

# An Achievable Rate Region for Distributed Source Coding with Reconstruction of an Arbitrary Function of the Sources

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**—A new rate region is presented for a general framework of distributed source coding where the decoder is interested in lossy reconstruction of an arbitrary function of the sources. The coding scheme involves vector quantization of the sources followed by “correlated” binning. Nested linear codes are used for quantization and binning as against the more prevalent random codes. Our rate region recovers many known rate regions in distributed source coding while unifying them under the same general framework.

## I. INTRODUCTION

A large number of problems in multi-user information theory fall under the general setup of distributed source coding. A general framework for a distributed source coding problem consists of a set of encoders which observe different components of a correlated vector source and communicate their quantized observations to a central decoder through a rate-constrained noiseless communication link. The decoder is interested in reconstructing a function of these observations to within some distortion as measured by a fidelity criterion. Such a formulation finds wide applications in many areas of communications such as sensor networks and distributed computing. In this work, we present an achievable rate region for this problem and demonstrate a coding scheme that achieves this rate region.

The novelty of our approach lies in an unified treatment of the problem that works for any arbitrary function that the decoder is interested in reconstructing. Further, our approach relies on the use of nested linear 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. We present a novel algebraic structure called the digit plane field which enables the decomposition of the source into its constituent digits which are then encoded sequentially. This approach unifies several known results in distributed source coding such as the Slepian-Wolf problem [1], Korner-Marton problem [2], Wyner-Ziv problem [3], [5], Berger-Tung problem [4], under a single framework while recovering their respective rate regions.

The organization of the paper is as follows. In Section II, we formally define the problem. We motivate our coding

scheme with some illustrative examples in Section III. We present some relevant definitions in Section IV and introduce nested linear codes in Section V. The main coding theorem and its proof are presented in Section VI along with an example. Some comments about the coding theorem are presented in Section VII which concludes the paper.

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  $X$ , the set of all  $n$ -length  $\epsilon$ -typical sequences are denoted by  $A_\epsilon^n(X)$ . The finite field of size  $p$  is denoted by  $\mathbb{F}_p$ .

## II. FORMAL PROBLEM STATEMENT

Consider a pair of discrete random variables  $(X, Y)$  with joint distribution  $p_{XY}(x, y)$ . 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  $\prod_{i=1}^n p_{XY}(x_i, y_i)$ . Let  $F: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$  be the function the decoder is interested in reconstructing. Let  $d: \mathcal{Z} \times \mathcal{Z} \rightarrow \mathbb{R}^+$  be an additive distortion measure. A transmission system with parameters  $(n, \theta_1, \theta_2, \Delta)$  is defined by the set of mappings  $f_1: \mathcal{X}^n \rightarrow \{1, \dots, \theta_1\}$ ,  $f_2: \mathcal{Y}^n \rightarrow \{1, \dots, \theta_2\}$ ,  $g: \{1, \dots, \theta_1\} \times \{1, \dots, \theta_2\} \rightarrow \mathcal{Z}^n$  such that the following constraint is satisfied:  $\mathbb{E}(d(F(X^n, Y^n), g(f_1(X^n), f_2(Y^n)))) \leq \Delta$ . We say that a tuple  $(R_1, R_2, D)$  is achievable if  $\forall \epsilon > 0, \exists$  for all sufficiently large  $n$ , a transmission system exists with parameters  $(n, \theta_1, \theta_2, \Delta)$  such that  $\frac{1}{n} \log \theta_i \leq R_i + \epsilon$  for  $i = 1, 2$  and  $\Delta \leq D + \epsilon$ . The performance limit is given by the optimal rate-distortion region which is defined as the set of all achievable tuples  $(R_1, R_2, D)$ .

## III. MOTIVATION FOR THE CODING SCHEME

In this section, we present a sketch of the ideas involved in our coding scheme by demonstrating it for a simple lossless coding example where the sources are binary. A formal exposition of the coding scheme will follow later in Section VI.

### A. Lossless Reconstruction of the Modulo-2 Sum of Binary Sources

The problem of reconstructing the modulo-2 sum of binary sources was studied in [2] where an ingenious coding scheme

involving linear codes was presented. This coding scheme can be understood as follows. It is well known [8] that linear codes can be used to losslessly compress a source down to its entropy. Formally, for any discrete memoryless source  $Z$  with distribution  $p_Z(z)$ , there exists a  $k \times n$  binary matrix  $A$  with  $\frac{k}{n} \leq H(Z) + \epsilon$  and a function  $\psi(\cdot)$  such that  $P(\psi(Az^n) \neq z^n) < \epsilon$  for all sufficiently large  $n$ .

