

Zero-error Slepian-Wolf Coding of Confined-Correlated Sources with Deviation Symmetry

Rick Ma* and Samuel Cheng†

October 31, 2018

Abstract

In this paper, we use linear codes to study zero-error Slepian-Wolf coding of a set of sources with deviation symmetry, where the sources are generalization of the Hamming sources over an arbitrary field. We extend our previous codes, *Generalized Hamming Codes for Multiple Sources*, to *Matrix Partition Codes* and use the latter to efficiently compress the target sources. We further show that every perfect or linear-optimal code is a Matrix Partition Code. We also present some conditions when Matrix Partition Codes are perfect and/or linear-optimal. Detail discussions of Matrix Partition Codes on Hamming sources are given at last as examples.

1 Introduction

Slepian-Wolf (SW) Coding or Slepian-Wolf problem refers to separate encoding of multiple correlated sources but joint lossless decoding of the sources [1]. Since then, many researchers have looked into ways to implement SW coding efficiently. Noticeably, Wyner was the first who realized that linear coset codes can be used to tackle the problem [2]. Essentially, considering the source from each terminal as a column vector, the encoding output will simply be the multiple of a “fat”¹ coding matrix and the input vector. The approach was popularized by Pradhan *et al.* more than two decades later [3]. Practical syndrome-based schemes for S-W coding using channel codes have been further studied in [4, 5, 6, 7, 8, 9, 10, 11, 12].

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 [13, 14, 15, 16, 17]. So we say the SW code can *compress* S only if any source tuple in S can be reconstructed losslessly. Obviously, a SW code can compress S if and only if its encoding map restricted to S is injective (or 1-1).

*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.

¹The input matrix is “fat” so that the length of encoded vector will be shorter than or equal to the original.

The source model for zero-error SW coding can be quite a bit different from the typical probabilistic model studied in classic SW coding literatures. For example, 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, and in the source that is different from the rest, only one bit differs from the corresponding bit of other sources. Such source is known to be *Hamming source* [18] since it turns out that it is closely related to Hamming codes.

In [18], we described a generalized syndrome based coset 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 [19], 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 [17], we extended HCMS to *generalized HCMS*. And we showed that any perfect SW code for a Hamming source is equivalent to a generalized HCMS (c.f. Theorem 3 in [17]).

Despite our prior results, Hamming source is a very restricted kind of sources and only binary Hamming sources had been studied in the past. In this paper, we extend our prior works to input sources in arbitrary fields. Moreover, we introduce a much general kind of sources with deviation symmetry as to be spelled out in Definition 2.5. We will also show such sources can be handled systematically with the proposed *Matrix Partition Codes*, which can be interpreted as an extension of the generalized HCMS described in [17]. We also show that the Matrix Partition Codes of any linear-optimal compression (i.e., higher compression is impossible) is a Matrix Partition Code. We also present some conditions when the Matrix Partition Codes are perfect and/or linear-optimal. Some more detail discussions are further given for special cases such as Hamming sources.

Let us briefly summarize here the notations and conventions used in this paper. Matrices are generally denoted with upper case letters while vectors are denoted by lower case letters. Sets are denoted using script font and fields are denoted using blackboard bold letter font. As matrices are used as mapping during encoding, we call a matrix *injective* (*surjective*) when the mapping corresponding to the matrix is injective (surjective). We may also specify the domain of the mapping. When none is specified, it is understood that the domain contains all possible vectors. For example, we say $A|_{\mathcal{S}}$ is injective if the mapping corresponding to matrix A with input domain \mathcal{S} is injective. In other words, for any $\sigma_1, \sigma_2 \in \mathcal{S}$ and $\sigma_1 \neq \sigma_2$, $A\sigma_1 \neq A\sigma_2$. Further, we call a matrix A a *row basis matrix* of a matrix B if rows of A form a basis of the row space of B .

This rest of the paper is organized as follows. In the next section, we will introduce the target sources with deviation symmetry and the Matrix Partition Codes. We will include some motivations of the setup in Section 2.1 and also derive the maximum possible compression achievable by a Matrix Partition Code. In Section 3, we discuss when a Matrix Partition Code will be *perfect*. Moreover, we use generalized Hamming sources as an example and derive the necessary conditions of perfectness. In Section 4, we present the major result of this paper—the uniqueness of Matrix Partition Codes. In Section 5, we will

present some new results that are restricted to a subset of sources with deviation symmetry, the Hamming sources. In Section 6, before concluding the paper, we will determine the condition on the source under which actual compression is possible.

2 Target Sources and Proposed Codes

2.1 Confined-Correlated Source and Connection to Classic Probabilistic Source Models

Slepian-Wolf (SW) coding is typically referred to as the (near-)lossless compression of jointly correlated sources with separate encoders but a joint decoder. And the source is usually modeled probabilistically in the *classic* setup. More precisely, an s terminal system can have the sources X_1, X_2, \dots, X_s , sampled from some joint distribution $p(x_1, x_2, \dots, x_s)$ at each time instance independent of another time instances.

Let us consider a simple example of a two terminal source ($s = 2$) with $Pr(X_1 = 0, X_2 = 0) = Pr(X_1 = 1, X_2 = 1) = 0.4$ and $Pr(X_1 = 1, X_2 = 0) = Pr(X_1 = 0, X_2 = 1) = 0.1$. One can see that the marginal distributions of both terminals are uniformly distributed (i.e., $Pr(X_1 = 1) = Pr(X_1 = 0) = Pr(X_2 = 1) = Pr(X_2 = 0) = 0.5$). Thus, any sequence drawn from each terminal will be equally likely and applying *variable length* code on a sequence from one terminal will not improve compression efficiency. Note that this is true in many scenarios when such kind of symmetry exists and will be described more precisely in Definition 2.5.

Given a block of n source sequence tuples $(\mathbf{x}_1, \dots, \mathbf{x}_s)$ sampled from the joint source (where each \mathbf{x}_i has length n), the encoders Enc_1, \dots, Enc_s apply on their corresponding source sequences only. That is, we have the i^{th} encoding output

$$\mathbf{y}_i = Enc_i(\mathbf{x}_i) \quad (2.1)$$

has length m_i and is independent of \mathbf{x}_j , $j \neq i$. For any encoder i , we choose to have the codeword length m_i fixed (independent of the input sequence) since as we mentioned in the previous paragraph, variable length coding is not going to increase efficiency for the symmetric source that we consider here.

Receiving the compressed outputs $\mathbf{y}_1, \dots, \mathbf{y}_s$, a joint decoding map Dec will try to recover the source blocks from all terminals. That is,

$$(\hat{\mathbf{x}}_1, \dots, \hat{\mathbf{x}}_s) = Dec(\mathbf{y}_1, \dots, \mathbf{y}_s), \quad (2.2)$$

where $\hat{\mathbf{x}}_i$ is the estimate of \mathbf{x}_i .

The problem of the aforementioned probabilistic setup is that for a finite n , true lossless compression is generally not possible. Denote \mathcal{S} as the set of all possible $(\mathbf{x}_1, \dots, \mathbf{x}_s)$ that can be sampled from the source. Define an encoding map

$$Enc(\mathbf{x}_1, \dots, \mathbf{x}_s) = (Enc_1(\mathbf{x}_1), \dots, Enc_s(\mathbf{x}_s)). \quad (2.3)$$

Obviously, for a SW coding scheme to be *truly* lossless, we must have the restricted map $Enc|_{\mathcal{S}}$ to be injective (i.e., no two possible inputs will result in the

same encoded output). Denote \mathcal{X}_i and \mathcal{Y}_i as the alphabets of input and output of the i^{th} encoder, respectively. For a finite n and a general distribution that $p(x_1, \dots, x_s) \neq 0$ for any combination of scalars x_1, \dots, x_s , every $(\mathbf{x}_1, \dots, \mathbf{x}_s)$ will have a non-zero probability and thus is in \mathcal{S} . This essentially means that the size of the compressed source $|\mathcal{Y}_1^{m_1} \times \dots \times \mathcal{Y}_s^{m_s}|$, which has to be larger than $|\mathcal{S}|$ for true *lossless* recovery, is just $|\mathcal{X}_1^n \times \dots \times \mathcal{X}_s^n|$. Therefore, one cannot have both true lossless recovery and real compression (i.e., the net encoded output is smaller than the input) in this case.

The catch here is that in a classic SW setup, we will allow n to go to infinity. In consequence, for any distribution, we will have some $(\mathbf{x}_1, \dots, \mathbf{x}_s)$ (the jointly typical sequences) to have much higher probabilities than the rest, in such an extend that the other joint sequences will have negligible probabilities (essentially 0 as n goes to infinity) and can be ignored. Thus we will have $|\mathcal{S}|$ smaller than $|\mathcal{X}_1^n \times \dots \times \mathcal{X}_s^n|$ if we exclude joint sequences that almost never happen. And this gives us a near-lossless compression for a very large but finite n .

