{V}_{\pi_A(b)}})$ and $\mathcal{C}_{2b}$ to be a good channel code for the triple $(\tilde{\mathcal{Z}}_{\pi_A(b)},\tilde{\mathcal{Z}}_{\Pi_A(b)},P_{\tilde{Z}_{\pi_A(b)}\tilde{Z}_{\Pi_A(b)}})$.

The encoding scheme used by the X-encoder to encode the bth digit, $1\leq b\leq k$ is detailed below. The X-encoder looks for a typical sequence $\tilde{U}_{\pi_A(b)}^n \in \mathcal{C}_{11b}$ such that it is jointly typical with the source sequence X^n and the previous encoder output digits $\tilde{U}_{\Pi_A(b)}^n$. If it finds at least one such sequence, it chooses one of these sequences and transmits the syndrome $Sx_b \triangleq H_{2b}\tilde{U}_{\pi_A(b)}^n$ to the decoder. If it finds no such sequence, it declares an encoding error. The operation of the Y-encoder is similar. Let $\psi_b(\cdot,\cdot)$ be the decoder corresponding to the good channel code $\mathcal{C}_{2b}$. The decoder receives the syndromes Sx_b and Sy_b and computes $\psi_b\left(Sx_b \oplus_{p_b{}^{r_b}} Sy_b, \tilde{Z}_{\Pi_A(b)}^n\right)$. It can be shown that this equals $\tilde{Z}_{\pi_A(b)}^n$ with high probability and that the corresponding rates needed are $(R_{1b}^{(1)}, R_{2b}^{(1)})$. The encoding strategy to achieve $R_{ib}^{(2)}, i=1,2$ also involves nested group codes similar to the ones above and is omitted. ■

VI. Special cases

In this section, we consider the various special cases of the rate region presented in Theorem 1.

A. Lossless Source Coding using Group Codes

We start by demonstrating the achievable rates using codes over groups for the problem of lossless source coding. A good group channel code $\mathcal{C}$ for the triple $(\mathcal{X},0,P_X)$ as defined in Definition 7 can be used to achieve lossless source coding of the source X. The source encoder outputs Hx^n where H is the $k\times n$ parity check matrix of $\mathcal{C}$. The decoder uses the associated decoding function $\psi(\cdot,\cdot)$ to recover $\psi(Hx^n,0)=x^n$ with high probability. Based on this scheme, we get the following corollary to Theorem 1.

Corollary 1: Suppose X is a non redundant random variable over the group $\mathbb{Z}_{p^r}$ and the decoder wants to reconstruct X losslessly. Then, there exists a group based coding scheme that achieves the rate

$$R \geq \max_{0\leq i<r}\left(\frac{r}{r-i}\right)(H(X)-H([X]_i)) \tag{10}$$

Putting $r=1$ in equation (10) reduces it to the well known result that linear codes over prime fields can compress a source down to its entropy. Note that this achievable rate region using group codes can be strictly greater than Shannon entropy.

B. Lossy Source Coding using Group Codes

We next consider the case of lossy point to point source coding using codes built over the group $\mathbb{Z}_{p^r}$. Consider a memoryless source X with distribution P_X. The decoder attempts to reconstruct U that is within distortion D of X as specified by some additive distortion measure $d\colon \mathcal{X}\times\mathcal{U}\to\mathbb{R}^+$. Suppose U takes its values from the group $\mathbb{Z}_{p^r}$. A good group source code $\mathcal{C}$ for the triple $(\mathcal{X},\mathcal{U},P_{XU})$ as defined in Definition 6 can be used to achieve lossy coding of the source X provided the joint distribution P_{XU} is such that $\mathbb{E}(d(X,U))\leq D$ and U is non-redundant. The source

encoder outputs $u^n \in \mathcal{C}$ that is jointly typical with the source sequence x^n. An encoding error is declared if no such u^n is found. The decoder uses u^n as its reconstruction of the source x^n. Based on this coding scheme, we get the following corollary to Theorem 1.