Let  $Z = X \oplus_2 Y$  be the modulo-2 sum of the binary sources  $X$  and  $Y$ . Let the matrix  $A$  be as described above. The  $X$  and  $Y$  encoders transmit  $s_1 = Ax^n$  and  $s_2 = Ay^n$  respectively at rates  $(H(Z), H(Z))$ . The decoder, upon receiving  $s_1$  and  $s_2$ , computes  $\psi(s_1 \oplus_2 s_2) = \psi(Ax^n \oplus_2 Ay^n) = \psi(Az^n)$ . By the above mentioned property of  $\psi(\cdot)$ , this equals  $z^n$  with high probability. Thus, the rate pair  $(H(Z), H(Z))$  is achievable. This coding strategy shall be referred to as the Korner-Marton coding scheme from here on.

The crucial part played by linear codes in this coding scheme is noteworthy. Had there been a centralized encoder with access to  $x^n$  and  $y^n$ , the coding scheme would be to compute  $z^n = x^n \oplus_2 y^n$  first and then compress it using any method known to achieve the entropy bound. Because the Korner-Marton encoding scheme is linear, it enables the decoder to use the *distributive* nature of the linear code over the modulo-2 operation to compute  $s_1 \oplus_2 s_2 = Az^n$ . Thus, from the decoder's perspective, there is no distinction between this distributed coding scheme and a centralized scheme involving a linear code. Also, in contrast to the usual norm in information theory, there is no known random coding scheme that approaches the performance of this linear coding scheme.

More generally, a sum rate of  $2H(X \oplus_q Y)$  can be achieved for the reconstruction of the sum of the two sources  $Z = X \oplus_q Y$  in any prime field  $\mathbb{F}_q$  [6]. If the source statistics is such that  $H(Z) > H(X)$ , then clearly it is better to compress  $X$  at a rate  $H(X)$ . Thus, the Korner-Marton coding scheme achieves the rate pair  $(R_1, R_2)$  with  $R_1 \geq \min\{H(X), H(Z)\}$  and  $R_2 \geq \min\{H(Y), H(Z)\}$ .

### B. Lossless Reconstruction of the Sources

The classical result of Slepian and Wolf [1] states that it is possible to reconstruct the sources  $X$  and  $Y$  noiselessly at the decoder with a sum rate of  $R_1 + R_2 = H(X, Y)$ . As was shown in [7], the Slepian-Wolf bound is achievable using linear codes. Here, we present another linear coding scheme similar to the one in the previous subsection.

We begin by making the observation that reconstructing the function  $Z = (X, Y)$  can be thought of as reconstructing a linear function in the field  $\mathbb{F}_4$ . This equivalence is demonstrated below. Let the elements of  $\mathbb{F}_4$  be  $\{00, 01, 10, 11\}$ . The addition operation in  $\mathbb{F}_4$  is simply bitwise XOR addition of the component bits. Define the mappings

$$\tilde{X} = \begin{cases} 00 & \text{if } X = 0 \\ 01 & \text{if } X = 1 \end{cases} \quad \tilde{Y} = \begin{cases} 00 & \text{if } Y = 0 \\ 10 & \text{if } Y = 1 \end{cases} \quad (1)$$

Clearly, reconstructing  $(X, Y)$  losslessly is equivalent to reconstructing the function  $\tilde{Z} = \tilde{X} \oplus_4 \tilde{Y}$  losslessly. The

next observation is that elements in  $\mathbb{F}_4$  can be represented as two dimensional vectors whose components are in  $\mathbb{F}_2$ . Let the first and second bits of  $\tilde{X}$  be denoted by  $\tilde{X}_1$  and  $\tilde{X}_2$  respectively. The same notation holds for  $\tilde{Y}$  and  $\tilde{Z}$  as well. Then, we have the decomposition of the vector function  $\tilde{Z}$  as  $\tilde{Z}_i = \tilde{X}_i \oplus_2 \tilde{Y}_i$  for  $i = 1, 2$ .

Encoding the vector function  $\tilde{Z}$  directly using the Korner-Marton coding scheme would entail a sum rate of  $R_1 + R_2 = \min\{H(X, Y), H(X)\} + \min\{H(X, Y), H(Y)\} = H(X) + H(Y)$  which is more than the sum rate dictated by the Slepian-Wolf bound. Instead, we encode the scalar components (digit planes) of the function  $\tilde{Z}$  sequentially using the Korner-Marton scheme.

Suppose the first digit plane  $\tilde{Z}_1$  is encoded first. Clearly, the Korner-Marton scheme can be used to encode the first digit plane  $\tilde{Z}_1$ . The rate pair  $(R_{11}, R_{21})$  achieved by the scheme is given by  $R_{11} \geq \min\{H(\tilde{Z}_1), H(\tilde{X}_1)\} = H(\tilde{X}_1) = 0$ ,  $R_{21} \geq \min\{H(\tilde{Z}_1), H(\tilde{Y}_1)\} = H(\tilde{Z}_1)$ .