While the probabilistic approach of the classic SW setup leads to interesting theoretical performance bounds, an infinite n is not realistic in practice. In particular, unlike a channel coding problem that is typically designed to operate at a very high sampling rate, the sampling rate of a SW problem is not a design parameter but is determined by the nature of the source. For example, in a typical scenario where the sources are the temperature readings sampled from different locations, let say, every five minutes. A rather small n , say 100, will already correspond to over eight hours of delay. Such a delay may not be acceptable in practical scenarios.

To accommodate a finite delay, one may give up either the lossless requirement or the conventional probabilistic model. Giving up the lossless requirement will result in the general multiterminal source coding problem, a much more complicated setup where a general theoretical rate-distortion limit is still unknown. Instead, we will forfeit the conventional probabilistic model in this paper. Unlike the conventional SW case, the set \mathcal{S} containing all possible joint sequences is a proper subset of $\mathcal{X}_1^n \times \dots \times \mathcal{X}_s^n$ even when n is finite. We will call such source *confined-correlated source* to distinguish it from the conventional case. Another interpretation is simply that joint sequences are directly drawn from the set \mathcal{S} .

Definition 2.1 (Confined-Correlated Source). Given a subset \mathcal{S} of $\mathcal{X}_1^n \times \dots \times \mathcal{X}_s^n$, we call the source from which joint sequences are drawn a *confined-correlated source* if the probability of having a joint sequence outside \mathcal{S} is zero. Note that once \mathcal{S} has been defined, we will treat every element of its equally, regardless of the original probabilistic structure. And our discussion always directly starts with a given \mathcal{S} . Hence our coding is completely characterized by the source set \mathcal{S} .

Just as most other works in the literatures, we will focus on linear code in this paper. Here is our mathematical setting. Let \mathbb{F} be an arbitrary field. Let s, n, m_1, \dots, m_s be integers that $s \geq 2, n \geq 1, m_1 \geq 0, \dots, m_s \geq 0$. We restrict that $\mathcal{X}_1 = \dots = \mathcal{X}_s = \mathcal{Y}_1 = \dots = \mathcal{Y}_s = \mathbb{F}$. Hence the source \mathcal{S} is a subset of $\underbrace{\mathbb{F}^n \times \dots \times \mathbb{F}^n}_s$ and the output codeword space $\mathcal{C} = \mathbb{F}^{m_1} \times \dots \times \mathbb{F}^{m_s}$. Later we

will further require \mathcal{S} to be a source with deviation symmetry (Definition 2.5). The encoding map is linear in the sense that $Enc_i(\mathbf{x}_i) = H_i \mathbf{x}_i$, where H_i are $m_i \times n$ encoding matrices over \mathbb{F} for all i . We can have lossless compression only if $(H_1, \dots, H_s)|_{\mathcal{S}}$ is injective. Since we will only consider linear lossless compression in this paper, we will simply refer such kind of compression to as *compression* in the following, except for emphasis.

Beside injectivity, we certainly want the output space \mathcal{C} to be small. For this purpose, we define some measure to quantify its size.

Definition 2.2 (Total Code Length, Compression Sum-Ratio, Compression Ratio Tuples). The total code length M of compression (H_1, \dots, H_s) is given by $M = m_1 + \dots + m_s$, which is $\dim \mathcal{C}$. We also define the compression sum-ratio as M/n and the compression ratio tuples as $(m_1/n, \dots, m_s/n)$.

Definition 2.3 (Linear-Optimal Compression). A linear compression is said to be linear-optimal if there is no other linear compression with respect to the same source resulting in a shorter total code length.

Definition 2.4 (Perfect Compression). The compression (H_1, H_2, \dots, H_s) is said to be perfect if \mathbb{F} is finite and $|\mathcal{C}| = |\mathbb{F}|^M = |\mathcal{S}|$.

While there is always a linear-optimal compression scheme, perfect compression does not always exist. A perfect compression scheme is obviously linear-optimal but the converse may not be true.

2.2 Confined-Correlated Sources with Deviation Symmetry

Even with the restriction of linear codes, the considered problem is still too general. We will introduce the symmetric constraint mentioned in the last subsection to our target source. Namely, if a joint sequence σ belongs to a source \mathcal{S} , so does a uniform shift $\sigma + (\mathbf{v}, \mathbf{v}, \dots, \mathbf{v})$. The condition is a rather mild one. Actually, if we imagine that each source output are just readings derived from a common base source, such symmetry will natural arise if the observers are symmetrically setup.

Let us consider the equivalent relation on $\overbrace{\mathbb{F}^n \times \dots \times \mathbb{F}^n}^{s \text{ terms}}$ that

$$\sigma_1 \sim \sigma_2 \text{ iff } \sigma_1 - \sigma_2 = (\mathbf{v}, \dots, \mathbf{v}) \text{ for some } \mathbf{v} \in \mathbb{F}^n. \quad (2.4)$$

Then the equivalence classes derived from the equivalence relation partition the joint sequence space $\mathbb{F}^n \times \dots \times \mathbb{F}^n$ and we may redefine our target source as follows.

Definition 2.5 (Sources with Deviation Symmetry). A confined-correlated $\overbrace{s \text{ terms}}$ source $\mathcal{S} \subset \mathbb{F}^n \times \dots \times \mathbb{F}^n$ is said to be a *source with deviation symmetry* if \mathcal{S} is an union of equivalence classes derived from the equivalence relation specified by (2.4).

A source with deviation symmetry is completely characterized by its composite equivalence classes, where each can in term be specified by any one element of the equivalence class. Let us define a representative set as follow.

Definition 2.6 (Representative Set). A representative set \mathcal{D} of a source with deviation symmetry \mathcal{S} contains exactly one element of each equivalence class that is a subset of \mathcal{S} .

Obviously, \mathcal{D} is not unique and since \mathcal{D} contains exactly one element from an equivalence class, we have the following property.

$$\delta \in \mathcal{D} \Rightarrow (\mathbf{v}, \dots, \mathbf{v}) + \delta \notin \mathcal{D}, \forall \text{ non-zero } \mathbf{v} \in \mathbb{F}^n. \quad (2.5)$$

Furthermore, if both \mathcal{D} and \mathcal{E} are representation sets of \mathcal{S} , then there exists a mapping $\mathbf{v} : \mathcal{D} \mapsto \mathbb{F}^n$ such that

$$\mathcal{E} = \{(\mathbf{v}(\delta), \dots, \mathbf{v}(\delta)) + \delta \mid \delta \in \mathcal{D}\}. \quad (2.6)$$

And from Definition 2.6, source \mathcal{S} can be completely characterized by \mathcal{D} with

$$\mathcal{S}(\mathcal{D}) = \{(\mathbf{v}, \dots, \mathbf{v}) + \delta \mid \mathbf{v} \in \mathbb{F}^n, \delta \in \mathcal{D}\}. \quad (2.7)$$

Moreover, $\forall \sigma \in \mathcal{S}$, \exists a unique $\delta \in \mathcal{D}$ and a unique $\mathbf{v} \in \mathbb{F}^n$ such that

$$\sigma = (\mathbf{v}, \dots, \mathbf{v}) + \delta. \quad (2.8)$$

Indeed, (2.7) guarantees the existence of such \mathbf{v} and δ and if $(\mathbf{v}, \dots, \mathbf{v}) + \delta = (\mathbf{u}, \dots, \mathbf{u}) + \zeta$ with another pair of $\mathbf{u} \in \mathbb{F}^n, \zeta \in \mathcal{D}$, then both δ and $(\mathbf{v} - \mathbf{u}, \dots, \mathbf{v} - \mathbf{u}) + \delta$ are in \mathcal{D} . By (2.5), we will have $\mathbf{v} = \mathbf{u}$ and hence $\delta = \zeta$, and this guarantees the uniqueness. Finally, if \mathbb{F} is a finite set, it is easy to see that

$$|\mathcal{S}| = |\mathbb{F}|^n |\mathcal{D}|. \quad (2.9)$$

Example 2.1 (Hamming Sources). A Hamming source [17] \mathcal{S} as defined by

$$\mathcal{S} = \{(\mathbf{v}, \dots, \mathbf{v}) + \underbrace{(\mathbf{0}, \dots, a\mathbf{e}_j, \dots, \mathbf{0})}_{i \text{ terms}} \mid a \in \mathbb{F}, 1 \leq i \leq s, 1 \leq j \leq n\} \quad (2.10)$$

is clearly a source with deviation symmetry, where \mathbf{e}_j is a length- n vector with zeros for all but the j^{th} component being 1. For $s \geq 3$, we can simply choose the representative set as

$$\mathcal{D} = \{(\mathbf{0}, \dots, \underbrace{a\mathbf{e}_j}_{i \text{ terms}}, \dots, \mathbf{0}) \mid a \in \mathbb{F}, 1 \leq i \leq s, 1 \leq j \leq n\} \quad (2.11)$$

and we have

$$|\mathcal{S}| = |\mathbb{F}|^n (1 + s(|\mathbb{F}| - 1)n) \text{ for finite } \mathbb{F}. \quad (2.12)$$

