The Universality of Generalized Hamming Code for Multiple Sources

Rick Ma and Samuel Cheng, *Member, IEEE*

***Abstract*—We consider zero-error Slepian-Wolf coding for a special kind of correlated sources known as Hamming sources. Moreover, we focus on the design of codes with minimum redundancy (i.e., perfect codes). As shown in a prior work by Koulgi *et al.*, the design of a perfect code for a general source is very difficult and in fact is NP-hard. In our recent work, we introduce a subset of perfect codes for Hamming sources known as Hamming Codes for Multiple Sources (HCMSs). In this work, we extend HCMSs to generalized HCMSs, which can be proved to include all perfect codes for Hamming sources. To prove our main result, we first show that any perfect code for a Hamming source with two terminals is equivalent to a Hamming code for asymmetric Slepian Wolf coding (c.f. Lemma 2). We then show that any multi-terminal (of more than two terminals) perfect code can be transformed to a perfect code for two terminals (c.f. Lemma 3) and to a perfect code with an asymmetric form (c.f. Lemma 4). Equipped with these results, we prove that every perfect Slepian-Wolf code for Hamming sources is equivalent to a generalized HCMS.**

I. Introduction

Slepian-Wolf (SW) coding refers to lossless distributed compression of correlated sources. Consider s correlated sources $X_1, X_2, \cdots, X_s$. SW coding studies a setup in which encoding is performed separately for each encoder that can see only one of the s sources whereas decoding is performed jointly.

Wyner is the first who realized that by taking computed syndromes as compressed sources, channel codes can be used to implement SW coding efficiently [1]. The approach was rediscovered and popularized by Pradhan *et al.* more than two decades later [2]. Practical syndrome-based schemes for S-W coding using channel codes have been further studied in [3], [4], [5], [6], [7], [8], [9], [10], [11]. Despite these efforts, most prior works are restricted to the discussion of two sources [2], [12], [13], [14], [15], [11] except for a few exceptions [16], [3], [17].

In [17], we described a generalized syndrome based SW code and extended the notions of a packing bound and a perfect code from regular channel coding to SW coding with an arbitrary number of sources. In [18], we introduced the notion of Hamming Code for Multiple Sources (HCMSs) as a perfect code solution for Hamming sources. Moreover, we have shown that there exist an infinite number of HCMSs for three sources. However, we have also pointed out that not all perfect codes for Hamming sources can be represented as HCMSs. In this paper, we extend HCMS to *generalized HCMS*. The main contribution is to show the universality of generalized HCMS. Namely, any perfect SW code for a Hamming source is equivalent to a generalized HCMS (c.f. Theorem 3).

This paper is organized as follows. In the next section, we will describe the problem setup and introduce perfect SW codes for Hamming sources. We will review HCMS and introduce generalized HCMS in Section III. In Section IV, before the conclusion we will show the universality of generalized HCMS.

R. Ma was with the Department of Mathematics at the Hong Kong University of Science and Technology, Hong Kong.

S. Cheng is with the School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, OK, 74135 USA email: samuel.cheng@ou.edu.
This work was supported in part by NSF under grant CCF 1117886.

II. General Syndrome based SW Coding and Perfect SW Codes for Hamming Sources

We will begin with a general definition of syndrome based SW codes with multiple sources [17].

Definition 1 (Syndrome based SW code)**.** A rate $(r_1, r_2, \cdots, r_s)$ *syndrome based SW code* for s correlated length-n sources contains s coding matrices $H_1, H_2, \cdots, H_s$ of sizes $m_1 \times n, m_2 \times n, \cdots, m_s \times n$, where $r_i = m_i/n$ for $i = 1, 2, \cdots, s$.

- Encoding: The i^{th} encoder compresses length-n input $\mathbf{x}_i$ into $\mathbf{y}_i = H_i \mathbf{x}_i$ and transmits the compressed m_i bits (with compression rate $r_i = m_i/n$) to the base station.
- Decoding: Upon receiving all $\mathbf{y}_i$, the base station decodes all sources by selecting a most probable $\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2, \cdots, \hat{\mathbf{x}}_s$ that satisfies $H_i \hat{\mathbf{x}}_i = \mathbf{y}_i, i = 1, 2, \cdots, s$.

Unlike many prior works focusing on near-lossless compression, in this work we consider true lossless compression (zero-error reconstruction) in which sources are *always* recovered losslessly [19], [20], [21], [22]. So we will characterize a set of s-terminal source tuples S to be *compressible* by a SW code if any source tuple in S can be reconstructed losslessly. Alternatively, we say the SW code can *compress* S. Apparently, a SW code can compress S if and only if its encoding map restricted to S is injective (or 1-1).

While asymptotically optimum SW codes [14], [16], [3] can be designed and approach quite close to the SW limit, in low delay applications, it may be more suitable to use zero-error codes rather than codes with an asymptotically vanishing error. For highly correlated sources, we expect that sources from most terminals are likely to be the same. The trivial case is when all s sources are identical. The next (simplest non-trivial) possible case is when all sources except one are identical. Moreover, in the source that is different from the rest, only one bit differs from the corresponding bit of other sources. We call the sources s-terminal *Hamming sources* of length n if their possible outcomes include the patterns described in the two aforementioned senarios with equal probability but exclude any other patterns. Let S be the set containing all s-terminal Hamming sources of length n. By simple counting, the set S has a size of $(sn+1)2^n$ when the number of terminals $s > 2$ and a size of $(n+1)2^n$ when $s = 2$ [17]. Thus, if S is compressible by a SW code with $\mathcal{C}$ denoted as the set of all compressed outputs, the code has to satisfy a packing bound that $|\mathcal{C}| \geq |S|$. We characterize a code as *perfect* if the code can compress S and the equality in the packing bound is satisfied ($i.e.$, $|\mathcal{C}| = |S|$). Note that the encoding map of a perfect code $\mathcal{C}$ restricted to the target source S has to be bijective (i.e., both surjective and injective). The mapping is injective due to the fact that S is compressible by $\mathcal{C}$ and surjective due to the perfectness condition that $|\mathcal{C}| = |S|$.

The notion of perfectness is a direct analogy of that in channel coding. Just as a perfect channel code can transmit information at the capacity of the target channel with a finite length code, a perfect SW code achieves the SW bound [23] of its target sources even with a finite source length. In fact, it is not difficult to show that a perfect code in channel coding can be used to construct a perfect code for asymmetric[1] SW coding of two sources with correlation modeled by a hypothetical channel. For Hamming sources, the corresponding channel is a bit error channel with no more than one bit error, which can be *perfectly* handled by a Hamming code.