It is straightforward to extend the Korner-Marton coding scheme to the case where decoder has available to it some side information. Since  $\tilde{Z}_1$  is now available as side information at the decoder, the rates needed to encode the second digit plane  $\tilde{Z}_2$  are  $R_{12} \geq \min\{H(\tilde{Z}_2 | \tilde{Z}_1), H(\tilde{X}_2 | \tilde{Z}_1)\} = H(\tilde{Z}_2 | \tilde{Z}_1)$ ,  $R_{22} \geq \min\{H(\tilde{Z}_2 | \tilde{Z}_1), H(\tilde{Y}_2 | \tilde{Z}_1)\} = H(\tilde{Y}_2 | \tilde{Z}_1) = 0$ .

Thus, the overall rate pair needed to reconstruct the sources losslessly is  $R_1 = H(\tilde{Z}_2 | \tilde{Z}_1) = H(\tilde{X}_2 | \tilde{Y}_1)$  and  $R_2 = R_{21} + R_{22} = H(\tilde{Z}_1) = H(\tilde{Y}_1)$ . The sum rate for this scheme is  $R_1 + R_2 = H(\tilde{X}_2, \tilde{Y}_1) = H(X, Y)$  thus equaling the Slepian-Wolf bound.

### C. Digit Plane Fields

The coding schemes in Sections III-A and III-B both use the same coding strategy, namely the Korner-Marton coding scheme applied sequentially to the digit planes of the function. They differ in the finite field in which the strategy is employed. This suggests a coding strategy for an arbitrary function  $F(X, Y)$  where we first "embed" the function in a suitable finite field and then code its digit plane decomposition sequentially.

Before we expand on this idea, we note that a finite structure less rigorous than a finite field would suffice for such a coding strategy. Note that the only property of the finite field  $\mathbb{F}_4$  that was used in the above encoding scheme is the field addition operation. More precisely, the fact that the digit planes of the addition operation  $\oplus_4$  could be expressed as finite field addition over  $\mathbb{F}_2$  was the only property of the finite field that was used in encoding. Since encoding is done at the digit plane level, it suffices if the finite structure that the function is embedded in can be decomposed into digit planes which are finite fields in themselves. We shall call such finite structures as digit plane fields (DPF). For example, the addition operation on a DPF of size 6 can be defined as follows. Since 6 is factorized as  $2 \times 3$ , the elements of DPF(6) are vectors of length 2, the first component of which is binary and the second is ternary. Addition is done component wise with the first component added in  $\mathbb{F}_2$  and the second

component added in  $\mathbb{F}_3$ . A formal definition of  $\text{DPF}(s)$  shall be provided later. Note that, the addition operation in the DPF structure reduces to that of a finite field in the case when the size of the DPF is a prime power.

#### D. Lossy Reconstruction of $F(X, Y)$

While there are more straightforward ways of achieving the Slepian-Wolf bound than the method outlined in Section III-B, our encoding scheme has the advantage of putting the Korner-Marton coding scheme and the Slepian-Wolf coding scheme under the same framework. The ideas used in these two examples can be abstracted and generalized for the case of lossy reconstruction of an arbitrary function  $F(X, Y)$ . We shall use nested linear codes to effect the quantization. Nested linear codes arise naturally in the area of distributed source coding and require that the fine code be a “good” source code and the coarse code be a “good” channel code for appropriate notions of goodness. We use a series of nested linear codes, one for each digit plane, over appropriate finite fields for quantization. This quantization operation is carried out sequentially.

The steps involved in the overall coding scheme is as follows: Let  $U, V$  be discrete random variables over the alphabet  $\mathcal{U}, \mathcal{V}$  respectively. Choose the joint density  $P(X, Y, U, V) = P(X, Y)P(U|X)P(V|Y)$  satisfying the Markov chain  $U - X - Y - V$ . Let  $G(U, V)$  be the best estimate of the function  $F$  given  $U, V$  with respect to the fidelity criterion. Embed the function  $G(U, V)$  in  $\text{DPF}(s)$  for some  $s$ . Decompose  $G(U, V)$  into its constituent digit planes. Suppose the  $b$ th digit plane is the finite field  $\mathbb{F}_{p_b}$ . Quantize the sources  $(X^n, Y^n)$  into digits  $(\tilde{U}_b, \tilde{V}_b)$  using the digits  $(\tilde{U}_1^{b-1}, \tilde{V}_1^{b-1})$  as side information. The details of the quantization procedure are detailed later. Encode  $\tilde{Z}_b = \tilde{U}_b \oplus_{p_b} \tilde{V}_b$  using the Korner-Marton encoding scheme.