Corollary 2: With definitions as above, there exists a group based coding scheme that achieves the rate

$$R \geq \log p^r - \min_{\substack{P_{U|X}:\, \mathbb{E}d(X,U)\leq D \\ \alpha\in\{1,r\}}} \frac{r|H(U|X) - \log p^{r-\alpha}|^+}{\alpha} \quad (11)$$

If U takes values in a general abelian group of order n that is not necessarily a primary cyclic group, then a decomposition based approach similar to the one used in the proof of Theorem 1 can be used. Putting $r = 1$ in equation (11) tells us that linear codes incur a strictly non-negative rate loss of $\log p - H(U)$ bits/sample when used for lossy source coding.

C. Nested Linear Codes

We specialize the rate region of Theorem 1 to the case when the nested group codes are built over cyclic groups of prime order, i.e., over Galois fields of prime order. It was already shown that Lemmas 1 and 2 imply that linear codes achieve the entropy bound and incur a rate loss while used in lossy source coding. In this section, we demonstrate the implications of Theorem 1 when specialized to the case of nested linear codes, i.e., when r is set to 1.

1) Shannon Rate-Distortion Function: We remark that Theorem 1 shows the existence of nested linear codes that can be used to approach the rate-distortion bound in the single-user setting for arbitrary discrete sources and arbitrary distortion measures.

Corollary 3: Let X be a discrete memoryless source with distribution P_X and let $\hat{\mathcal{X}}$ be the reconstruction alphabet. Let the fidelity criterion be given by $d\colon \mathcal{X} \times \hat{\mathcal{X}} \to \mathbb{R}^+$. Then, there exists a nested linear code $(\mathcal{C}_1, \mathcal{C}_2)$ that achieves the rate-distortion bound

$$R(D) = \min_{\substack{P_{\hat{X}|X} \\ \mathbb{E}d(X,\hat{X})\leq D}} I(X;\hat{X}) \quad (12)$$

Proof: Let the optimal forward test channel that achieves the bound be given by $P_{\hat{X}|X}$. Suppose q is a prime such that $\hat{\mathcal{X}} \subset \mathbb{Z}_q$ and $\hat{X}$ is non-redundant. The rate bound, given by $I(X;\hat{X})$ can be approached using a nested linear code $(\mathcal{C}_1, \mathcal{C}_2)$ built over the group $\mathbb{Z}_q$. Here $\mathcal{C}_1$ is a good source code for the triple $(\mathcal{X}, \hat{\mathcal{X}}, P_{X,\hat{X}})$ and $\mathcal{C}_2$ is a good channel code for the triple $(\hat{\mathcal{X}}, \mathcal{S}, P_{\hat{X}S})$ where $\mathcal{S} = \{0\}$ and S is a degenerate random variable with $P_S(0) = 1$. It follows from Lemmas 2 and 1 that the dimensions of the parity check matrices associated with $\mathcal{C}_1$ and $\mathcal{C}_2$ satisfy $\lim_{n\to\infty} \frac{k_1(n)}{n} \log q = H(\hat{X}|X), \lim_{n\to\infty} \frac{k_2(n)}{n} \log q = H(\hat{X})$. Thus, the rate achieved by this scheme is given by $n^{-1}(k_2(n) - k_1(n)) \log q = I(X;\hat{X})$. ∎

2) Berger-Tung Rate Region: We now show that Theorem 1 implies that nested linear codes built over prime fields can achieve the rate region of the Berger-Tung based coding scheme presented in Lemma 1.