For the ease of exposition, we will define a *Hamming matrix* as follows.

Definition 2 (Hamming Matrix)**.** An m-bit Hamming matrix consists of all nonzero column vectors of length m. Note that the size of the matrix is $m \times (2^m - 1)$.

We call the aforementioned matrices as Hamming matrices since in channel coding. They correspond to the parity check matrix of a Hamming code.

An example of *perfectly* compressing a 7-bit binary source with side information was described in [2]. In this setup, two 7-bit binary sources $\mathbf{x}$ and $\mathbf{y}$ that differ no more than 1 bit are encoded separately and decoded jointly. Assuming that all allowed combinations are equally likely, we have the joint entropy $H(\mathbf{x},\mathbf{y}) = \log_2(2^7(\binom{7}{1}+1)) = 10$ bits. Now, if we consider the asymmetric case that we are only compressing $\mathbf{x}$ using $\mathbf{y}$ as side information whereas $\mathbf{y}$ is compressed independently, then we need $H(\mathbf{y}) = 7$ bits to compress $\mathbf{y}$ but only need $H(\mathbf{x}|\mathbf{y}) = 3$ bits to compress $\mathbf{x}$. This can be achieved if we use a 3-bit Hamming matrix and 7×7 identity matrix as the coding matrices of $\mathbf{x}$ and $\mathbf{y}$, respectively. More generally, the defined code below can compress and reconstruct perfectly a source pair $\mathbf{x}$ and $\mathbf{y}$ as long as $\mathbf{x}$ and $\mathbf{y}$ differ no more than one bit.

Definition 3 (Hamming Code for Asymmetric SW Coding)**.** We call a syndrome based SW code (H_X, H_Y) as a Hamming Code for Asymmetric SW Coding (HCASWC) for a pair of length-n sources if H_Y is invertible and H_X is an m-bit Hamming matrix with $n = 2^m - 1$.

For a pair of target sources that differ no more than one bit, *Compressibility* and *perfectness* can be easily verified by showing that the mapping restricted to the source is both injective and surjective.

This two-source asymmetric example can be extended to "non-asymmetric" cases that the compression rates of the sources can be arbitrarily rebalanced while perfectness is conserved [12], [3]. Decompose the Hamming matrix H_X as $[P|I] = [P_1 P_2|I]$, where I is an identity matrix of size $m \times m$. By the so-called code partitioning technique [12], [3], one can be easily shown that a pair of coding matrices $\tilde{H}_X = \left[\begin{smallmatrix} I & 0 & 0 \\ 0 & P_2 & I \end{smallmatrix}\right]$ and $\tilde{H}_Y = \left[\begin{smallmatrix} 0 & I & 0 \\ P_1 & 0 & I \end{smallmatrix}\right]$ can perfectly compress a two-terminal Hamming source by treating $\mathbf{x}+\mathbf{y}$ as a noise vector. For example, to compress two-terminal Hamming source of length-7, $\mathbf{x}$ and $\mathbf{y}$, to 4 bits and 6 bits, respectively, we can employ coding matrices $\tilde{H}_X = \begin{pmatrix} 0001000 \\ 1110100 \\ 0110010 \\ 1010001 \end{pmatrix}$ and $\tilde{H}_Y = \begin{pmatrix} 1000000 \\ 0100000 \\ 0010000 \\ 0000100 \\ 0001010 \\ 0001001 \end{pmatrix}$ and the total number of encoded bits (i.e., 10 bits) is kept unchanged. However, the aforementioned code partitioning technique cannot be naturally extended to more than two sources. For example, for a three-terminal source $(\mathbf{x},\mathbf{y},\mathbf{z})$, a code extended from a Hamming matrix will compress and recover the source perfectly if and only if $\mathbf{x}+\mathbf{y}+\mathbf{z}$ has no more than one 1. This hardly relates to any realistic physical source.

The design of zeror-error SW codes is related to the chromatic number problem for graphs [24]. Even though the design of zero-error SW codes is described in [19], [21], [22], they are restricted to two terminals only. Moreover, even for this case, the design of perfect SW codes (also described as minimum redundancy zero-error source codes with side information) is shown to be very challenging. Indeed, the problem for arbitrary sources can be shown to be NP-hard [20]. For the case with more than two terminals, it was not until recently that the existence of perfect SW codes for three sources was illustrated using HCMS [18].

[1]"Asymmetric SW coding" refers to a setup that only one of the two sources is compressed.

III. Hamming Code for Multiple Sources

For the rest of the paper, let us denote S as the set containing all s-terminal Hamming sources of length n. Denote $M = m_1 + m_2 + \cdots + m_s$ as the total number of compressed bits. Then we have $|\mathcal{C}| = 2^M$ and from the previous section the equation for perfect compression as

$$\begin{array}{ll} 2^n(sn+1) = 2^M, & s > 2, \\ 2^n(n+1) = 2^M, & s = 2. \end{array} \tag{1}$$

Since $sn + 1 = 2^{(M-n)}$, s obviously cannot be even except for $s = 2$. On the other hand, by Fermat's Little Theorem, we have $2^{(s-1)} \equiv 1 \pmod{s}$ for every odd prime $s > 1$. This gives an infinite number of solutions to (1)

A. HCMS

Theorem 1 (Hamming Code for Multiple Sources)**.** *For positive integers $s > 2, n, M$ satisfying (1), let P be an $(M-n)$-bit Hamming matrix of size $(M-n) \times (2^{M-n} - 1) = (M-n) \times (sn)$.*

If P can be partitioned into

$$P = [Q_1, Q_2, \cdots, Q_s] \tag{2}$$

such that each Q_i is an $(M-n) \times n$ matrix and

$$Q_1 + Q_2 + \cdots + Q_s = 0, \tag{3}$$

and there exists a matrix T of dimension[2] $(n-(s-1)(M-n)) \times n$ *such that the $n \times n$ matrix R defined by*

$$R = \begin{pmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_{s-1} \\ T \end{pmatrix} \tag{4}$$

is invertible, then we have a set of s coding matrices

$$\begin{pmatrix} G_1 \\ Q_1 \end{pmatrix}, \begin{pmatrix} G_2 \\ Q_2 \end{pmatrix}, \cdots, \begin{pmatrix} G_s \\ Q_s \end{pmatrix} \tag{5}$$

that forms a perfect compression, where $G_1, G_2, \cdots, G_s$ be any kind of row partition of T. That is,

$$T = \begin{pmatrix} G_1 \\ G_2 \\ \cdots \\ G_s \end{pmatrix}, \tag{6}$$

and some G_i can be chosen as a void matrix [18].