#### IV. DEFINITIONS

The intuitive ideas behind Digit plane fields and embedding of functions in them as outlined in Section III are made precise in the following series of definitions. First, we define the finite algebraic structure that we termed Digit plane field in Section III-C. In what follows,  $s$  is a positive integer that can be factorized as  $s = \prod_{i=1}^k p_i^{e_i}, p_1 < \dots < p_k$ . Let  $\Omega(s) = \sum_{i=1}^k e_i$ . For  $1 \leq b \leq \Omega(s)$ , let  $m$  be such that  $\sum_{i=1}^{m-1} e_i + 1 \leq b \leq \sum_{i=1}^m e_i$ . Then, define  $\rho_s(b) \triangleq p_m$ .

*Definition 1:* The finite structure  $\text{DPF}(s)$  is the set  $X$  along with an addition operation  $\oplus_s$ . The elements of  $X$  are the set of  $\Omega(s)$ -tuples  $\{0, 1, \dots, p_1 - 1\}^{e_1} \times \dots \times \{0, 1, \dots, p_k - 1\}^{e_k}$  with  $A \times B$  denoting the Cartesian product of sets  $A$  and  $B$ . Let  $x, y \in \text{DPF}(s)$  and let  $z = x \oplus_s y$ . The addition operation  $\oplus_s$  is then defined for  $j = 1, \dots, \Omega(s)$  as  $z_j = (x_j + y_j) \bmod p_l$  for  $p_l = \rho_s(j)$ .

Suppose a random variable  $X$  takes values over the set  $\mathcal{X}$  with cardinality  $|\mathcal{X}| = s$ . One can think of  $X$  as taking values in the set  $\text{DPF}(s)$ . We now make the idea of embedding of a function in a digit plane field precise.

*Definition 2:* A bivariate function  $F(X, Y)$  is said to be embeddable in  $\text{DPF}(s)$  if there exists bijective functions

$S_X^{(s)}: \mathcal{X} \rightarrow \text{DPF}(s), S_Y^{(s)}: \mathcal{Y} \rightarrow \text{DPF}(s)$  and a function  $S_F^{(s)}: \text{DPF}(s) \rightarrow \mathcal{Z}$  such that  $S_F^{(s)}(S_X^{(s)}(x) \oplus_s S_Y^{(s)}(y)) = F(x, y)$  for all  $(x, y) \in \mathcal{X} \times \mathcal{Y}$  with  $p_{XY}(x, y) > 0$ . If the function  $F(X, Y)$  is indeed embeddable in  $\text{DPF}(s)$ , it is denoted as  $F(X, Y) \subset \text{DPF}(s)$ .

Our general coding scheme is similar in spirit to the Slepian-Wolf coding scheme outlined in Section III-B in that coding is done one digit of the sources at a time. In the most general case, coding takes place one digit plane of the digit plane field at a time. The following definition makes precise the idea of a digit plane.

*Definition 3:* Suppose the function  $F(X, Y)$  is embeddable in  $\text{DPF}(s)$ . Let  $x(i), 1 \leq i \leq |\mathcal{X}|$  denote the  $i$ th letter of the  $X$  alphabet.  $y(j)$  is similarly defined. Let  $\rho_s(b) = p_m$  for some  $1 \leq b \leq \Omega(s)$ . Let  $\tilde{x}(i) \triangleq S_X^{(s)}(x(i))$  and  $\tilde{y}(j) \triangleq S_Y^{(s)}(y(j))$ . Then the  $b$ th digit plane is defined as the  $p_m \times p_m$  matrix  $D_b$  with its  $(i, j)$ th element  $D_b(i, j) = \tilde{x}(i)_b \oplus_{p_m} \tilde{y}(j)_b$  where  $\oplus_{p_m}$  represents addition modulo- $p_m$ .

#### V. GOOD NESTED LINEAR CODES

Nested codes occur naturally in problems of distributed source coding. Their usefulness in structured approaches to various problems has been demonstrated in [9], [10]. 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 define in this section the various notions of “goodness” associated with a linear code.

An  $n$ -dimensional linear code  $\mathcal{C}$  over the space  $\mathbb{F}_p^n$  is a collection of codewords that form a linear subspace of  $\mathbb{F}_p^n$ . Every linear code  $\mathcal{C}$  has associated with it a  $k \times n$  parity check matrix  $H$  which completely defines the linear code as  $\mathcal{C} \triangleq \{x^n: Hx^n = 0^k\}$ .