But when $s = 2$, (2.11) is not a good choice as

$$(\mathbf{0}, \mathbf{e}_1) = (\mathbf{e}_1, \mathbf{e}_1) + (-\mathbf{e}_1, \mathbf{0}), \quad (2.13)$$

which contravenes the restriction (2.5). Instead, we may choose

$$\mathcal{D} = \{(\mathbf{0}, a\mathbf{e}_j) \mid a \in \mathbb{F}, 1 \leq j \leq n\} \quad (2.14)$$

and get

$$|\mathcal{S}| = |\mathbb{F}|^n (1 + (|\mathbb{F}| - 1)n) \text{ for finite } \mathbb{F}. \quad (2.15)$$

Before we end this section, we would like to define a vectorized correspondence of \mathcal{D} for later usage. Let

$$\tilde{\mathcal{D}} = \left\{ \left(\begin{pmatrix} \mathbf{d}_1 \\ \mathbf{d}_2 \\ \vdots \\ \mathbf{d}_s \end{pmatrix} \right) \middle| (\mathbf{d}_1, \dots, \mathbf{d}_s) \in \mathcal{D} \right\} \subset \mathbb{F}^{sn}. \quad (2.16)$$

We have

$$|\mathcal{D}| = |\tilde{\mathcal{D}}| \text{ for finite field } \mathbb{F}. \quad (2.17)$$

2.3 Pre-Matrix Partition Codes

The following theorem suggests a way to construct codes for sources with deviation symmetry. We call such codes Pre-Matrix Partition Codes as the name *Matrix Partition Codes* will be reserved to the more refined codes to be discussed shortly afterward.

Theorem 2.1 (Pre-Matrix Partition Codes). *Let P be an $r \times sn$ matrix ($r \in \mathbb{Z}_+$) over \mathbb{F} s.t.*

$$P|_{\tilde{\mathcal{D}}} \text{ is injective.} \quad (2.18)$$

Suppose P can be partitioned into

$$P = [Q_1 | \dots | Q_s] \text{ s.t. } Q_1 + \dots + Q_s = 0, \quad (2.19)$$

where all Q_i are $r \times n$ matrices. Then for any matrix T' that

$$\begin{pmatrix} Q_1 \\ \vdots \\ Q_s \\ T' \end{pmatrix} \text{ forms an injective matrix,} \quad (2.20)$$

we let $\{G'_i | 1 \leq i \leq s\}$ be a row partition of T' , ie

$$\begin{pmatrix} G'_1 \\ \vdots \\ G'_s \end{pmatrix} = T'. \quad (2.21)$$

Encoding matrices (H_1, \dots, H_s) with

$$\text{null}H_i = \text{null} \begin{pmatrix} G'_i \\ Q_i \end{pmatrix} \text{ for all } i \quad (2.22)$$

form a compression that we name Pre-Matrix Partition Code.

Proof. Define $\mathcal{S}_+ = \{\sigma_1 - \sigma_2 | \sigma_1, \sigma_2 \in \mathcal{S}\}$. Since $(H_1, \dots, H_s)|_{\mathcal{S}}$ is injective iff

$$\text{null}H_1 \times \text{null}H_2 \times \dots \times \text{null}H_s \cap \mathcal{S}_+ = \{0\}, \quad (2.23)$$

the validity of the compression solely depends on the null spaces of coding matrices H_i . Thus we only need to prove for the special case when $H_i = \begin{pmatrix} G'_i \\ Q_i \end{pmatrix}$ for all i .

Suppose

$$\begin{pmatrix} G'_i \\ Q_i \end{pmatrix} (\mathbf{u} + \mathbf{d}_i) = \begin{pmatrix} G'_i \\ Q_i \end{pmatrix} (\mathbf{v} + \mathbf{f}_i) \text{ for } 1 \leq i \leq s, \quad (2.24)$$

where $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$; $(\mathbf{d}_1, \dots, \mathbf{d}_s), (\mathbf{f}_1, \dots, \mathbf{f}_s) \in \mathcal{D}$. We get

$$\begin{pmatrix} G'_i \\ Q_i \end{pmatrix} (\mathbf{w} + \mathbf{d}_i - \mathbf{f}_i) = \mathbf{0} \text{ for } 1 \leq i \leq s, \quad (2.25)$$

where $\mathbf{w} = \mathbf{u} - \mathbf{v}$. In particular,

$$Q_i(\mathbf{w} + \mathbf{d}_i - \mathbf{f}_i) = \mathbf{0} \text{ for } 1 \leq i \leq s \quad (2.26)$$

and hence

$$Q_1(\mathbf{w} + \mathbf{d}_1 - \mathbf{f}_1) + \dots + Q_s(\mathbf{w} + \mathbf{d}_s - \mathbf{f}_s) = \mathbf{0}. \quad (2.27)$$

By (2.19), we get

$$Q_1(\mathbf{d}_1) + \dots + Q_s(\mathbf{d}_s) = Q_1(\mathbf{f}_1) + \dots + Q_s(\mathbf{f}_s) \quad (2.28)$$

$$\Rightarrow P \begin{pmatrix} \mathbf{d}_1 \\ \vdots \\ \mathbf{d}_s \end{pmatrix} = P \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_s \end{pmatrix}. \quad (2.29)$$

By (2.18),

$$\begin{pmatrix} \mathbf{d}_1 \\ \vdots \\ \mathbf{d}_s \end{pmatrix} = \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_s \end{pmatrix}. \quad (2.30)$$

Then (2.25) become

$$\begin{pmatrix} G'_i \\ Q_i \end{pmatrix} (\mathbf{w}) = \mathbf{0} \text{ for } 1 \leq i \leq s, \quad (2.31)$$

which gives

$$\begin{pmatrix} Q_1 \\ \vdots \\ Q_s \\ T' \end{pmatrix} (\mathbf{w}) = \mathbf{0} \text{ (c.f. (2.21))}. \quad (2.32)$$

Hence we must have $\mathbf{w} = \mathbf{u} - \mathbf{v} = \mathbf{0}$ by (2.20). □

The Pre-Matrix Partition Codes fulfill the basic requirement of our definition of compression, i.e., injectivity. They do not take the sizes of the output codeword spaces into account. In the following, we are going to put more restriction on the codes to maximize the compression efficiency (in the sense of Theorem 2.2).

2.4 Matrix Partition Codes

Definition 2.7 (Matrix Partition Codes). Let P be a matrix satisfying (2.18) and (2.19). Let

$$Y \text{ be a row basis matrix of } \begin{pmatrix} Q_1 \\ \vdots \\ Q_s \end{pmatrix} \quad (2.33)$$

and T be a matrix s.t.

$$\begin{pmatrix} Y \\ T \end{pmatrix} \text{ is an invertible } n \times n \text{ matrix.} \quad (2.34)$$

Then we call the compression with encoding matrices

$$U_1 \begin{pmatrix} C_1 \\ G_1 \end{pmatrix}, \dots, U_s \begin{pmatrix} C_s \\ G_s \end{pmatrix} \quad (2.35)$$

a Matrix Partition Code for source \mathcal{S} , where $T = \begin{pmatrix} G_1 \\ \vdots \\ G_s \end{pmatrix}$, C_i are row basis matrices of Q_i , and U_i are arbitrary invertible matrices with appropriate sizes for all i .

Those U_i may seem redundant and we usually set it to identity. But they are indispensable for the code to cover all perfect compression and linear-optimal compression. A Matrix Partition Code can be seen as a Pre-Matrix Partition Code with $T' = T$ and $G'_i = G_i$ for all i , and hence it is a valid compression too.

This type of compression (2.35) first appeared in [17] to deal with the multiple Hamming sources over \mathbb{Z}_2 , in which we called it Generalized HCMS for perfect compressions. Now we find that it is applicable to any source with deviation symmetry, a class of source much wider than Hamming source, over an arbitrary field. We would now call the code described by (2.35) as a Matrix Partition Code and the matrix P as the *parent matrix* of the Matrix Partition Code. We will show in Section 4 that every compression of a source with deviation symmetry can be deduced from Theorem 2.1. Every linear-optimal or perfect compression is a Matrix Partition Code. Before doing that, we derive here the minimum possible sum-ratio (highest compression) allowed by a Matrix Partition Code.

Theorem 2.2 (Compression Ratio Tuples). *Suppose the parent matrix P of (2.18) and (2.19) is given. Then the compression ratio tuples $(m_1/n, \dots, m_s/n)$ of any Pre-Matrix Partition Code fulfill $m_i = \text{rank} Q_i + r_i$, where $r_i \in \{0, 1, 2, \dots\}$ for all i such that*

$$r_1 + \dots + r_s \geq n - \text{rank} \begin{pmatrix} Q_1 \\ \vdots \\ Q_s \end{pmatrix}. \quad (2.36)$$

Moreover equality (2.36) holds if and only if the code is a Matrix Partition Code.