Corollary 4: Suppose we have a pair of correlated discrete sources (X, Y) and the decoder is interested in reconstructing $\hat{Z}$ to within distortion D as measured by a fidelity criterion $d\colon \mathcal{X} \times \mathcal{Y} \times \hat{\mathcal{Z}} \to \mathbb{R}^+$. For this problem, an achievable rate region using nested linear codes is given by

$$\mathcal{RD}_{BT} = \bigcup_{(P_{U|X}, P_{V|Y})\in\mathcal{P}} \{(R_1, R_2)\colon R_1 \geq I(X;U|Y), \\ R_2 \geq I(Y;V|X), R_1 + R_2 \geq I(XY;UV)\} \quad (13)$$

where $\mathcal{P}$ is the family of all joint distributions P_{XYUV} that satisfy the Markov chain $U - X - Y - V$ such that the distortion criterion $\mathbb{E}d(X, Y, \hat{Z}(U,V)) \leq D$ is met. Here $\hat{Z}(U,V)$ is the optimal reconstruction of $\hat{Z}$ with respect to the distortion criterion given U and V.

Proof: We proceed by first reconstructing the function $G(U,V) = (U,V)$ at the decoder and then computing the function $\hat{Z}(U,V)$. For ease of exposition, assume that $\mathcal{U} = \mathcal{V} = \mathbb{Z}_q$ for some prime q. If they are not, a decomposition based approach can be used and the proof is similar to the one presented below. Clearly, $G(U,V)$ can be embedded in the abelian group $A \triangleq \mathbb{Z}_q \oplus \mathbb{Z}_q$ with the mappings $\tilde{U} = (U, 0)$ and $\tilde{V} = (0, V)$. Thus, $\tilde{Z}_1 = U + 0 = U$ and $\tilde{Z}_2 = 0 + V = V$. Encoding is done in two stages. Let the permutation $\pi_A(\cdot)$ be the identity permutation. With these choices, it can be verified that Theorem 1 yields $R_1 \geq I(X;U), R_2 \geq I(Y;V|U)$. This is one of the corner points of the rate region given in equation (13). Choosing the permutation $\pi_A(\cdot)$ to be the derangement gives us the other corner point and time sharing between the two points yields the entire rate region of equation (13). The rate needed to reconstruct U, V at the decoder coincides with the Berger-Tung rate region [5]. ∎

We note that this implies that our theorem recovers the rate regions of the problems considered by Wyner and Ziv [4], Ahlswede-Korner-Wyner [3], [13], Berger and Yeung [6] and Slepian and Wolf [12] since the Berger-Tung problem encompasses all these problems as special cases.

D. Lossless Reconstruction of Modulo-2 Sum of Binary Sources

In this section, we show that Theorem 1 recovers the rate region derived by Korner and Marton [1] for the reconstruction of the modulo-2 sum of two binary sources. Let X, Y be correlated binary sources. Let the decoder be interested in reconstructing the function $F(X,Y) = X \oplus_2 Y$ losslessly. In this case, the auxiliary random variables can be chosen as $U = X, V = Y$. Clearly, this function can be embedded in the groups $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. For embedding in $\mathbb{Z}_2$, the rate region of Theorem 1 reduces to $R_1 \geq \min(H(X), H(X \oplus_2 Y))$ and $R_2 \geq \min(H(Y), H(X \oplus_2 Y))$. It can be verified that embedding in $\mathbb{Z}_3$ or $\mathbb{Z}_4$ always gives a worse rate than embedding in $\mathbb{Z}_2$. Embedding in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ results in the Slepian-Wolf rate region. Combining these rate regions, we see that a sum rate of $R_1 + R_2 = \min(2H(X \oplus_2 Y), H(X,Y))$ is achievable using our coding scheme. This recovers the Korner-Marton

rate region for this problem [1], [10]. Moreover, one can also show that this approach can recover the Ahlswede-Han rate region [8] for this problem, which is an improvement over the Korner-Marton region.

VII. Examples

In this section, we consider applications of the coding theorem (Theorem 1) for a lossless and lossy distributed source coding problem.

A. Lossless Encoding of a Quaternary Function

Consider the following distributed source coding problem. Let (X, Y) be correlated random variables both taking values in $\mathbb{Z}_4$. Let X, Z be independent random variables taking values in $\mathbb{Z}_4$ according to the distributions P_X and P_Z respectively. Assume further that the random variable Z is non-redundant. Define the random variable Y as $Y = X \oplus_4 Z$. Suppose X and Y are observed by two separate encoders which communicate their quantized observations to a central decoder. The decoder is interested in reconstructing the function $Z = (X - Y) \mod 4$ losslessly.