Definition 4 (Hamming Code for Multiple Sources)**.** We call a code composed of coding matrices described in (5) as a Hamming code for mulitple sources (HCMS).

Remark 1 (SW coding of three sources of length-1)**.** Apparently, HCMS only exists if the $(s-1)(M-n) \leq n$, otherwise the required height of T will be negative. For example, let $s = 3$, $n = 1$, and $M = 3$. Even though the parameters satisfy (1), we will not have HCMS because $n - (s-1)(M-n) = -3$. However, a perfect (trivial) SW code actually exists in this case; the coding matrices for all three terminals are simply the scalar matrix [1].

From Remark 1, we see that HCMS cannot model all perfect codes that can compress s-terminal Hamming sources. It turns out that we can modify HCMS slightly and the extension will cover all perfect

[2]We need $n - (s-1)(M-n) \geq 0$.

SW codes for Hamming sources. Before we continue, we need the following definitions.

Definition 5 (Full Row Rank Matrix)**.** A *full row rank matrix* is a full rank fat or square matrix. Note that the corresponding mapping is surjective when a full row rank matrix is used as a coding matrix.

Definition 6 (Row Basis Matrix)**.** Given a matrix A, we say a full row rank matrix B is a *row basis matrix* of A, if $\text{row}(B) = \text{row}(A)$, where $\text{row}(A)$ denotes the row space of A, i.e., all linear combinations of rows of A.

Example 1 (Row Basis Matrix)**.** $\left(\begin{smallmatrix}100\\011\end{smallmatrix}\right)$ is a row basis matrix of both $\left(\begin{smallmatrix}100\\100\\111\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}100\\111\\111\end{smallmatrix}\right)$.

Remark 2. When B is a row basis matrix of A, there is a *unique* matrix C s.t. $A = CB$ (because every row of A can be decomposed as a unique linear combination of B since B is a full row rank matrix). And there exists matrix D s.t. $B = DA$ but D is not necessarily unique. Thus, given a vector $\mathbf{v}$, if we know $A\mathbf{v}$, we can compute $B\mathbf{v}$ (as $DA\mathbf{v}$). Similarly, we have $A\mathbf{v}$ given $B\mathbf{v}$.

B. Generalized HCMS

The main idea of generalized HCMS is to "loosen" the condition in (4) using the notion of row basis matrices. Let Y, a $d \times n$ matrix, be a row basis matrix of $\begin{pmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_{s-1} \end{pmatrix}$, where $Q_1, \cdots, Q_s$ is a partition of a Hamming matrix satisfying (2) and (3). Since Y is a full row rank matrix, there always exists a T s.t. $R = \left(\begin{smallmatrix} Y \\ T \end{smallmatrix}\right)$ is an $n \times n$ invertible matrix regardless of whether $(s-1)(M-n) \le n$ is satisfied (c.f. Remark 1).

Theorem 2 (Generalized HCMS)**.** *With T constructed according to the previous paragraph, we let $G_i, i = 1, \cdots, s$ be any row partition of T as in (6) and C_i be a row basis matrix of Q_i for $i = 1, \cdots, s$. Then a set of coding matrices 4.2 $\left(\begin{smallmatrix} G_1 \\ C_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} G_2 \\ C_2 \end{smallmatrix}\right), \cdots, \left(\begin{smallmatrix} G_s \\ C_s \end{smallmatrix}\right)$ forms a compression for the set of s-terminal Hamming sources of length n. Moreover, the compression will be perfect if $d_1 + d_2 + ... + d_s + (n - d) = M$, where d_i is the number of rows of C_i.*

Proof: Denote $|\mathbf{x}|$ as the Hamming weight of any binary vector $\mathbf{x}$ that maps $\mathbf{x}$ in $\mathbb{Z}_2^n$ to its norm in $\mathbb{Z}$ by counting the number of nonzero components, e.g., $|(1,1,0,1)| = 3$. For any $\mathbf{b}$, $\mathbf{v}_i \in \mathbb{Z}_2^n$ s.t. $|\mathbf{v}_1| + |\mathbf{v}_2| + \cdots + |\mathbf{v}_s| \le 1$, the input of correlated sources $[\mathbf{b}+\mathbf{v}_1, \mathbf{b}+\mathbf{v}_2, \cdots, \mathbf{b}+\mathbf{v}_s]$ will result in syndrome $\left[\left(\begin{smallmatrix} G_1(\mathbf{b}+\mathbf{v}_1) \\ C_1(\mathbf{b}+\mathbf{v}_1) \end{smallmatrix}\right), \left(\begin{smallmatrix} G_2(\mathbf{b}+\mathbf{v}_2) \\ C_2(\mathbf{b}+\mathbf{v}_2) \end{smallmatrix}\right), \cdots, \left(\begin{smallmatrix} G_s(\mathbf{b}+\mathbf{v}_s) \\ C_s(\mathbf{b}+\mathbf{v}_s) \end{smallmatrix}\right)\right]$ to be received at the decoder. Given $C_i(\mathbf{b}+\mathbf{v}_i)$ at the decoder, we can recover $Q_i(\mathbf{b}+\mathbf{v}_i)$ from Remark 2.

The decoder can then retrieve $(\mathbf{v}_1, \cdots, \mathbf{v}_s)$ since $Q_1(\mathbf{b}+\mathbf{v}_1) + Q_2(\mathbf{b}+\mathbf{v}_2) + \cdots + Q_s(\mathbf{b}+\mathbf{v}_s) \overset{(a)}{=} Q_1(\mathbf{v}_1) + \cdots + Q_s(\mathbf{v}_s) \overset{(b)}{=} P \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_s \end{pmatrix}$, where (a) and (b) are due to (3) and (2), respectively, and P is bijective over the set of all length-sn vectors with weight 1.

After knowing $(\mathbf{v}_1, \cdots, \mathbf{v}_s)$, we can compute $G_1\mathbf{b}, \cdots, G_s\mathbf{b}$ and $C_1\mathbf{b}, \cdots, C_s\mathbf{b}$. This in turn gives us $T\mathbf{b}$ and $Y\mathbf{b}$, respectively, (the latter is again by Remark 2). So we have $R\mathbf{b}$. Since R is invertible, we can retrieve $\mathbf{b}$ and thus all sources.