*Definition 4:* A nested linear code  $(\mathcal{C}_1, \mathcal{C}_2)$  is a pair of linear codes such that every codeword in the codebook  $\mathcal{C}_2$  is also a codeword in  $\mathcal{C}_1$ , i.e.,  $\mathcal{C}_2 \subset \mathcal{C}_1$ . 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 linear code while  $\mathcal{C}_2$  is called the coarse linear code. When nested linear codes are employed 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 linear code would be  $n^{-1}(k_2 - k_1) \log p$  bits when the codebooks are over the linear space  $\mathbb{F}_p^n$ .

We define the notion of “goodness” associated with a linear code below.

*Definition 5:* A nested linear code  $(\mathcal{C}_1, \mathcal{C}_2)$  is said to be good if the fine code  $\mathcal{C}_1$  is a good linear source code and the coarse code  $\mathcal{C}_2$  is a good linear channel code. The notion of source and channel coding goodness is as below.

Let  $P_{XU}$  be a distribution over  $\mathcal{X} \times \mathcal{U}$  where without loss of generality  $\mathcal{U} = \{0, \dots, q - 1\}$  for some prime  $q$ . For a given linear code  $\mathcal{C}$  over  $\mathcal{U}^n$  and a given  $\epsilon > 0$ , let the set  $A_\epsilon(\mathcal{C})$  be defined as

$$A_\epsilon(\mathcal{C}) \triangleq \{x^n: \exists u^n \in \mathcal{C} \text{ s.t. } (x^n, u^n) \in A_\epsilon^{(n)}(X, U)\}. \quad (2)$$

The linear code  $\mathcal{C}$  is called a good source code for the triple  $(\mathcal{X}, \mathcal{U}, P_{XU})$  if we have  $P_X^n(A_\epsilon(\mathcal{C})) \geq 1 - \epsilon$  for sufficiently large  $n$ . It can be shown that there exists a sequence of good linear source codes  $\mathcal{C}$  such that the dimensions of their associated  $k(n) \times n$  parity check matrices satisfy  $\frac{k(n)}{n} \log q \nearrow H(U|X)$  as  $n \rightarrow \infty$ .

Let  $P_{ZS}$  be a distribution over  $\mathcal{Z} \times \mathcal{S}$  where without loss of generality  $\mathcal{Z} = \{0, \dots, q-1\}$  for some prime  $q$ . For a given linear code  $\mathcal{C}$  over  $\mathcal{Z}^n$  and a given  $\epsilon > 0$ , define the set  $B_\epsilon(\mathcal{C})$  as

$$B_\epsilon(\mathcal{C}) \triangleq \{(z^n, s^n): \exists \tilde{z}^n \text{ s.t. } (\tilde{z}^n, s^n) \in A_\epsilon^n(Z, S) \text{ and } H\tilde{z}^n = Hz^n\} \quad (3)$$

Here,  $H$  is the parity check matrix associated with the linear code  $\mathcal{C}$ .  $\mathcal{C}$  is called a good channel code for the triple  $(\mathcal{Z}, \mathcal{S}, P_{ZS})$  if we have  $P_{ZS}^n(B_\epsilon(\mathcal{C})) \leq \epsilon$  for sufficiently large  $n$ . It can be shown that there exists a sequence of good linear channel codes  $\mathcal{C}$  such that the dimensions of their associated  $k(n) \times n$  parity check matrices satisfy  $\frac{k(n)}{n} \log q \searrow H(Z|S)$  as  $n \rightarrow \infty$ . Associated with such a good linear channel code would be a decoding function  $\psi(\cdot, \cdot)$  such that  $P(\psi(Hz^n, s^n) = z^n) \geq 1 - \epsilon$ .

Note that, a linear code which is a good source code in this sense is not a good source code in the usual Shannon sense. Rather, such a linear code contains a subset which is a good source code in the Shannon sense for the source  $P_X$  with test channel  $P_{U|X}$ . Similarly, a linear code which is a good channel code in this sense is not a good channel code in the usual Shannon sense. Rather, every coset of such a linear code contains a subset that is a good channel code in the Shannon sense for the channel  $P_{S|Z}$  with input distribution  $P_Z$ . The proofs of the existence of good nested linear codes and bounds on the dimensions of their associated parity check matrices are omitted.

## VI. THE CODING THEOREM

Suppose we are given discrete random variables  $X$  and  $Y$  which are jointly distributed according to  $p(x, y)$ . The sources are observed by separate encoders which communicate quantized versions of their observations to a central decoder. The decoder is interested in reconstructing the function  $F(X, Y)$  to within some distortion  $D$ .