Since we are interested in lossless reconstruction, we can choose the auxiliary random variables U, V to be $U = X, V = Y$. The function $G(U, V)$ then reduces to $F(X, Y) \triangleq (X - Y) \mod 4$. This function can be embedded in several groups with order less than or equal to 16. For simplicity, we only present the achievable rates for embedding in $\mathbb{Z}_4$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Lets consider the group $\mathbb{Z}_4$ first. Define the mappings $\tilde{x} \triangleq S_X^{(\mathbb{Z}_4)}(x) = x$ for all $x \in \mathbb{Z}_4, \tilde{y} \triangleq S_Y^{(\mathbb{Z}_4)}(y) = -y$ for all $y \in \mathbb{Z}_4$ and $S_F^{(\mathbb{Z}_4)}(z) = z$ for all $z \in \mathbb{Z}_4$. With these mappings, it follows from Definition 2 that $F(X, Y)$ is embeddable in $\mathbb{Z}_4$ with respect to the distribution P_{XY}. From Theorem 1, it follows that an achievable rate region using this embedding is given by $R_1 = R_2 = \max\{H(Z), 2(H(Z) - H([Z]_1))\}$. It is easy to verify that if $G(U, V) \subset \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and this embedding results in the Slepian-Wolf rate region given by $R_1 + R_2 = H(X, Y) = H(X) + H(Z)$. For certain source distributions, it is possible that embedding in $\mathbb{Z}_4$ results in a lower sum rate than the joint entropy. For example, taking X to be uniformly distributed and $P_Z(0) = 1/2, P_Z(1) = 0, P_Z(2) = P_Z(3) = 1/4$, we get that embedding in $\mathbb{Z}_4$ results in a sum rate of 3 bits/sample whereas the joint entropy $H(X, Y)$ is 3.5 bits/sample. Further enlargement of this achievable rate region is possible by embedding the function $G(U, V)$ in the groups $\mathbb{Z}_7$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The overall achievable rate region for this problem is the union of the achievable rate regions over all groups in which the function $G(U, V)$ can be embedded. The details are omitted.

B. Lossy Reconstruction of the Modulo-2 Sum of Binary Sources

This example concerns the reconstruction of the binary XOR function with the Hamming distortion criterion. The rate region of Theorem 1 is very cumbersome to calculate analytically in the general case. So, we restrict our attention to the case of symmetric source distribution and additive test channels in the derivation below where the intention is to demonstrate the analytical evaluation of the rate region of Theorem 1. We then present plots where the entire sum rate-distortion region is computed without any restrictive assumptions.

Consider a binary correlated source (X, Y) with symmetric joint distribution $P_{XY}(0, 0) = P_{XY}(1, 1) = q/2$ and $P_{XY}(1, 0) = P_{XY}(0, 1) = p/2$. Suppose we are interested in reconstructing $F(X, Y) = X \oplus_2 Y$ within Hamming distortion D. We present an achievable rate pair for this problem based on Theorem 1 and compare it to the achievable rate region presented in Lemma 1. It was shown in [14] that it suffices to restrict the cardinalities of the auxiliary random variables U and V to the cardinalities of their respective source alphabets in order to compute the Berger-Tung rate region. Since the scheme presented in Lemma 1 is based on the Berger-Tung coding scheme, the rate region $\mathcal{RD}_{BT}$ for this problem can be computed by using binary auxiliary random variables.