The proof below frequently uses the fact that $\text{rank } A + \text{rank } B \geq \text{rank } \begin{pmatrix} A \\ B \end{pmatrix}$ and the equality holds iff $\text{row } A \cap \text{row } B = \{\mathbf{0}\}$, where the word *row* means *the row space of*.

Proof. Let $i \in \{1, \dots, s\}$. Let G'_i, Q_i, H_i be those defined in Theorem 2.1. WLOG, we decompose

$$G'_i = \begin{pmatrix} A_i \\ D_i \end{pmatrix}, \quad (2.37)$$

such that

$$\text{row } A_i \cap \text{row } Q_i = \{\mathbf{0}\}, \quad \text{row } \begin{pmatrix} A_i \\ Q_i \end{pmatrix} = \text{row } \begin{pmatrix} G'_i \\ Q_i \end{pmatrix}. \quad (2.38)$$

Equation (2.22) becomes $\text{null } H_i = \text{null } \begin{pmatrix} A_i \\ Q_i \end{pmatrix}$. Therefore $\text{row } H_i = \text{row } \begin{pmatrix} A_i \\ Q_i \end{pmatrix}$ and $\text{rank } H_i = \text{rank } \begin{pmatrix} A_i \\ Q_i \end{pmatrix}$. Thus we have

$$m_i = \text{number of rows of } H_i \geq \text{rank } H = \text{rank } A_i + \text{rank } Q_i. \quad (2.39)$$

Moreover $\begin{pmatrix} Q_1 \\ \vdots \\ Q_s \\ A_1 \\ \vdots \\ A_s \end{pmatrix}$ is injective (with n columns) by (2.20) and the second equation in (2.38). We get

$$\text{rank } A_1 + \dots + \text{rank } A_s \geq n - \text{rank } \begin{pmatrix} Q_1 \\ \vdots \\ Q_s \end{pmatrix}. \quad (2.40)$$

By (2.39) and (2.40), we get (2.36) with $r_i = m_i - \text{rank } Q_i$.

Secondly, equality (2.36) holds iff equalities (2.39) and (2.40) both hold. Let G_i be a row basic matrix of A_i and C_i be a row basic matrix of Q_i . We have $\text{row } G_i \cap \text{row } C_i = \{\mathbf{0}\}$, thanks to the first equation in (2.38). Equality (2.39) holds iff H_i is a surjective matrix and hence a row basic matrix of $\begin{pmatrix} A_i \\ Q_i \end{pmatrix}$. Notice that $\begin{pmatrix} G_i \\ C_i \end{pmatrix}$ is also a surjective matrix of $\begin{pmatrix} A_i \\ Q_i \end{pmatrix}$, we conclude that equality (2.39) holds iff

$$H_i = U_i \begin{pmatrix} G_i \\ C_i \end{pmatrix} \quad (2.41)$$

for an invertible matrix U_i . We also let Y be a row basic matrix of $\begin{pmatrix} Q_1 \\ \vdots \\ Q_s \end{pmatrix}$. So

$\begin{pmatrix} Y \\ G_1 \\ \vdots \\ G_s \end{pmatrix}$ is injective and (2.40) is equivalent to $\text{rank } G_1 + \dots + \text{rank } G_s \geq n - \text{rank } Y$,

which holds iff $\text{row}G_1 \oplus \cdots \oplus \text{row}G_s \oplus \text{row}Y = \mathbb{F}^n$. Since all G_1, \dots, G_s and Y are surjective, we conclude equality (2.40) holds iff

$$\begin{pmatrix} Y \\ T \end{pmatrix} \text{ is bijective, for } T = \begin{pmatrix} G_1 \\ \vdots \\ G_s \end{pmatrix}. \quad (2.42)$$

Notice that (2.41) and (2.42) are all we need to define a Matrix Partition Code with the given P (c.f. Definition 2.7) and so we complete the proof. \square

Corollary 1. *All the values of compression ratio tuples allowed by (2.36) are achievable by the Pre-Matrix Partition Codes.*

Proof. Given any r_1, \dots, r_s such that equality (2.36) holds. Let T be a matrix defined in (2.34) or (2.42). We have

$$r_1 + \cdots + r_s = n - \text{rank} \begin{pmatrix} Q_1 \\ \vdots \\ Q_s \end{pmatrix} = \text{number of rows of } T. \quad (2.43)$$

Hence we can partition T into those G_i such that G_i have r_i rows for all i , respectively. Let (H_1, \dots, H_s) be a compression of Matrix Partition Code defined by (2.35) or (2.41). We have

$$r_i = m_i - \text{rank}Q_i = \text{number of rows of } G_i. \quad (2.44)$$

Therefore (H_1, \dots, H_s) has the corresponding compression ratio tuples of the given r_1, \dots, r_s . As a result all the values allowed by the equality in (2.36) are achievable.

In general, for any (r_1, \dots, r_s) allowed by (2.36), we let $a_i \in \{0, 1, 2, \dots\}$ such that $r_i \geq a_i$ and

$$a_1 + \cdots + a_s = n - \text{rank} \begin{pmatrix} Q_1 \\ \vdots \\ Q_s \end{pmatrix}. \quad (2.45)$$

By the previous argument, there exists a Matrix Partition Code (H_1, \dots, H_s) such that $m_i = a_i + \text{rank}Q_i$ for all i . Then (H'_1, \dots, H'_s) is the Pre-Matrix Partition Code with the desired compression ratio tuples, where those H'_i are obtained by augmenting the corresponding H_i vertically with $r_i - a_i$ zero rows for all i . \square

Corollary 2. *The total code length $M \geq \text{rank}Q_1 + \cdots + \text{rank}Q_s - \text{rank} \begin{pmatrix} Q_1 \\ \vdots \\ Q_s \end{pmatrix}$ for any Pre-Matrix Partition Code, and the equality holds if and only if the code is a Matrix Partition Code.*

Proof. Simply because $M = m_1 + \cdots + m_s$. \square

It is tempting to think that changing the choice of \mathcal{D} should end up with a different parent matrix P that may increase compression efficiency. However, it turns out that it is not the case. The parent matrix P is independent of such a choice as shown by the following theorem.

Theorem 2.3. *Let both \mathcal{D} and \mathcal{E} be representation sets of source \mathcal{S} . If P is a parent matrix of \mathcal{D} as specified in Theorem 2.1, then $P|_{\tilde{\mathcal{E}}}$ is also injective, where $\tilde{\mathcal{E}}$ is a vectorized \mathcal{E} given by*

$$\tilde{\mathcal{E}} = \left\{ \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_s \end{pmatrix} \middle| (\mathbf{f}_1, \dots, \mathbf{f}_s) \in \mathcal{E} \right\}. \quad (\text{c.f. (2.16)}) \quad (2.46)$$

Proof. From (2.6), there exists mapping $\mathbf{v}(\cdot)$ such that

$$\tilde{\mathcal{E}} = \left\{ \begin{pmatrix} \mathbf{v}(\delta) + \mathbf{d}_1 \\ \vdots \\ \mathbf{v}(\delta) + \mathbf{d}_s \end{pmatrix} \middle| \delta = (\mathbf{d}_1, \dots, \mathbf{d}_s) \in \mathcal{D} \right\}. \quad (2.47)$$

Suppose

$$P \begin{pmatrix} \mathbf{v}(\delta) + \mathbf{d}_1 \\ \vdots \\ \mathbf{v}(\delta) + \mathbf{d}_s \end{pmatrix} = P \begin{pmatrix} \mathbf{v}(\gamma) + \mathbf{g}_1 \\ \vdots \\ \mathbf{v}(\gamma) + \mathbf{g}_s \end{pmatrix}, \quad (2.48)$$

where $\delta, \gamma \in \mathcal{D}$ such that $\delta = (\mathbf{d}_1, \dots, \mathbf{d}_s)$, $\gamma = (\mathbf{g}_1, \dots, \mathbf{g}_s)$. Then

$$\begin{aligned} P \begin{pmatrix} \mathbf{d}_1 \\ \vdots \\ \mathbf{d}_s \end{pmatrix} &= P \begin{pmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_s \end{pmatrix} \text{ by (2.19) ;} \\ \begin{pmatrix} \mathbf{d}_1 \\ \vdots \\ \mathbf{d}_s \end{pmatrix} &= \begin{pmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_s \end{pmatrix} \text{ by (2.18);} \end{aligned}$$

i.e. $\delta = \gamma$ and we get

$$\begin{pmatrix} \mathbf{v}(\delta) + \mathbf{d}_1 \\ \vdots \\ \mathbf{v}(\delta) + \mathbf{d}_s \end{pmatrix} = \begin{pmatrix} \mathbf{v}(\gamma) + \mathbf{g}_1 \\ \vdots \\ \mathbf{v}(\gamma) + \mathbf{g}_s \end{pmatrix}.$$

Hence, $P|_{\tilde{\mathcal{E}}}$ is also injective. \square

3 Perfect Compression of Matrix Partition Code

In this section, we study perfect compression. By Definition 2.4, the field \mathbb{F} is required to be finite, and a code is perfect if and only if the cardinality of the range of the mapping is the same as that of the source, i.e. $|\mathcal{C}| = |\mathcal{S}|$. Since $|\mathcal{C}| = |\mathbb{F}|^M$ and $|\mathcal{S}| = |\mathbb{F}|^n |\mathcal{D}|$ in (2.9) and $|\mathcal{D}| = |\tilde{\mathcal{D}}|$ in (2.17), we have

$$|\mathbb{F}|^{M-n} = |\mathcal{D}| = |\tilde{\mathcal{D}}|. \quad (3.1)$$

For the sake of simplicity, we won't extend the definition to infinite field.