The second claim is apparent by simple counting. ∎

Definition 7 (Generalized HCMS)**.** We call a code composed of the coding matrices described in Theorem 2 as a Generalized HCMS.

Example 2 (Generalized HCMS of three sources of length-1)**.** Let us revisit Remark 1. For the case $s = 3$, $n = 1$, and $M = 3$, consider the Hamming matrix $P = \left(\begin{smallmatrix}101\\011\end{smallmatrix}\right) = [Q_1 Q_2 Q_3]$ we must obtain $C_1 = C_2 = C_3 = [1]$. $\left(\begin{smallmatrix} C_1 \\ C_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \Rightarrow Y = [1]$ and T is void and hence G_i are void. So $d_1 = d_2 = d_3 = d = 1$ and $d_1 + d_2 + d_3 + (n - d) = M$. So from generalized HCMS, we get perfect compression with coding matrices [1], [1], and [1] just as in Remark 1.

Note that even a generalized HCMS does not guarantee the existence of perfect compression. For example, it has been proven there is no perfect compression for $s = 3$, $n = 5$, and $M = 3$ [17]. On the other hand, we showed in [18] that HCMS for three sources exists when n and M satisfy (1) and $n > 5$.

IV. Universality of Generalized HCMS

We will now prove that every perfect compression for Hamming sources S is equivalent to a generalized HCMS. We say two perfect compressions are equivalent (denoted by $\sim$) to each other if and only if their nullspaces can be converted to each other through the steps of the *nullspace shifting* as to be described in Lemma 1. Since each step of nullspace shifting is invertible, the term "equivalent" is mathematically justified. In essence, the objective of this section is to prove the following theorem.

Theorem 3. *Every perfect compression of a Hamming source is equivalent to a generalized HCMS.*

The outline of the proof is as follows. First, we will show the special case that every 2-source perfect compression is equivalent to a Hamming code (c.f. Lemma 2 below). We will then connect any perfect multi-source compression to a perfect compression of two sources with Hamming codes by direct construction (c.f. Lemma 3 below). Using Lemma 1 [18], we will show that any perfect compression can be "transformed" to a perfect compression of an *asymmetric* setup (c.f. Lemma 4 below) and thus we can focus ourselves only in this asymmetric case. Finally, with the help of Lemmas 2 and 3, we show by construction that any perfect compression of the *asymmetric* setup is equivalent to a generalized HCMS and thus conclude our proof by combining this result along with Lemma 3 (c.f. Theorem 3).

Before we continue, we would like to clarify some of our notations used in the rest of the paper.

1) For an $m \times n$ matrix H over $\mathbb{Z}_2$. We denote the nullspace of H as $\text{null}H = \{v \in \mathbb{Z}_2^n | Hv = 0\}$.
2) Let U and V be some subspaces of $\mathbb{Z}_2^n$. We denote the sum of the two vector spaces as $U + V = \{u + v | u \in U, v \in V\}$. Moreover, we will write $U + V$ as $U \oplus V$ to indicate a "direct" sum when $U \cap V = \{\mathbf{0}\}$.

We will now restate an important lemma that defines nullspace shifting [18]. In a nutshell, the lemma tells us that it is possible to tradeoff the compression rates of different source tuples by shifting a part of the nullspace of a coding matrix to another. Simply put, any overlapping of the nullspaces among all except one coding matrice H_r can be shifted, partially or entirely, to H_r from all other matrices to form a new nullspace combination. The resulting matrices will work as well as the original.

Lemma 1. *Let $H_1, \cdots, H_s$ be coding matrices of a SW code that can compress S. Suppose there exist vector spaces K and N_i, $1 \le i \le s$, such that $\text{null}H_i = K \oplus N_i$ when $i \ne r$ and $\text{null}H_r = N_r$. Then matrices $H_1', ..., H_s'$, with $\text{null}H_i' = K \oplus N_i$ when $i \ne d$ and $\text{null}H_d' = N_d$, can also compress S.*

Furthermore, if all H'_j are full row rank matrices and $(H_1, \cdots, H_s)$ is a perfect compression, then $(H'_1, ..., H'_s)$ is also a perfect compression [18].

The following lemma can be viewed as an illustration of Lemma 1. It is interesting in its own right and indispensable in the proof of Theorem 3.

Lemma 2. *Every 2-source perfect compression of* a Hamming source *is equivalent to a HCASWC.*

Proof: Let $s = 2$. If (H_1, H_2) can compress a Hamming source, then by Fact 3 in the Appendix, we have $\text{null}H_1 \cap \text{null}H_2 = \{\mathbf{0}\}$. Therefore we can let $N_1 = \{\mathbf{0}\}$ and $K = \text{null}(H_1)$ and construct (H'_1, H'_2) using Lemma 1. Having $\{\mathbf{0}\}$ as nullspace, H'_1 can be any invertible $n \times n$ matrix and we can set H'_1 to the identity matrix without loss of generality. Meanwhile, since (H'_1, H'_2) is perfect, H'_2 is a full rank $m \times n$ matrix with $m = M - n = \log_2(2^n(n+1)) - n = \log_2(n+1)$. And since the columns of H'_2 must be nonzero and different from each other, H'_2 is unique up to a permutation of columns. Therefore, H'_2 is an $(M-n)$-bit Hamming matrix and (H'_1, H'_2) is a HCASWC. Conversely, we can construct (H_1, H_2) (up to their nullspaces) from (H'_1, H'_2) by Lemma 1. That means any perfect compression is equivalent to a Hamming code under Lemma 1. ∎

The special case as described in Lemma 2 is an important intermediate step to show our main result depicted in Theorem 3. The significance of Lemma 2 may not be apparent as it only deals with two sources while Theorem 3 is meant for more than two sources. However, the following lemma provides a crucial link in extending Lemma 2 to the more general case.

Lemma 3. *Given the coding matrices, $(H_1, \cdots, H_s)$, of a perfect (s, n, M)-compression, we can form a perfect $(2, sn, M+(s-1)n)$-compression with coding matrices (X, J), where*

$$X = \begin{pmatrix} I & I & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & I & I & 0 & \cdots & 0 & 0 & 0 \\ & & & \cdots & & & & \\ 0 & 0 & 0 & 0 & \cdots & 0 & I & I \end{pmatrix} \tag{7}$$

is a $(s-1)n \times sn$ matrix, and

$$J = \begin{pmatrix} H_1 & 0 & \cdots & 0 \\ 0 & H_2 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & H_s \end{pmatrix} \tag{8}$$

is a $M \times sn$ matrix, and I denotes the $n \times n$ identity matrix.