Let the  $X$  and  $Y$  quantizer outputs be indicated by the discrete random variables  $U$  and  $V$  respectively. Let their cardinalities be  $|\mathcal{U}| = \alpha$ ,  $|\mathcal{V}| = \beta$ . Let  $\mathcal{P}$  denote the family of joint distributions  $P(X, Y, U, V)$  that satisfy  $P(X, Y, U, V) = P(X, Y)P(U|X)P(V|Y)$ . Define  $G(U, V)$  to be the optimal reconstruction of  $F(X, Y)$  given  $U, V$  with respect to the distortion measure. Let  $\mathcal{S} \triangleq \{s: |\mathcal{G}| \leq s \leq \alpha\beta, G(U, V) \subset \text{DPF}(s)\}$ . For  $s \in \mathcal{S}$ , let  $\tilde{U} = S_U^{(s)}(U)$  and  $\tilde{V} = S_V^{(s)}(V)$  where  $S_U^{(s)}(\cdot)$  and  $S_V^{(s)}(\cdot)$  are as given in Definition 2. For a given  $s \in \mathcal{S}$ , let  $\pi_s: \{1, \dots, \Omega(s)\} \rightarrow \{1, \dots, \Omega(s)\}$  be a permutation. The permutation  $\pi_s$  can be thought of as determining the order in which the digit planes get encoded and decoded. Let the set  $\Pi_s(b), 1 \leq b \leq \Omega(s)$  be defined as  $\Pi_s(b) = \{k: \pi_s(k) < b\}$ . The set  $\Pi_s(b)$  contains the

indices of all the digit planes that get encoded before the  $b$ th stage. With these definitions, an achievable rate region for the problem is presented below.

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

$$\mathcal{RD}_{\text{in}} \triangleq \bigcup_{\substack{U, V \in \mathcal{P} \\ s \in \mathcal{S}, \pi_s}} \left\{ (R_1, R_2): R_1 \geq \sum_{b=1}^{\Omega(s)} \min \{R_{1b}^{(1)}, R_{1b}^{(2)}\} \right. \\ \left. R_2 \geq \sum_{b=1}^{\Omega(s)} \min \{R_{2b}^{(1)}, R_{2b}^{(2)}\}, D \geq d(F(X, Y), G(U, V)) \right\}$$

where  $R_{1b}^{(1)} = I(X\tilde{U}_{\Pi_s(b)}; \tilde{U}_{\pi_s(b)} | \tilde{Z}_{\Pi_s(b)})$  and  $R_{1b}^{(2)} = H(\tilde{Z}_{\pi_s(b)} | \tilde{Z}_{\Pi_s(b)}) - H(\tilde{U}_{\pi_s(b)} | X, \tilde{U}_{\Pi_s(b)})$ .  $R_{2b}^{(1)}$  and  $R_{2b}^{(2)}$  are similarly defined with  $(Y, V)$  replacing  $(X, U)$ . Then, any  $(R_1, R_2, D) \in \mathcal{RD}_{\text{in}}^*$  is achievable where  $*$  denotes convex closure.

**Proof:** Since the encoders don't communicate with each other, it is necessary to impose the Markov chain  $V - Y - X - U$  on the joint distribution  $P(X, Y, U, V)$ . The family  $\mathcal{P}$  contains all distributions that satisfy these Markov chains. Fix such a joint distribution. It can be shown that any function  $G(U, V)$  can be embedded in  $\text{DPF}(\alpha\beta)$  and hence the set  $\mathcal{S}$  is non-empty. In what follows, fix  $s \in \mathcal{S}$ . The encoding operation of the  $X$  and  $Y$  encoders proceeds in  $\Omega(s)$  steps with each step producing one digit of  $\tilde{U}$  and  $\tilde{V}$  respectively.

Let  $\rho_s(\pi_s(b)) \triangleq p$ . Then,  $\mathbb{F}_p$  is the finite field over which the digits  $\tilde{U}_{\pi_s(b)}$  and  $\tilde{V}_{\pi_s(b)}$  take their values. Note that, while decoding the  $b$ th digit plane, the decoder has access to the previous digit planes  $\tilde{Z}_{\Pi_s(b)}$  which can be used as side information. The encoders have two encoding options available at the  $b$ th stage. They can either encode the digits  $\tilde{U}_{\pi_s(b)}, \tilde{V}_{\pi_s(b)}$  directly or encode in such a way that the decoder is able to reconstruct  $\tilde{Z}_{\pi_s(b)}$  directly.