Let us now evaluate the rate region provided by Theorem 1 for this problem. The auxiliary random variables U and V are binary and suppose the test channel $P_{XY} P_{U|X} P_{V|Y}$ is fixed. The function $G(U, V)$ which is the optimal reconstruction of $X \oplus_2 Y$ given U and V can then be computed. In general, this function can take any of the 16 possible values depending upon the test channel $P_{XY} P_{U|X} P_{V|Y}$. For ease of exposition, let the auxiliary random variables be defined as $U = X \oplus_2 Q_1$ and $V = Y \oplus_2 Q_2$. Here Q_1, Q_2 are independent binary random variables with $P(Q_i = 0) = q_i, i = 1, 2$. Let $p_i = 1 - q_i, i = 1, 2$. Define $\alpha = q_1 q_2 + p_1 p_2$ and $\beta = 1 - \alpha$. Once the test channel $P_{XY} P_{U|X} P_{V|Y}$ is thus fixed, the optimal reconstruction function $G(U, V)$ that minimizes the probability $P(F(X, Y) \neq G(U, V))$ can be computed. It can be showed that

$$G(U,V) = \begin{cases} 0 & \alpha > p, \alpha < q \\ U \oplus_2 V & \alpha > p, \alpha > q \\ \overline{U \oplus_2 V} & \alpha < p, \alpha < q \\ 1 & \alpha < p, \alpha > q \end{cases} \tag{14}$$

where $\overline{a}$ denotes the complement of the bit a. The corresponding distortion for these reconstructions can be calculated as

$$D(\alpha) = \begin{cases} p & \alpha > p, \alpha < q \\ \beta & \alpha > p, \alpha > q \\ \alpha & \alpha < p, \alpha < q \\ q & \alpha < p, \alpha > q \end{cases} \tag{15}$$

Clearly, no rate need be expended if the function to be reconstructed is $G(U, V) = 0$ or $G(U, V) = 1$ and the rates needed would be the same for both $G(U, V) = U \oplus_2 V$ and $G(U, V) = \overline{U \oplus_2 V}$. Let us therefore consider only reconstructing $G(U, V) = U \oplus_2 V$. It can be shown that this function is embeddable in the groups $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Let us consider the group $A \triangleq \mathbb{Z}_2$. The associated mappings $S_U^{(A)}(\cdot), S_V^{(A)}(\cdot)$ and $S_G^{(A)}(\cdot)$ are all identity mappings. In this case, we have only one digit to encode. Further, note that $P(Z_1 = 0) = P(U_1 \oplus_2 V_1 = 0) = q\alpha + p\beta$.

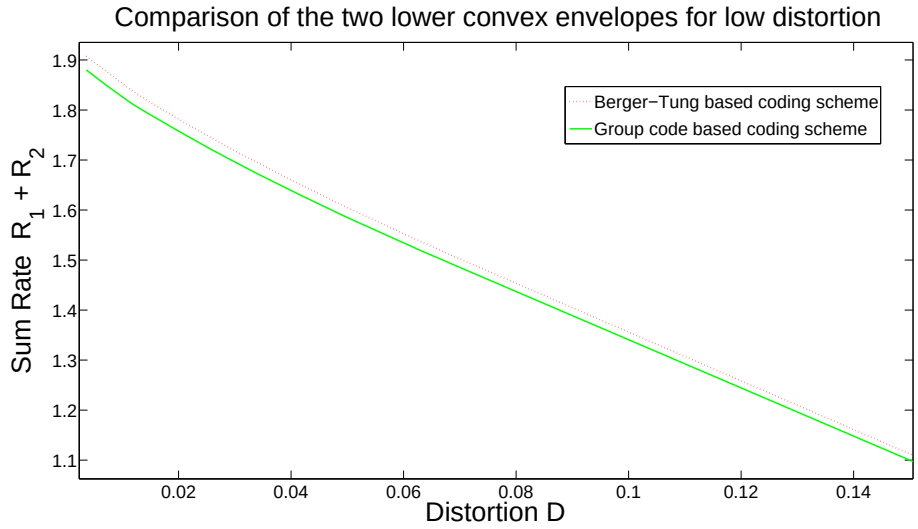

Fig. 1. Comparison of the lower convex envelopes of the two coding schemes

The rates of the encoders can be shown to be $R_1 = h(q\alpha + p\beta) - h(q_1), R_2 = h(q\alpha + p\beta) - h(q_2)$ where $h(\cdot)$ is the binary entropy function. These rates together with an achievable distortion $D \geq D(\alpha)$ (as given in equation (15) give an achievable rate region for the problem. Rate points achieved by embedding the function in the abelian groups $\mathbb{Z}_3, \mathbb{Z}_4$ are strictly worse than that achieved by embedding the function in $\mathbb{Z}_2$ while embedding in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ gives the Slepian-Wolf rate region for the lossless reconstruction of (U, V).