Proof: Since $2^n(sn+1) = 2^M$ implies $2^{(sn)}((sn)+1) = 2^{M+(s-1)n}$ (c.f. (1)), we only need to show how to retrieve the input vectors. Let us decompose any pair of the input vectors for X and J, respectively, into $\begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \cdots \\ \mathbf{b}_s \end{pmatrix}$ and $\begin{pmatrix} \mathbf{b}_1+\mathbf{v}_1 \\ \cdots \\ \mathbf{b}_s+\mathbf{v}_s \end{pmatrix}$, where $\mathbf{b}_i$'s are n-entry vectors, $\mathbf{v}_i$'s are also n-entry vectors but restricted to the condition $|\mathbf{v}_1| + \cdots + |\mathbf{v}_s| \le 1$, where $|\cdot|$ maps an element in $\mathbb{Z}_2^n$ to its norm in $\mathbb{Z}$ by counting the number of nonzero components.

From the output of X, we will get $\mathbf{b}_1+\mathbf{b}_2, \mathbf{b}_2+\mathbf{b}_3, \cdots, \mathbf{b}_{s-1}+\mathbf{b}_s$. Thus we can obtain $\mathbf{b}_1+\mathbf{b}_2, \mathbf{b}_1+\mathbf{b}_3, \cdots, \mathbf{b}_1+\mathbf{b}_s$ and $H_2(\mathbf{b}_1+\mathbf{b}_2), H_3(\mathbf{b}_1+\mathbf{b}_3), \cdots, H_s(\mathbf{b}_1+\mathbf{b}_s)$.

From the output of J, we will obtain $H_2(\mathbf{b}_2+\mathbf{v}_2), H_3(\mathbf{b}_3+\mathbf{v}_3), \cdots, H_s(\mathbf{b}_s+\mathbf{v}_s)$ and $H_1(\mathbf{b}_1+\mathbf{v}_1)$. Combining the results, we get $H_1(\mathbf{b}_1+\mathbf{v}_1), H_2(\mathbf{b}_1+\mathbf{v}_2), \cdots, H_s(\mathbf{b}_1+\mathbf{v}_s)$. Since $(H_1, \cdots, H_s)$ is a perfect compression, we can compute $\mathbf{b}_1, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_s$. Together with the output of X, we can retrieve all $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_s$ and $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_s$. ∎

Notice that in Lemma 3, we have

$$\begin{aligned} \text{null}X &= \left\{ \begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c} \end{pmatrix} \middle| \mathbf{c} \in \mathbb{Z}_2^n \right\}, \\ \text{null}J &= \left\{ \begin{pmatrix} \mathbf{n}_1 \\ \vdots \\ \mathbf{n}_s \end{pmatrix} \middle| \mathbf{n}_i \in \text{null}H_i \right\}. \end{aligned} \tag{9}$$

Then Lemma 1 tells us that two full row rank matrices with nullspaces $\{0\}$ and $\text{null}X \oplus \text{null}J$[3], respectively, are also a perfect compression. From the proof of Lemma 2, the first matrix is an invertible matrix and the second one is a $M+(s-1)n-sn = M-n$-bit Hamming matrix. Let us denote the latter matrix as P. Then

$$\text{null}P = \text{null}X \oplus \text{null}J. \tag{10}$$

Partition P into

$$P = [Q_1 Q_2 \cdots . Q_s], \tag{11}$$

such that Q_i is a $(M-n) \times n$ matrix. We have

$$Q_1 + Q_2 + \cdots + Q_s = 0 \tag{12}$$

because $\text{null}X \subset \text{null}P$.

Secondly, $\text{null}J \subset \text{null}P$ implies

$$\text{null}H_i \subset \text{null}Q_i \tag{13}$$

for $1 \le i \le s$. Furthermore, for any

$$\mathbf{b}_i \in \text{null}Q_i, \tag{14}$$

we have $\begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{b}_i \\ \vdots \\ \mathbf{0} \end{pmatrix} \in \text{null}P$ and we can decompose it into $\begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c} \\ \vdots \\ \mathbf{c} \end{pmatrix} + \begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c}+\mathbf{b}_i \\ \vdots \\ \mathbf{c} \end{pmatrix}$. Since $\begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c} \\ \vdots \\ \mathbf{c} \end{pmatrix} \in \text{null}X$, by (10) we have

$$\begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c}+\mathbf{b}_i \\ \vdots \\ \mathbf{c} \end{pmatrix} \in \text{null}J, \tag{15}$$

and thus $\mathbf{c} \in \text{null}H_j$, $j \neq i$, and $\mathbf{c}+\mathbf{b}_i \in \text{null}H_i$. Let

$$L_i = \bigcap_{1 \le j \le s | j \neq i} \text{null}H_j, \tag{16}$$

then we have $c \in L_i$. Suppose $L_i = \{\mathbf{0}\}$, then $\mathbf{c} = \mathbf{0}$ and $\mathbf{b}_i \in \text{null}H_i$. Together with (13), we will get $\text{null}H_i = \text{null}Q_i$. It will be convenient for our analysis to have $L_i = \{\mathbf{0}\}$ for as many i as possible. Actually, it is possible to force a maximum number of $(s-1)$ intersections to satisfy this condition by applying Lemma 1 repeatedly. This is more precisely stated in the following lemma:

Lemma 4. *Given a perfect compression $(H'_1, H'_2, \cdots, H'_s)$, there exists $(H_1, \cdots, H_s) \sim (H'_1, \cdots, H'_s)$ s.t. $\text{null}H_1 \cap ... \cap \text{null}H_{i-1} \cap \text{null}H_{i+1} \cap ... \cap \text{null}H_s = 0$ for $1 \le i < s$.*

Proof: See Appendix. ∎

It is interesting to point out that the case considered in Lemma 4 corresponds to an asymmetric case where the maximum amount of rate is allocated to source s with the rest of the sources given minimally sufficient rates for lossless reconstruction. Now, we are ready to prove our main result.

[3]Note that $\text{null}X$ and $\text{null}J$ are orthogonal from Fact 3 in the Appendix since X and J form a compression for a Hamming source.

Proof of Theorem 3:

By Lemma 4, we can restrict our attention only to perfect compression whose coding matrices $H_1, \cdots, H_s$ satisfy $L_i = \{\mathbf{0}\}, 1 \le i < s$ (c.f. (16)) without loss of generality. Our goal here is to show that any of the aforementioned perfect compression can be transformed to some equivalent generalized HCMS.