3.1 Perfect Compression for \mathcal{S} over Finite Fields

The following theorem explains a necessary condition for a perfect Matrix Partition Code.

Theorem 3.1 (Necessary Condition of Perfect Codes). *To have a perfect compression of Matrix Partition Code, we must have an $(M - n) \times sn$ matrix P such that*

$$P|_{\tilde{\mathcal{D}}} \text{ is bijective.} \quad (3.2)$$

Proof. Suppose we have a perfect code constructed from a parent matrix P' , any matrix P with the same row space of P' can be viewed as the parent matrix of the code. Indeed if $\text{row } P = \text{row } P'$, then $\text{null } P = \text{null } P'$ and $\text{row } Q_i = \text{row } Q'_i$ for all i . Hence P also satisfies (2.18) and (2.19), and shares the same other components (such as Y, C_i, \dots , etc.) with P' in Definition 2.7. In particular, we let P be a row basic matrix of P' . Let r be the number of rows of P so that P is an $r \times sn$ matrix. We are going to show $P|_{\tilde{\mathcal{D}}}$ is bijective and $r = M - n$.

Since we have shown $P|_{\tilde{\mathcal{D}}}$ is injective (that is (2.18)), we only need to show that $P|_{\tilde{\mathcal{D}}}$ is also surjective. Suppose $P|_{\tilde{\mathcal{D}}}$ is not surjective, then we can pick a $\mathbf{u} \in \mathbb{F}^r$ such that $\mathbf{u} \notin P(\tilde{\mathcal{D}})$. Since P is a row basis matrix and thus is a surjective matrix, there exists a $\boldsymbol{\delta} \in \mathbb{F}^{sn}$ with $P\boldsymbol{\delta} = \mathbf{u}$. Notice that by (2.19),

$$P \left(\boldsymbol{\delta} + \begin{pmatrix} \mathbf{v} \\ \vdots \\ \mathbf{v} \end{pmatrix} \right) = P(\boldsymbol{\delta}) = \mathbf{u} \text{ for all } \mathbf{v} \in \mathbb{F}^n, \quad (3.3)$$

thus $\boldsymbol{\delta} + \begin{pmatrix} \mathbf{v} \\ \vdots \\ \mathbf{v} \end{pmatrix} \notin \tilde{\mathcal{D}}$ for all $\mathbf{v} \in \mathbb{F}^n$. Therefore we can extend $\tilde{\mathcal{D}}$ to $\tilde{\mathcal{D}}' = \tilde{\mathcal{D}} \cup \{\boldsymbol{\delta}\}$

and the source \mathcal{S} to the corresponding \mathcal{S}' . Notice that $P|_{\tilde{\mathcal{D}}'}$ is injective and hence we can compress \mathcal{S}' by the same compression. This leads to a contradiction as $|\mathcal{S}'| > |\mathcal{S}| = |\mathcal{C}|$.

Finally, by (3.1), we must have $r = M - n$ if $P|_{\tilde{\mathcal{D}}}$ is bijective. \square

Actually (3.2) is a necessary condition for any perfect compression of the given \mathcal{S} simply because it turns out that any perfect compression can be realized by a Matrix Partition Code. We will defer the discussion to Section 4.

3.2 Necessary Conditions for Perfect Compression on Generalized Hamming Source

Let \mathcal{L} be a non-empty subset of \mathbb{F} s.t. $0 \notin \mathcal{L}$. We define

$$\mathcal{S} = \{(\mathbf{v}, \dots, \mathbf{v}) + \underbrace{(\mathbf{0}, \dots, \lambda \mathbf{e}_j, \dots, \mathbf{0})}_{i\text{-th}} | \mathbf{v} \in \mathbb{F}^n, \lambda \in \mathcal{L} \cup \{0\}, 1 \leq i \leq s, 1 \leq j \leq n\}. \quad (3.4)$$

Notice that if $\mathcal{L} = \mathbb{F} - \{0\}$, then \mathcal{S} is just the Hamming source over \mathbb{F} (c.f. (2.10)). Therefore we call \mathcal{S} as generalized Hamming source. Obviously it is a source with deviation symmetry.

Let $s \geq 3$. We pick

$$\mathcal{D} = \{(\underbrace{\mathbf{0}, \dots, \lambda \mathbf{e}_j}_{i\text{-th}}, \dots, \mathbf{0}) \mid \lambda \in \mathcal{L} \cup \{0\}, 1 \leq i \leq s, 1 \leq j \leq n\} \quad (3.5)$$

and the corresponding

$$\tilde{\mathcal{D}} = \{\lambda \mathbf{e}_i \mid \lambda \in \mathcal{L} \cup \{0\}, 1 \leq i \leq sn\}. \quad (3.6)$$

We have

$$|\tilde{\mathcal{D}}| = 1 + |\mathcal{L}|sn. \quad (3.7)$$

To have a perfect compression, we must have (3.1) and hence

$$|\mathbb{F}|^{M-n} = 1 + |\mathcal{L}|sn. \quad (3.8)$$

So, s and $|\mathcal{L}|$ can't be multiplier of p , the characteristic of \mathbb{F} ($|\mathbb{F}| = p^u$ for some positive integer u). If it is the case, then we have infinite pair of numbers (M, n) satisfying (3.8) by Euler theorem.

Theorem 3.2 (Necessary Conditions of Perfect Matrix Partition Codes for Generalized Hamming Sources). *The necessary and sufficient condition for the existence of an $(M - n) \times sn$ matrix P which is bijective when restricted to $\tilde{\mathcal{D}}$ is that $|\mathbb{F}| - 1$ is divisible by $|\mathcal{L}|$ and \exists distinct $a_1, a_2, \dots, a_k \in \mathbb{F}$, with $k = (|\mathbb{F}| - 1)/|\mathcal{L}|$, such that*

$$\mathbb{F} - \{0\} = \{a_i \lambda \mid 1 \leq i \leq k; \lambda \in \mathcal{L}\}. \quad (3.9)$$

Proof. If \mathcal{L} fulfills the conditions, then $sn/k = (|\mathbb{F}|^{M-n} - 1)/(|\mathbb{F}| - 1)$ by (3.8). Thus sn/k is an integer. Let $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{sn/k}\}$ be a subset of \mathbb{F}^{M-n} that each element is a not multiplier of the other. Define P through its column

$$\mathbf{P}_{i+(j-1)k} = a_i \mathbf{v}_j, \text{ for } 1 \leq i \leq k, 1 \leq j \leq sn/k. \quad (3.10)$$

Then we will show $P|_{\tilde{\mathcal{D}}}$ is injective. Suppose

$$P(\lambda_1 \mathbf{e}_{i+(j-1)k}) = P(\lambda_2 \mathbf{e}_{b+(c-1)k}), \quad (3.11)$$

where $\lambda_1, \lambda_2 \in \mathcal{L} \cup \{0\}; i, b \leq k; j, c \leq sn/k$. Then

$$\lambda_1 a_i \mathbf{v}_j = \lambda_2 a_b \mathbf{v}_c, \quad (3.12)$$

which gives $\lambda_1 = \lambda_2 = 0$ that yields $\lambda_1 \mathbf{e}_{i+(j-1)k} = \lambda_2 \mathbf{e}_{b+(c-1)k}$ immediately or $j = c$ with $\lambda_1 \neq 0 \neq \lambda_2$. So let assume we are in the second case. By counting the number of elements in both sides of (3.9), we conclude that every nonzero element of \mathbb{F} is a product of a unique λ and a unique a_j ($\lambda \in \mathcal{L}, 1 \leq j \leq k$). Thus, we get $\lambda_1 = \lambda_2$ and $i = b$. Hence $P|_{\tilde{\mathcal{D}}}$ is injective. By (3.1), $P|_{\tilde{\mathcal{D}}}$ is bijective.