The encoding scheme to accomplish the rates  $R_{1b}^{(2)}, R_{2b}^{(2)}$  is as follows. We shall use a pair of good nested linear codes  $(\mathcal{C}_{11b}, \mathcal{C}_{2b})$  ( $\mathcal{C}_{2b} \subset \mathcal{C}_{11b}$ ) and  $(\mathcal{C}_{12b}, \mathcal{C}_{2b})$  ( $\mathcal{C}_{2b} \subset \mathcal{C}_{12b}$ ) to encode  $\tilde{Z}_{\pi_s(b)}$ . 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  $k_{11b} \times n, k_{12b} \times n, k_{2b} \times n$  respectively. These codebooks are all over the linear space  $\mathbb{F}_p^n$ . We need  $\mathcal{C}_{11b}$  to be a good source code for the triple  $(\mathcal{X} \times \tilde{U}_{\Pi_s(b)}, \tilde{U}_{\pi_s(b)}, P_{X\tilde{U}_{\Pi_s(b)}\tilde{U}_{\pi_s(b)}})$ ,  $\mathcal{C}_{12b}$  to be a good source code for the triple  $(\mathcal{Y} \times \tilde{V}_{\Pi_s(b)}, \tilde{V}_{\pi_s(b)}, P_{Y\tilde{V}_{\Pi_s(b)}\tilde{V}_{\pi_s(b)}})$  and  $\mathcal{C}_{2b}$  to be a good channel code for the triple  $(\tilde{Z}_{\pi_s(b)}, \tilde{Z}_{\Pi_s(b)}, P_{\tilde{Z}_{\pi_s(b)}\tilde{Z}_{\Pi_s(b)}})$ .

The encoding scheme used by the  $X$ -encoder to encode the  $b$ th digit plane,  $1 \leq b \leq \Omega(s)$  is detailed below. The  $X$ -encoder looks for a typical sequence  $\tilde{U}_{\pi_s(b)}^n \in \mathcal{C}_{11b}$  such that it is jointly typical with the source sequence  $X^n$  and the previous encoder output digits  $\tilde{U}_{\Pi_s(b)}^n$ . If it finds at least one such sequence, it chooses one of these sequences and transmits the syndrome  $Sx_b \triangleq H_{2b}\tilde{U}_{\pi_s(b)}$  to the decoder. If

it finds no such sequence, it declares an encoding error. The operation of the  $Y$ -encoder is similar. Since  $\mathcal{C}_{11b}$  and  $\mathcal{C}_{12b}$  are good linear source codes for the appropriate distributions, the probability of encoding error goes to zero provided the dimensions of the corresponding parity check matrices satisfy the bound given in Definition 5. Let  $\psi_b(\cdot, \cdot)$  be the decoder corresponding to the good linear channel code  $\mathcal{C}_{2b}$ . The decoder, on receiving the syndromes  $Sx_b$  and  $Sy_b$ , computes  $\psi_b(Sx_b \oplus_p Sy_b, \tilde{Z}_{\Pi_s(b)})$ . It can be shown that this equals  $\tilde{Z}_{\pi_s(b)}$  with high probability.

The rate expended by the  $X$ -encoder at the  $b$ th stage can be calculated as follows. Since  $\mathcal{C}_{11b}$  is a good source code, it follows from Definition 5 that  $\frac{k_{11b}}{n} \log p \leq H(\tilde{U}_{\pi_s(b)} | X, \tilde{U}_{\Pi_s(b)}) - \epsilon_1$  where  $\epsilon_1 \rightarrow 0$  as  $n \rightarrow \infty$ . A similar bound holds for the dimensions of  $H_{12b}$ . Since  $\mathcal{C}_{2b}$  is a good channel code, it follows that  $\frac{k_{2b}}{n} \log p \geq H(\tilde{Z}_{\pi_s(b)} | \tilde{Z}_{\Pi_s(b)}) + \epsilon_2$  where  $\epsilon_2 \rightarrow 0$  as  $n \rightarrow \infty$ . The rate of the nested linear code in bits would be  $R_{1b} = n^{-1}(k_{2b} - k_{11b}) \log p$ . Therefore

$$R_{1b}^{(2)} \geq H(\tilde{Z}_{\pi_s(b)} | \tilde{Z}_{\Pi_s(b)}) - H(\tilde{U}_{\pi_s(b)} | X, \tilde{U}_{\Pi_s(b)}) + \epsilon_1 + \epsilon_2 \quad (4)$$

The rates  $R_{1b}^{(1)}, R_{2b}^{(1)}$  can also be accomplished using nested linear codes. The source codes  $\mathcal{C}_{11b}, \mathcal{C}_{12b}$  are chosen to be good for the same triples as before. However, in this case, the encoders use different channel codes. The channel code  $\mathcal{C}_{21b}$  of the  $X$ -encoder is chosen to be good for the triple  $(\tilde{U}_{\pi_s(b)}, \tilde{Z}_{\Pi_s(b)}, P_{\tilde{U}_{\pi_s(b)} \tilde{Z}_{\Pi_s(b)}})$ . This gives the rate of the  $X$ -encoder for the  $b$ th stage as

$$R_{1b}^{(1)} = I(X \tilde{U}_{\Pi_s(b)}; \tilde{U}_{\pi_s(b)} | \tilde{Z}_{\Pi_s(b)}) \quad (5)$$