To transform to a generalized HCMS, we first generate X and J according to (7) and (8) and hence a corresponding Hamming matrix P and its partition matrices Q_i (c.f. (11)). From the argument after Lemma 3, we have $\text{null}Q_i = \text{null}H_i$ for $i \neq s$. This does not hold for s because $L_s \neq \{\mathbf{0}\}$. Instead, we can compute $\text{null}Q_s$ as follows. Let Y be a row basis matrix of $\begin{pmatrix} Q_1 \\ \cdots \\ Q_{s-1} \end{pmatrix}$ as in the setup of the generalized HCMS, and thus

$$\text{null}Y = \text{null}Q_1 \cap \cdots \cap \text{null}Q_{s-1} = \text{null}H_1 \cap \cdots \cap \text{null}H_{s-1}. \quad (17)$$

With this, we can show

$$\text{null}Q_s = \text{null}H_s \oplus \text{null}Y \quad (18)$$

from the following:

- *$\text{null}Q_s \subset \text{null}H_s \oplus \text{null}Y$*: Following the same logic from (14) to (15), if we assume $\mathbf{b}_s \in \text{null}Q_s$, we have $\mathbf{c} \in \text{null}H_1 \cap \cdots \cap \text{null}H_{s-1} = \text{null}Y$ and $\mathbf{c} + \mathbf{b}_s \in \text{null}H_s$ by (15). Therefore, $\mathbf{b}_s = \mathbf{c} + \mathbf{b}_s + \mathbf{c} \in \text{null}H_s + \text{null}Y$. Since $\text{null}H_s \cap \text{null}Y = \text{null}H_1 \cap ... \cap \text{null}H_s = \mathbf{0}$ (c.f. Fact 3), we have $\text{null}Q_s \subset \text{null}H_s \oplus \text{null}Y$.
- *$\text{null}H_s \oplus \text{null}Y \subset \text{null}Q_s$*: Given $\mathbf{b}_s \in \text{null}H_s$ and $\mathbf{c} \in \text{null}Y$, $\begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{b}_s+\mathbf{c} \end{pmatrix} = \begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c} \\ \mathbf{c} \end{pmatrix} + \begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c} \\ \mathbf{b}_s \end{pmatrix} \in \text{null}P$ (c.f. (10)) because $\begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c} \\ \mathbf{c} \end{pmatrix} \in \text{null}X$ and $\begin{pmatrix} \mathbf{c} \\ \vdots \\ \mathbf{c} \\ \mathbf{b}_s \end{pmatrix} \in \text{null}J$ (c.f. (17)). Thus $\mathbf{0} = P \begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{b}_s+\mathbf{c} \end{pmatrix} = Q_s(\mathbf{b}_s + \mathbf{c})$. Hence $\mathbf{b}_s + \mathbf{c} \in \text{null}Q_s$ and so we have $\text{null}H_s \oplus \text{null}Y \subset \text{null}Q_s$.

Following the construction procedure of the generalized HCMS, we need to find a matrix T s.t.

$$R = \begin{pmatrix} Y \\ T \end{pmatrix} \quad (19)$$

is an invertible $n \times n$ matrix. Since the nullspaces of H_s and Y are orthogonal to each other (c.f. (18)), there exists a subspace A such that

$$\text{null}H_s \oplus \text{null}Y \oplus A = \mathbb{Z}_2^n. \quad (20)$$

Now, if we let T be a full row rank matrix with

$$\text{null}T = \text{null}H_s \oplus A, \quad (21)$$

we have

$$\text{null}T \oplus \text{null}Y = \mathbb{Z}_2^n. \quad (22)$$

Being a row basis matrix matrix of $\begin{pmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_{s-1} \end{pmatrix}$, Y is a full row rank matrix and this ensures that we can find T such that R is invertible (c.f.(19)).

We will now start to construct the coding matrix of the generalized HCMS. Denote C_i as a row basis matrix of Q_i for all i and consider the generalized HCMS with coding matrices $C_1, C_2, \cdots, C_{s-1}, \begin{pmatrix} T \\ C_s \end{pmatrix}$. We will prove that the code is equivalent to the target perfect code by showing that each coding matrix is a full row rank matrix and shares the same nullspace with the corresponding coding matrix of the target code. More precisely, we need to show

1) C_i to be full row rank matrices and $\text{null}C_i = \text{null}H_i$ for $1 \le i < s$; and
2) $\begin{pmatrix} T \\ C_s \end{pmatrix}$ to be a full row rank matrix and $\text{null}\begin{pmatrix} T \\ C_s \end{pmatrix} = \text{null}H_s$.

We got 1) easily since each C_i is a row basis matrix of Q_i and $\text{null}Q_i = \text{null}H_i$. So we only need to show 2) to finish the proof.

Since C_s is a row basis matrix of Q_s, we have

$$\text{row}C_s = \text{row}Q_s \subset \text{row}\begin{pmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_{s-1} \end{pmatrix} = \text{row}Y, \quad (23)$$

where $\text{row}Q_s \subset \text{row}\begin{pmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_{s-1} \end{pmatrix}$ is due to $Q_s = Q_1 + Q_2 + ... + Q_{s-1}$ (c.f. (12)) and $\text{row}\begin{pmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_{s-1} \end{pmatrix} = \text{row}Y$ since Y is a row basis matrix matrix of $\begin{pmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_{s-1} \end{pmatrix}$. Then we have $\begin{pmatrix} T \\ C_s \end{pmatrix}$ to be a full row rank matrix as desired because its row vectors are linear independent, thanks to (23) and the fact that $R = \begin{pmatrix} Y \\ T \end{pmatrix}$ is invertible (c.f. (19)). Further, $\text{null}\begin{pmatrix} T \\ C_s \end{pmatrix} = \text{null}T \cap \text{null}C_s = \text{null}T \cap \text{null}Q_s$ since C_s is a row basis matrix of Q_s. But $\text{null}Q_s \cap \text{null}T = (\text{null}H_s \oplus \text{null}Y) \cap \text{null}T$. Since $\text{null}H_s \subset \text{null}T$ (c.f. (21)), we can apply Fact 2 (see Appendix) to obtain $\text{null}Q_s \cap \text{null}T = (\text{null}T \cap \text{null}Y) \oplus \text{null}H_s = 0 \oplus \text{null}H_s$ (c.f. (22)) $= \text{null}H_s$. Therefore, we have $\text{null}\begin{pmatrix} T \\ C_s \end{pmatrix} = \text{null}H_s$ as desired.