Conversely, let \mathcal{J} be a maximal subset of the index set $\{1, 2, \dots, sn\}$ such that \mathbf{P}_j , the j -th column of P , is a multiplier of \mathbf{P}_1 for all $j \in \mathcal{J}$. So if \mathbf{P}_i is a multiplier of \mathbf{P}_1 , then $i \in \mathcal{J}$. Let $\mathbf{P}_j = a_j \mathbf{P}_1$ for all $j \in \mathcal{J}$. The columns of P must be nonzero and distinct from each other, otherwise $P|_{\tilde{\mathcal{D}}}$ can't be injective. It follows that a_j are nonzero for all $j \in \mathcal{J}$ and distinct from each other. Then the bijectivity of $P|_{\tilde{\mathcal{D}}}$ implies $\forall b \in \mathbb{F} - \{0\}, \exists$ unique $\lambda \mathbf{e}_i \in \tilde{\mathcal{D}}$ (c.f. (3.6)) with $\lambda \in \mathcal{L}, 1 \leq i \leq sn$, such that $P(\lambda \mathbf{e}_i) = b \mathbf{P}_1$. Hence $i \in \mathcal{J}$ and $\lambda a_i = b$. By counting, we get $(|\mathbb{F}| - 1)/|\mathcal{L}|$ is an integer and (3.9) is fulfilled with $k = |\mathcal{J}|$. \square

We remark that Theorem 3.2 only characterizes necessary conditions since even if P is bijective when restricted to $\tilde{\mathcal{D}}$, it does not mean that we will have a perfect compression of Matrix Partition Codes (see [18]). However, it is not the case when $s = 2$. Here we give some examples of perfect compression:

Example 3.1. $\mathbb{F} = \mathbb{Z}_{11}, \mathcal{L} = \mathbb{Z}_{11} - \{0\}$ (Hamming source over \mathbb{Z}_{11}), $n = 4$ and $s = 3$:

$$H_1 = Q_1 = \begin{pmatrix} 1 & 1 & -2 & -2 \\ 0 & 2 & -1 & -7 \end{pmatrix}, \quad (3.13)$$

$$H_2 = Q_2 = \begin{pmatrix} 0 & 9 & 1 & 1 \\ 1 & 5 & 5 & 8 \end{pmatrix}, \quad (3.14)$$

$$H_3 = Q_3 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ -1 & 4 & 7 & -1 \end{pmatrix}. \quad (3.15)$$

Notice that each nonzero vector of \mathbb{F}^2 has one and only one multiplier as a column vector of $P = [Q_1; Q_2; Q_3]$.

Example 3.2. $\mathbb{F} = \mathbb{Z}_5, \mathcal{L} = \{1, -1\}, n = 4$ and $s = 3$:

$$H_1 = Q_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 2 & 2 & -2 \end{pmatrix}, \quad (3.16)$$

$$H_2 = Q_2 = \begin{pmatrix} 0 & 2 & -2 & 2 \\ 1 & 0 & -1 & -1 \end{pmatrix}, \quad (3.17)$$

$$H_3 = Q_3 = \begin{pmatrix} -1 & -2 & 1 & 2 \\ -1 & -2 & -1 & -2 \end{pmatrix}, \quad (3.18)$$

Notice that $\{a_1, a_2\} = \{1, 2\}$ (c.f.(3.9)),
 $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$ (c.f.(3.10)).

Example 3.3. $\mathbb{F} = \mathbb{Z}_5, \mathcal{L} = \{1\}, n = 6, s = 4$:

$$H_1 = Q_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 1 & 2 & -2 & -1 \end{pmatrix}, \quad (3.19)$$

$$H_2 = Q_2 = \begin{pmatrix} -1 & 0 & 2 & -1 & 2 & -1 \\ 0 & 2 & 2 & -2 & 1 & 1 \end{pmatrix}, \quad (3.20)$$

$$H_3 = Q_3 = \begin{pmatrix} 2 & 0 & -2 & 1 & -2 & 1 \\ 0 & -1 & -2 & -2 & 2 & -1 \end{pmatrix}, \quad (3.21)$$

$$H_4 = Q_4 = \begin{pmatrix} -2 & 0 & -1 & -1 & -2 & -2 \\ 0 & -2 & -1 & 2 & -1 & 1 \end{pmatrix}. \quad (3.22)$$

The matrix $P = [Q_1; Q_2; Q_3; Q_4]$ consists of all nonzero vectors of \mathbb{F}^2 without repetition.

Example 3.4. $\mathbb{F} = \text{GF}(4) = \mathbb{Z}_2(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$; $\mathcal{L} = \{1, \alpha, \alpha + 1\}$,

$$n = 7, s = 3$$

$$T = (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1), \quad (3.23)$$

$$Q_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & \alpha & \alpha \\ 1 & 0 & 1 & 0 & \alpha & 1 & \alpha \\ 0 & 0 & 0 & 1 & \alpha & \alpha & 1 \end{pmatrix}, \quad (3.24)$$

$$H_1 = \begin{pmatrix} T \\ Q_1 \end{pmatrix}, \quad (3.25)$$

$$H_2 = Q_2 = \begin{pmatrix} 1 & \alpha+1 & 0 & 1 & \alpha & \alpha+1 & \alpha+1 \\ 0 & 1 & \alpha+1 & 0 & 1 & \alpha+1 & 1 \\ 1 & 0 & 1 & \alpha+1 & 1 & 1 & \alpha+1 \end{pmatrix}, \quad (3.26)$$

$$H_3 = Q_3 = \begin{pmatrix} 0 & \alpha & 0 & 1 & \alpha+1 & 1 & 1 \\ 1 & 1 & \alpha & 0 & \alpha+1 & \alpha & \alpha+1 \\ 1 & 0 & 1 & \alpha & \alpha+1 & \alpha+1 & \alpha \end{pmatrix}. \quad (3.27)$$

It is a Hamming source over $\text{GF}(4)$. Each nonzero vector of \mathbb{F}^3 has one and only one multiplier as a column vector of $P = [Q_1; Q_2; Q_3]$. Besides, $(Q_1, \begin{pmatrix} T \\ Q_2 \end{pmatrix}, Q_3)$ and $(Q_1, Q_2, \begin{pmatrix} T \\ Q_3 \end{pmatrix})$ are also perfect compressions.

Let $s = 2$. We rewrite (3.4) as

$$\mathcal{S} = \{(\mathbf{v}, \mathbf{v}) + (\mathbf{0}, a\mathbf{e}_i) | \mathbf{v} \in \mathbb{F}^n, 1 \leq i \leq n, a \in \mathcal{L} \cup \mathcal{L}_- \cup \{0\}\}, \quad (3.28)$$

where $\mathcal{L}_- = \{-a | a \in \mathcal{L}\}$. We have

$$\mathcal{D} = \{(\mathbf{0}, a\mathbf{e}_i) | 1 \leq i \leq n, a \in \mathcal{L} \cup \mathcal{L}_- \cup \{0\}\}. \quad (3.29)$$

The corresponding

$$\tilde{\mathcal{D}} = \{a\mathbf{e}_i | a \in \mathcal{L} \cup \mathcal{L}_- \cup \{0\}, n < i \leq 2n\}. \quad (3.30)$$

Then

$$|\tilde{\mathcal{D}}| = 1 + n|\mathcal{L} \cup \mathcal{L}_-|. \quad (3.31)$$

To have a perfect compression, we must have (3.1), i.e.

$$|\mathbb{F}|^{M-n} = 1 + n|\mathcal{L} \cup \mathcal{L}_-|. \quad (3.32)$$

Now we are seeking an $(M-n) \times 2n$ matrix P to be bijective when restricted to $\tilde{\mathcal{D}}$. Since the first n columns in P virtually play no role on $\tilde{\mathcal{D}}$, it can be arbitrary. Let

$$P = [-Q_2; Q_2]. \quad (3.33)$$

where Q_2 is an $(M-n) \times n$ matrix so that P satisfies (2.19). Let

$$\tilde{\mathcal{D}}' = \{a\mathbf{e}_i | a \in \mathcal{L} \cup \mathcal{L}_- \cup \{0\}, 1 \leq i \leq n\}, \quad (3.34)$$

which is just the nontrivial segment of the $\tilde{\mathcal{D}}$ in (3.30).

Theorem 3.3 (Necessary and Sufficient Conditions of Perfect Matrix Partition Codes for Generalized Hamming Sources with $s = 2$). *The following statements imply each other:*

- We have an $(M - n) \times 2n$ matrix P which is bijective when restricted to $\tilde{\mathcal{D}}$.
- We have an $(M - n) \times n$ matrix Q_2 which is bijective when restricted to $\tilde{\mathcal{D}}'$.
- \exists distinct $a_1, a_2, \dots, a_k \in \mathbb{F}$, with $k = (|\mathbb{F}| - 1)/|\mathcal{L} \cup \mathcal{L}_-|$, such that $\mathbb{F} - \{0\} = \{a_i \lambda \mid 1 \leq i \leq k; \lambda \in \mathcal{L} \cup \mathcal{L}_-\}$.

Proof. Similar to the proof of Theorem 3.2 . \square

Once we have the Q_2 in the above theorem, it can be shown that the pair $\begin{pmatrix} G_1 \\ Q_2 \end{pmatrix}, \begin{pmatrix} G_2 \\ Q_2 \end{pmatrix}$ is a Matrix Partition Code and a perfect compression whenever $\begin{pmatrix} G_1 \\ G_2 \\ Q_2 \end{pmatrix}$ forms an $n \times n$ invertible matrix. Notice that $(I_{n \times n}, Q_2)$ is also a perfect compression, which is a Matrix Partition Code with certain U_1 .