We now plot the entire sum rate-distortion region for the case of a general source distribution and general test channels $P_{U|X}, P_{V|Y}$ and compare it with the Berger-Tung rate region $\mathcal{RD}_{BT}$ of Fact 1. The source distribution used is $P_{XY}(00) = 0.3381, P_{XY}(01) = 0.1494, P_{XY}(10) = 0.2291, P_{XY}(11) = 0.2834$.

Figure 1 demonstrates that the sum rate-distortion regions of Theorem 1 and Fact 1 and shows that Theorem 1 offers improvements over the rate region of Fact 1 for low distortions. We expect the gains afforded by Theorem 1 over the rate region of Lemma 1 would increase as we increase the cardinality of the source alphabets.

VIII. Conclusion

We have introduced structured codes built over arbitrary abelian groups for lossless and lossy source coding and derived their performance limits. We also derived a coding theorem based on nested group codes for reconstructing an arbitrary function of the sources based on a fidelity criterion. The encoding proceeds sequentially in stages based on the primary cyclic decomposition of the underlying abelian group. This coding scheme recovers the known rate regions of many distributed source coding problems while presenting new rate regions to others. The usefulness of the scheme is demonstrated with both lossless and lossy examples.

Acknowledgements

The authors would like to thank Professor Hans-Andrea Loeliger of ETH, Zurich and Dr. Soumya Jana of University of Illinois, Urbana-Champaign for helpful discussions.

References

[1] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 219–221, March 1979.

[2] A. D. Wyner, "On source coding with side information at the decoder," *IEEE Trans. on Inform. Theory*, vol. IT-21, pp. 294–300, May 1975.

[3] R. Ahlswede and J. Korner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inform. Theory*, vol. IT- 21, pp. 629–637, November 1975.

[4] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. IT- 22, pp. 1–10, January 1976.

[5] S.-Y. Tung, *Multiterminal source coding*. PhD thesis, School of Electrical Engineering, Cornell University, Ithaca, NY, May 1978.

[6] T. Berger and R. W. Yeung, "Multiterminal source coding with one distortion criterion", *IEEE Trans. on Inform. Theory*, vol. IT-35, pp. 228–236, March 1989.

[7] S. Gelfand and M. Pinsker, "Coding of sources on the basis of observations with incomplete information," *Problemy Peredachi Informatsii*, vol. 15, pp. 45–57, Apr-June 1979.

[8] R. Ahlswede and T. S. Han, "On source coding with side information via a multiple-access channel and related problems in multi-user information theory," *IEEE Trans. on Inform. Theory*, vol. 29, pp. 396–412, May 1983.

[9] D. Krithivasan and S. S. Pradhan, "Lattices for distributed source coding: Jointly Gaussian Sources and Reconstruction of a linear function," *Submitted to IEEE Trans. Inform. Theory*.

[10] I. Csiszár and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Academic Press Inc. Ltd., 1981.

[11] D. S. Dummit and R. M. Foote, *Abstract Algebra*. John Wiley & sons Inc., 2004.

[12] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources, " *IEEE Trans. on Inform. Theory*, vol. 19, pp. 471–480, July 1973.

[13] A. D. Wyner, "On source coding with side information at the decoder," *IEEE Trans. on Inform. Theory*, vol. 21, pp. 294–300, May 1975.

[14] W. Gu, S. Jana and M. Effros, "On approximating the rate regions for lossy source coding with coded and uncoded side information", *Proc. IEEE International Symposium on Inform. Theory*, Toronto, Canada, 2008.