■

V. Discussions and Conclusions

This paper concludes our effort in seeking perfect codes for Hamming sources with an arbitrary number of sources. In [18], we showed the existence of such codes. In this paper, we showed that for any perfect code in Hamming sources, there is an equivalent generalized HCMS and all can be derived from a Hamming matrix.

A contribution of this work is to further strenghten the connection of a perfect code in channel coding and that in SW coding, where for the case with more than two sources, the proof is highly non-trivial but can be shown with a significant amount of effort as illustrated in this paper. One may wonder the usefulness of the current work due to the restrictiveness of the Hamming source model. Indeed, extending to more complicated correlation models could be a very difficult task. For a more complex model, it is probably extremely challenging just to show if a perfect code exists or can be constructed using linear codes. However, we believe that our experience in this series of work (along with [17], [18]) should provide valuable insight to future researchers who choose to pursue this challenge. To summarize, the following suggestions may be useful:

1) *Do not underestimate the importance of the two-source scenario*. It was surprising to us that multi-source ($s > 2$) cases will turn out to be so tightly coupled with the two-source case ($s = 2$) (via Lemma 3). For more complex models, we will recommend researchers to also closely look into this special case first.
2) *Seek a "nullspace shifting" lemma for the corresponding model.* Lemma 1 [18] is a cornerstone of the entire series of our work. It essentially allows us to shift the rate flexibly from one encoder to another without changing the property of the code. We envision a similar lemma will be necessary in extending our results to any correlation model.
3) *Focus on an asymmetric case.* If a "nullspace shifting" lemma exists, it will always be helpful to focus on an asymmetric case (as described in Lemma 4) since it corresponds to a corner point in the SW region and is typicially the simplest case. In particular, it is highly likely that only one encoder will need

special treatment in the asymmetric case (i.e., Encoder s in the Proof of Theorem 3).

■

APPENDIX

Simple facts

Fact 1. *For vector spaces U, V, and W, it is easy to show that*

$$(V+U)\cap W \subset (V\cap W)+U \text{ if } U\subset W. \tag{24}$$

Proof: Let $v\in V, u\in U$ that $v+u\in W$. Then $u\in U\subset W \Rightarrow v\in W \Rightarrow v\in V\cap W$. As a result $v+u\in (V\cap W)+U$. ■

Fact 2. *For vector spaces V, U, and W, $(V\oplus U)\cap W=(V\cap W)\oplus U$ if $U\subset W$.*

Proof: From Fact 1, we know that $(V+U)\cap W\subset (V\cap W)+U$. Now let $\mathbf{v}\in V\cap W$, $\mathbf{u}\in U\subset W$. Then $\mathbf{v}+\mathbf{u}\in W$ and $\mathbf{v}+\mathbf{u}\in V+U$. Therefore $(V\cap W)+U\subset (V+U)\cap W$. Lastly, we notice that $V\cap U=(V\cap W)\cap U$ as $U\subset W$. Hence $V\cap U=\{\mathbf{0}\}$ iff $(V\cap W)\cap U=\{\mathbf{0}\}$, that justifies the direct sum signs. ■

Fact 3. *If a code with coding matrices $H_1, H_2, \cdots, H_s$ can compress a Hamming source S, then we must have null$H_1\cap$ null$H_2\cap\cdots\cap$ null$H_s=\{\mathbf{0}\}$.*

Proof: If there exists some vector $\mathbf{c}\neq\mathbf{0}$ and $\mathbf{c}\in H_1\cap \text{null}H_2\cap\cdots\cap\text{null}H_s$, then the source outcome with all s terminals equal to $\mathbf{c}$ will share the same codeword as the outcome with all s terminals equal to $\mathbf{0}$. Since both of them are in S, therefore the mapping restricted to S is not surjective and thus contradicts with the assumption that the code can compress S. ■

Proof of Lemma 4

Let $R_i=\bigcap_{1\le j\le s|j\neq i}\text{null}H'_j$. Notice that if all $i\neq s$, $R_i=\{\mathbf{0}\}$, then we are finished as there is nothing to prove. In general we can still make use of Lemma 1 to shift each R_i from encoder s to encoder i. After the shifting, the new R_i, that we would call L_i, should have a zero dimension. Let us see the details. We have

$$R_i\subset \text{null}H'_j, \text{ for } i\neq j, \tag{25}$$

and

$$R_i\cap R_k=\bigcap_{1\le j\le s}\text{null}H'_j \overset{(a)}{=} \{\mathbf{0}\} \text{ for } i\neq k, \tag{26}$$

where (a) is due to Fact 3.

By (25) and (26), there exists a space N_s that we can decompose

$$\text{null}H'_s=N_s\oplus R_1\oplus ...\oplus R_{s-1}. \tag{27}$$

Apply Lemma 1 for $s-1$ times, we can form an equivalent perfect compression by first moving the entire R_i (i.e., K in Lemma 1) from nullH'_s to nullH'_i for i runs from 1 to $s-1$ and obtain

$$N_i=\text{null}H'_i\oplus R_i, 1\le i<s. \tag{28}$$

Then if we let H_j be a full row rank matrix with

$$\text{null}H_j=N_j \text{ for } 1\le j\le s, \tag{29}$$

we have $(H_1,\cdots,H_s)\sim(H'_1,\cdots,H'_s)$.

Recall that $L_i=\bigcap_{1\le j\le s|j\neq i}\text{null}H_j=\bigcap_{1\le j\le s|j\neq i}N_j$ We still need to show $L_i=\{\mathbf{0}\}$ for $1\le i<s$.

By symmetry, we only need to show that $L_1=\{\mathbf{0}\}$. By (28), we have $N_2\subset\text{null}H'_2\oplus R_2$. Suppose $N_2\cap\cdots\cap N_k\subset(\text{null}H'_2\cap\cdots\cap\text{null}H'_k)+(R_2+\cdots+R_k)$ for a $k<s-1$. Then $N_2\cap\cdots\cap N_{k+1}$ is a subset of

$$((\text{null}H'_2\cap\cdots\cap\text{null}H'_k)+(R_2+\cdots+R_k))\cap(\text{null}H'_{k+1}+R_{k+1}) \tag{30}$$

by induction hypothesis.