Example 3.5. $\mathbb{F} = GF(4)$ with $\alpha^2 + \alpha + 1 = 0$, $\mathcal{L} = \mathbb{F} - \{0\}$, $n = 5$, $s = 2$. Let

$$Q_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & 1 + \alpha \end{pmatrix}. \quad (3.35)$$

The following pairs of matrices are all perfect compression:

- $I_{5 \times 5}$ and Q_2 ;
- $\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ Q_2 \end{pmatrix}$ and Q_2 ;
- $\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ Q_2 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ Q_2 \end{pmatrix}$.

3.3 Examples beyond Generalized Hamming Source

Here we will provide some examples where the sources are not generalized Hamming. The first two examples illustrate that one can modify a given compression when the original source has been deformed.

Example 3.6. $\mathbb{F} = \mathbb{Z}_{11}$, $s = 5$, $n = 6$.

$$\mathcal{D} = \{(\underbrace{0, \dots, 0}_{i\text{-th}}, a\mathbf{e}_j, 0, \dots, 0) \mid a \in \mathbb{F}, 1 \leq i \leq 3, 1 \leq j \leq 4\}.$$

Notice that this is just the Hamming source (c.f. Example 3.1) trapping in a bigger space. So we can modify the previous setting to obtain a new perfect

compression.

$$H_1 = Q_1 = \begin{pmatrix} 1 & 1 & -2 & -2 & 0 & 0 \\ 0 & 2 & -1 & -7 & 0 & 0 \end{pmatrix}, \quad (3.36)$$

$$H_2 = Q_2 = \begin{pmatrix} 0 & 9 & 1 & 1 & 0 & 0 \\ 1 & 5 & 5 & 8 & 0 & 0 \end{pmatrix}, \quad (3.37)$$

$$H_3 = Q_3 = \begin{pmatrix} -1 & 1 & 1 & 1 & 0 & 0 \\ -1 & 4 & 7 & -1 & 0 & 0 \end{pmatrix}, \quad (3.38)$$

$$Q_4 = Q_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (3.39)$$

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (3.40)$$

And we chose $H_4 = (0 \ 0 \ 0 \ 0 \ 1 \ 0)$, $H_5 = (0 \ 0 \ 0 \ 0 \ 0 \ 1)$.

Example 3.7. $\mathbb{F} = \mathbb{Z}_{11}$, $s = 4$, $n = 5$.

$$\mathcal{D} = \{(\underbrace{0, \dots, 0}_{i\text{-th}}, ae_j, 0, \dots, 0) \mid a \in \mathbb{F}, 1 \leq i \leq 3, 1 \leq j \leq 5\} \quad (3.41)$$

$$- \{(ae_1, 0, 0, 0), (0, ae_1, 0, 0), (0, 0, ae_2, 0) \mid a \in \mathbb{F}\}. \quad (3.42)$$

This is the source of the Example 3.1 with some shifting. We extend $P = [Q_1; Q_2; Q_3; Q_4]$ accordingly.

$$H_1 = Q_1 = \begin{pmatrix} 1 & 1 & -2 & -2 & 1 \\ 0 & 2 & -1 & -7 & 0 \end{pmatrix}, \quad (3.43)$$

$$H_2 = Q_2 = \begin{pmatrix} 0 & 9 & 1 & 1 & 0 \\ 1 & 5 & 5 & 8 & 1 \end{pmatrix}, \quad (3.44)$$

$$H_3 = Q_3 = \begin{pmatrix} -1 & 1 & 1 & 1 & 1 \\ -1 & 4 & 7 & -1 & 4 \end{pmatrix}, \quad (3.45)$$

$Q_4 = -Q_1 - Q_2 - Q_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & -5 \end{pmatrix}$, and $H_4 = (0 \ 0 \ 0 \ 0 \ 1)$, a row basis matrix of Q_4 .

In the third example, we make use of an existing code to create a compression for another source, where \mathcal{D} has been changed almost completely. The old code works as long as the parent matrix P still fulfills (2.18) with the new $\tilde{\mathcal{D}}$. If the existing one is a perfect compression and $P|_{\text{new } \tilde{\mathcal{D}}}$ is bijective, then the compression is also perfect for the new source simply by counting.

Example 3.8. $\mathbb{F} = \mathbb{Z}_5$, $n = 6$, $s = 4$.

$$\begin{aligned} \mathcal{D} = & \{(\pm \mathbf{e}_j, \mathbf{0}, \mathbf{0}) \mid 1 \leq j \leq 6\} \cup \{(\mathbf{0}, \mathbf{e}_j, \mathbf{0}, \mathbf{0}) \mid j \in \{2, 3, 5, 6\}\} \cup \\ & \{(\mathbf{e}_3, \mathbf{0}, \mathbf{e}_1, \mathbf{e}_3), (\mathbf{e}_1 + \mathbf{e}_2, \mathbf{0}, \mathbf{e}_3, \mathbf{e}_3), (\mathbf{0}, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_4, \mathbf{0}, \mathbf{0})\} \cup \\ & \{(3\mathbf{e}_1, 2\mathbf{e}_2, -2\mathbf{e}_1, \mathbf{e}_4 + \mathbf{e}_2), (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{e}_4), (\mathbf{e}_5, \mathbf{e}_6, \mathbf{0}, \mathbf{0})\} \cup \\ & \{(\mathbf{0}, \mathbf{0}, \mathbf{e}_4, \mathbf{0}), (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{e}_2), (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0})\}. \end{aligned} \quad (3.46)$$

The compression (H_1, H_2, H_3, H_4) is the same as Example 3.3.

4 Uniqueness of Matrix Partition Codes

In this section, we will show that Matrix Partition Codes are unique in the sense that any linear-optimal or perfect compression is a Matrix Partition Code.

4.1 Null Space View

We will first study the null spaces of lossless compression simply because null spaces of coding matrices determines injectivity entirely.

Lemma 4.1. *If (H_1, \dots, H_s) is a lossless compression of a source with deviation symmetry, then we have $\text{null}H_1 \cap \dots \cap \text{null}H_s = \{\mathbf{0}\}$.*

Proof. Let $\mathbf{v} \in \text{null}H_1 \cap \dots \cap \text{null}H_s$. Pick a $\sigma \in \mathcal{S}$. We have $\sigma + (\mathbf{v}, \dots, \mathbf{v}) \in \mathcal{S}$ (c.f. Definition 2.5). Moreover, $(H_1, \dots, H_s)(\sigma) = (H_1, \dots, H_s)(\sigma + (\mathbf{v}, \dots, \mathbf{v}))$. As (H_1, \dots, H_s) is a compression, $\sigma = \sigma + (\mathbf{v}, \dots, \mathbf{v})$ that $\mathbf{v} = \mathbf{0}$. \square

Thus if $\text{null}H_1 \cap \dots \cap \text{null}H_{s-1} \supset K \neq \{\mathbf{0}\}$, we have $\text{null}H_s \cap K = \{\mathbf{0}\}$. In this situation, the following theorem tells us that we can build up another compression H'_1, \dots, H'_s merely by shifting the K from the one of the first $s-1$ terminals to the last terminal.

Theorem 4.1 (Nullspace Shifting). *Suppose (H_1, \dots, H_s) is a compression for \mathcal{S} . Let π be a permutation of the index set $\{1, 2, \dots, s\}$ that*

$$\begin{cases} \text{null}H_{\pi(i)} &= K \oplus N_i, & \text{for } 1 \leq i < s, \\ \text{null}H_{\pi(s)} &= N_s, \end{cases} \quad (4.1)$$

where K, N_i are subspaces of \mathbb{F}^n . Then (H'_1, \dots, H'_s) is also a compression for \mathcal{S} if

$$\begin{cases} \text{null}H'_{\pi(1)} &= N_1, \\ \text{null}H'_{\pi(i)} &= K \oplus N_i, & \text{for } 1 < i \leq s. \end{cases} \quad (4.2)$$

Furthermore if H_i and H'_i are surjective for all i , then the two compressions have the same compression sum-ratio. For finite field that if (H_1, \dots, H_s) is a perfect compression, then (H'_1, \dots, H'_s) is also a perfect compression.