The channel code  $\mathcal{C}_{22b}$  and  $R_{2b}^{(1)}$  are similarly defined. At the  $b$ th stage, the  $X$ -encoder uses that scheme that offers the lower rate of the two options available to it. Thus, combining equations (5) and (4), the rate  $R_{1b}$  of the  $X$ -encoder at the  $b$ th stage is  $R_{1b} = \min\{R_{1b}^{(1)}, R_{1b}^{(2)}\}$ . The rate of the  $Y$ -encoder at the  $b$ th stage is similarly given. Summing over the  $\Omega(s)$  stages of encoding gives us the rates claimed in Theorem 1. Clearly, the distortion achieved by this scheme is  $\mathbb{E}d(F(X, Y), G(U, V))$  and thus, the rate region is established.

#### A. Lossy Reconstruction of $X \oplus_2 Y$

In this section, we present a simple example to illustrate the application of Theorem 1. Consider a binary correlated source  $(X, Y)$  with  $p_{XY}(0, 0) = p_{XY}(1, 1) = q/2$ ,  $p_{XY}(0, 1) = p_{XY}(1, 0) = p/2$ . We are interested in reconstructing  $F(X, Y) = X \oplus_2 Y$  to within Hamming distortion  $D$ . For simplicity, let us choose the auxiliary random variables to be binary and define them as  $U = X \oplus_2 Q_1$ ,  $V = Y \oplus_2 Q_2$  for independent binary random variables  $Q_1, Q_2$ . In place of the optimal reconstruction function  $G(U, V)$ , let us use  $G(U, V) = U \oplus_2 V$  for the sake of illustration. Clearly, this function can be embedded in DPF(2) and the associated mappings  $S_U^{(2)}(\cdot), S_V^{(2)}(\cdot), S_G^{(2)}(\cdot)$

are all identity mappings. Let then  $Z \triangleq U \oplus_2 V$ . The achievable rate of transmission for the  $X$  encoder as given by equations (5) and (4) is  $R_{11} = \min(H(U), H(Z)) - H(U|X) = H(Z) - H(U|X)$ . A similar expression holds for  $R_2$ . Thus, an achievable sum rate for this problem is given by  $R_{sum} = 2H(Z) - H(U|X) - H(V|Y)$ . The distortion is simply  $D = P(Q_1 \oplus_2 Q_2 = 1)$ . Note that this rate region can be improved by considering more general test channels, using the optimal reconstruction function  $G(U, V)$  and embedding in higher digit plane fields.

## VII. COMMENTS AND CONCLUSIONS

It is worth noting that the rate region presented in Theorem 1 doesn't include bounds on the cardinalities of the auxiliary random variables  $U$  and  $V$ . However, the rate region can be computed for fixed cardinalities of  $U$  and  $V$  and this approach recovers many known results of distributed source coding. By applying Theorem 1 to the case of reconstructing  $F(X, Y) = (X, Y)$  with independent distortion criteria for the sources, it can be shown that the rate region of Berger and Tung [4] can be rederived. This implies that our coding scheme also subsumes the Slepian-Wolf problem [1] and the Wyner-Ziv problem [3], [5] among others as these are special cases of the Berger-Tung problem. We also note that Theorem 1 implies that nested linear codes achieve the rate-distortion bound for an arbitrary source with an arbitrary distortion criterion.

In summary, we have presented a coding scheme for the general problem of distributed source coding in this paper. This approach unifies many different problems in the area under the same framework while recovering their rate regions. The scheme makes use of structured nested linear codes for vector quantization and binning.

## REFERENCES

- [1] D. Slepian and J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell Syst. Tech. J.*, vol. 52, pp. 1037–1076, September 1973.
- [2] 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.
- [3] 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.
- [4] S.-Y. Tung, *Multiterminal source coding*. PhD thesis, School of Electrical Engineering, Cornell University, Ithaca, NY, May 1978.
- [5] H. Yamamoto, "Wyner-Ziv theory for a general function of correlated sources," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 803–807, September 1982.
- [6] T. S. Han and K. Kobayashi, "A dichotomy of functions  $F(X, Y)$  of correlated sources  $(X, Y)$ ," *IEEE Trans. on Inform. Theory*, vol. 33, pp. 69–76, January 1987.
- [7] I. Csiszar, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 585–592, July 1982.
- [8] A. D. Wyner, "Recent results in Shannon theory," *IEEE Trans. on Inform. Theory*, vol. 20, pp. 2–10, January 1974.
- [9] H. A. Loeliger, "On the basic averaging arguments for linear codes" in *Communications and Cryptography: Two Sides of One Tapestry*, pp. 252–262, Luwer Academic Publishers, 1994.
- [10] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inform. Theory*, vol. IT-48, pp. 1250–1276, June 2002.