By (25), we have $R_2+\cdots+R_k\subset\text{null}H'_{k+1}\subset\text{null}H'_{k+1}+R_{k+1}$. So we can apply Fact 1 on (30) and thus obtain $N_2\cap\cdots\cap N_{k+1}$ as a subset of $((\text{null}H'_2\cap..\cap\text{null}H'_k)\cap(\text{null}H'_{k+1}+R_{k+1}))+(R_2+\cdots+R_k)$. Apply Fact 1 once more with $V=\text{null}H'_{k+1}, U=R_{k+1}, W=\text{null}H'_2\cap\cdots\cap\text{null}H'_k$, and we have (c.f. (25) for $U\subset W$) $N_2\cap\cdots\cap N_{k+1}$ to be a subset of $(\text{null}H'_2\cap\cdots\cap\text{null}H'_{k+1})+R_2+R_3+\cdots+R_{k+1}$. By induction we get $N_2\cap\cdots\cap N_{s-1}\subset(\text{null}H'_2\cap\cdots\cap\text{null}H'_{s-1})+R_2+\cdots+R_{s-1}$.

Lastly, $N_2\cap\cdots\cap N_s\overset{(a)}{\subset}((\text{null}H'_2\cap\cdots\cap\text{null}H'_{s-1})+R_2+\cdots+R_{s-1})\cap\text{null}H'_s\overset{(b)}{\subset}(\text{null}H'_2\cap\cdots\cap\text{null}H'_s)+R_2+\cdots+R_{s-1}\overset{(c)}{=}R_1+R_2+\cdots+R_{s-1}$, where (a) is due to $N_s\in\text{null}H'_s$ (c.f. (27)), (b) is due to Fact 1, and (c) is from the definition of R_1.

Thus, $N_2\cap\cdots\cap N_s\subset(R_1+\cdots+R_{s-1})\cap N_s=\{\mathbf{0}\}$, where the last equality is from the construction of N_s (c.f. (27)). ■

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their constructive comments. In particular, a suggestion triggered a reorganization of the paper which improved the readability significantly. They also caught numerous typos and mistakes in the earlier drafts. We would also like to thank Ms. Renee Wagenblatt for correcting grammar mistakes and typos in previous drafts.

REFERENCES

[1] A. Wyner, “Recent results in the Shannon theory,” *IEEE Trans. Inform. Theory*, vol. 20, pp. 2–10, Jan. 1974.
[2] S. S. Pradhan and K. Ramchandran, “Distributed source coding using syndromes (DISCUS): design and construction,” in *Proc. DCC*, 1999, pp. 158–167.
[3] V. Stankovic, A. D. Liveris, Z. Xiong, and C. N. Georghiades, “On code design for the Slepian-Wolf problem and lossless multiterminal networks,” *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1495–1507, 2006.
[4] S. Pradhan and K. Ramchandran, “Generalized coset codes for distributed binning,” *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3457–3474, 2005.
[5] Y. Yang, S. Cheng, Z. Xiong, and Z. Wei, “Wyner-Ziv coding based on TCQ and LDPC codes,” in *Proc. Asilomar*, vol. 1, 2003, pp. 825–829.
[6] A. Liveris, Z. Xiong, and C. Georghiades, “Nested convolutional/turbo codes for the binary Wyner-Ziv problem,” in *Proc. ICIP’03*, Barcelona, Spain, Sep 2003.
[7] J. Chou, S. Pradhan, and K. Ramchandran, “Turbo and trellis-based constructions for source coding with side information,” in *Proc. DCC’03*, Snowbird, UT, Mar 2003.
[8] P. Mitran and J. Bajcsy, “Coding for the Wyner-Ziv problem with turbo-like codes,” in *Proc. ISIT’02*, Lausanne, Switzerland, Jun 2002.
[9] X. Wang and M. Orchard, “Design of trellis codes for source coding with side information at the decoder,” in *Proc. DCC’01*, Snowbird, UT, Mar 2001.
[10] S. Servetto, “Lattice quantization with side information,” in *Proc. DCC’00*, Snowbird, UT, Mar 2000.
[11] M. Zamani and F. Lahouti, “A flexible rate Slepian-Wolf code construction,” *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2301–2308, 2009.
[12] D. Schonberg, K. Ramchandran, and S. S. Pradhan, “Distributed code constructions for the entire Slepian-Wolf rate region for arbitrarily correlated sources,” in *Proc. DCC’04*, Snowbird, UT, 2004, pp. 292–301.
[13] B. Rimoldi and R. Urbanke, “Asynchronous Slepian-Wolf coding via source-splitting,” in *Proc. ISIT’97*, Ulm, Germany, 1997, p. 271.
[14] J. Garcia-Frias and Y. Zhao, “Near-Shannon/Slepian-Wolf performance for unknown correlated sources over AWGN channels,” *IEEE Trans. Commun.*, vol. 53, no. 4, pp. 555–559, 2005.

[15] J. Chen, D.-k. He, A. Jagmohan, and L. A. Lastras-Montano, “On the reliability function of variable-rate Slepian-Wolf coding,” in *45th Annual Allerton Conference*, Urbana-Champaign, IL, 2007.

[16] A. Liveris, C. Lan, K. Narayanan, Z. Xiong, and C. Georghiades, “Slepian-Wolf coding of three binary sources using LDPC codes,” in *Proc. Intl. Symp. Turbo Codes and Related Topics*, 2003.

[17] S. Cheng and R. Ma, “The non-existence of length-5 perfect slepian-wolf codes of three sources,” in *Proc. DCC’10*. Snowbird, UT, Mar 2010.

[18] R. Ma and S. Cheng, “Hamming coding for multiple sources,” in *Proc. ISIT’10*, Austin, TX, Jun. 2010.

[19] A. Al Jabri and S. Al-Issa, “Zero-error codes for correlated information sources,” *Crytography and Coding*, pp. 17–22, 1997.

[20] P. Koulgi, E. Tuncel, S. Regunathan, and K. Rose, “Minimum redundancy zero-error source coding with side information,” in *Proc. ISIT*. IEEE, 2001, p. 282.

[21] ——, “On zero-error source coding with decoder side information,” *IEEE Trans. Inform. Theory*, vol. 49, no. 1, pp. 99–111, 2003.

[22] Y. Yan and T. Berger, “On instantaneous codes for zero-error coding of two correlated sources,” in *Proc. ISIT*. IEEE, 2000, p. 344.

[23] D. Slepian and J. Wolf, “Noiseless coding of correlated information sources,” *IEEE Trans. Inform. Theory*, vol. 19, pp. 471–480, Jul. 1973.

[24] H. Witsenhausen, “The zero-error side information problem and chromatic numbers (corresp.),” *IEEE Trans. Inform. Theory*, vol. 22, no. 5, pp. 592–593, 1976.