Proof of Theorem 4.1. WLOG, let's put $\pi = 1$ for simplicity. Note that $(H'_1, \dots, H'_s)|_{\mathcal{S}}$ is injective if and only if $\text{null}H'_1 \times \dots \times \text{null}H'_s \cap \mathcal{S}_+ = \{\mathbf{0}\}$, where $\mathcal{S}_+ = \{\sigma_1 - \sigma_2 | \sigma_1, \sigma_2 \in \mathcal{S}\}$.² Let $\sigma_+ \in \text{null}H'_1 \times \dots \times \text{null}H'_s \cap \mathcal{S}_+$. Decompose $\sigma_+ = (\mathbf{n}_1, \mathbf{k}_2 + \mathbf{n}_2, \dots, \mathbf{k}_{s-1} + \mathbf{n}_{s-1}, \mathbf{k}_s + \mathbf{n}_s)$, where $\mathbf{n}_i \in N_i$ and $\mathbf{k}_i \in K$ for all i . Since \mathcal{S}_+ is also a source with deviation symmetry, we have

$$\sigma_+ - (\mathbf{k}_s, \dots, \mathbf{k}_s) = (\mathbf{n}_1 - \mathbf{k}_s, \mathbf{k}_2 + \mathbf{n}_2 - \mathbf{k}_s, \dots, \mathbf{k}_{s-1} + \mathbf{n}_{s-1} - \mathbf{k}_s, \mathbf{n}_s) \in \mathcal{S}_+. \quad (4.3)$$

By checking the null space of (H_1, \dots, H_s) , we find $\sigma_+ - (\mathbf{k}_s, \dots, \mathbf{k}_s) \in \mathcal{S}_+ \cap \text{null}H_1 \times \dots \times \text{null}H_s = \{\mathbf{0}\}$ because $(H_1, \dots, H_s)|_{\mathcal{S}}$ is injective. The first entry in the RHS of (4.3) gives $\mathbf{n}_1 = \mathbf{k}_s = \mathbf{0}$, and all other entries follow suit and give $\mathbf{k}_i = \mathbf{0} = \mathbf{n}_i$ for all i . Hence $\sigma_+ = \mathbf{0}$ and $(H'_1, \dots, H'_s)|_{\mathcal{S}}$ is injective.

² Here we use the notation \mathcal{S}_+ for the sake of consistence with [17], where $\{\sigma_1 - \sigma_2 | \sigma_1, \sigma_2 \in \mathcal{S}\} = \{\sigma_1 + \sigma_2 | \sigma_1, \sigma_2 \in \mathcal{S}\}$ since only binary sources were considered.

Next if all H_i and H'_i are surjective for all i , then the two compressions have the same compression sum-ratio $(sn - \sum_{i=1}^s \dim N_i - (s-1)\dim K)/n$.

Lastly, if (H_1, \dots, H_s) is a perfect compression, then $(H_1, \dots, H_s)|_{\mathcal{S}}$ is surjective, still more so for (H_1, \dots, H_s) per se. If (H'_1, \dots, H'_s) is also surjective, the codeword spaces of the two compressions will be of the same dimension $sn - \sum_{i=1}^s \dim N_i - (s-1)\dim K$ and hence same cardinality. \square

4.2 Proof of Uniqueness of Matrix Partition Codes

In this part, we present a major result of the paper—the proof of uniqueness of Matrix Partition Codes. We will need to first illustrate how a parent matrix can be extracted from arbitrary compression. This in turn requires the following lemma.

Lemma 4.2. *Given a compression (H_1, \dots, H_s) of \mathcal{S} , we define an $(s-1)n \times sn$ matrix*

$$X = \begin{pmatrix} I & -I & 0 & \cdots & 0 & 0 \\ 0 & I & -I & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & I & -I \end{pmatrix}, \quad (4.4)$$

where I denotes the $n \times n$ identity matrix, and an $M \times sn$ matrix

$$J = \begin{pmatrix} H_1 & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & H_s \end{pmatrix}. \quad (4.5)$$

We have (X, J) forms a compression for another source with deviation symmetry

$$\mathcal{S}' = \{(\mathbf{v}, \mathbf{v} + \mathbf{d}') | \mathbf{v} \in \mathbb{F}^{sn}, \mathbf{d}' \in \tilde{\mathcal{D}}\} \subset \mathbb{F}^{sn} \times \mathbb{F}^{sn}, \quad (4.6)$$

where $\tilde{\mathcal{D}}$ was defined in (2.16). If in addition, (H_1, \dots, H_s) is a perfect compression for \mathcal{S} , then (X, J) is a perfect compression for \mathcal{S}' .

Proof. Suppose

$$\left(X \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_s \end{pmatrix} \middle| J \begin{pmatrix} \mathbf{v}_1 + \mathbf{d}_1 \\ \vdots \\ \mathbf{v}_s + \mathbf{d}_s \end{pmatrix} \right) = \left(X \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_s \end{pmatrix} \middle| J \begin{pmatrix} \mathbf{u}_1 + \mathbf{f}_1 \\ \vdots \\ \mathbf{u}_s + \mathbf{f}_s \end{pmatrix} \right) \quad (4.7)$$

where $\mathbf{v}_i, \mathbf{u}_i \in \mathbb{F}^n$ for all i ; $(\mathbf{d}_1, \dots, \mathbf{d}_s), (\mathbf{f}_1, \dots, \mathbf{f}_s) \in \mathcal{D} (\Leftrightarrow \begin{pmatrix} \mathbf{d}_1 \\ \vdots \\ \mathbf{d}_s \end{pmatrix}, \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_s \end{pmatrix} \in \tilde{\mathcal{D}})$.

From the outputs of X , we get

$$\begin{pmatrix} \mathbf{v}_1 - \mathbf{v}_2 \\ \mathbf{v}_2 - \mathbf{v}_3 \\ \vdots \\ \mathbf{v}_{s-1} - \mathbf{v}_s \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1 - \mathbf{u}_2 \\ \mathbf{u}_2 - \mathbf{u}_3 \\ \vdots \\ \mathbf{u}_{s-1} - \mathbf{u}_s \end{pmatrix} \Rightarrow \begin{pmatrix} \mathbf{v}_1 - \mathbf{u}_1 \\ \mathbf{v}_2 - \mathbf{u}_2 \\ \vdots \\ \mathbf{v}_{s-1} - \mathbf{u}_{s-1} \end{pmatrix} = \begin{pmatrix} \mathbf{v}_2 - \mathbf{u}_2 \\ \mathbf{v}_3 - \mathbf{u}_3 \\ \vdots \\ \mathbf{v}_s - \mathbf{u}_s \end{pmatrix}. \quad (4.8)$$

Thus we have

$$\mathbf{w} \triangleq \mathbf{v}_1 - \mathbf{u}_1 = \mathbf{v}_2 - \mathbf{u}_2 = \cdots = \mathbf{v}_s - \mathbf{u}_s. \quad (4.9)$$

The outputs of J give

$$\begin{aligned} \begin{pmatrix} H_1(\mathbf{v}_1 + \mathbf{d}_1) \\ \vdots \\ H_s(\mathbf{v}_s + \mathbf{d}_s) \end{pmatrix} &= \begin{pmatrix} H_1(\mathbf{u}_1 + \mathbf{f}_1) \\ \vdots \\ H_s(\mathbf{u}_s + \mathbf{f}_s) \end{pmatrix} \\ \begin{pmatrix} H_1(\mathbf{w} + \mathbf{d}_1) \\ \vdots \\ H_s(\mathbf{w} + \mathbf{d}_s) \end{pmatrix} &= \begin{pmatrix} H_1(\mathbf{f}_1) \\ \vdots \\ H_s(\mathbf{f}_s) \end{pmatrix} \end{aligned} \quad (4.10)$$

Since $(\mathbf{w} + \mathbf{d}_1, \dots, \mathbf{w} + \mathbf{d}_s)$ and $(\mathbf{f}_1, \dots, \mathbf{f}_s) \in \mathcal{S}$ and (H_1, \dots, H_s) is a compression for \mathcal{S} , we have $(\mathbf{w} + \mathbf{d}_1, \dots, \mathbf{w} + \mathbf{d}_s) = (\mathbf{f}_1, \dots, \mathbf{f}_s)$. By (2.8) and the fact that $(\mathbf{d}_1, \dots, \mathbf{d}_s)$ and $(\mathbf{f}_1, \dots, \mathbf{f}_s)$ are both in \mathcal{D} , we get

$$\mathbf{w} = \mathbf{0} \text{ and } (\mathbf{d}_1, \dots, \mathbf{d}_s) = (\mathbf{f}_1, \dots, \mathbf{f}_s), \quad (4.11)$$

i.e.

$$\begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_s \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_s \end{pmatrix} \text{ and } \begin{pmatrix} \mathbf{v}_1 + \mathbf{d}_1 \\ \vdots \\ \mathbf{v}_s + \mathbf{d}_s \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1 + \mathbf{f}_1 \\ \vdots \\ \mathbf{u}_s + \mathbf{f}_s \end{pmatrix}. \quad (4.12)$$

Thus, (X, J) is a compression for \mathcal{S}' .

Finally, if (H_1, \dots, H_s) is a perfect compression, then $|\mathcal{C}| = |\mathcal{S}| = |\mathbb{F}|^n |\mathcal{D}|$. On the other hand, the target space of (X, J) is $\mathbb{F}^{(s-1)n} \times \mathcal{C}$, whose cardinality is $|\mathbb{F}|^{(s-1)n} |\mathcal{C}| = |\mathbb{F}|^{sn} |\mathcal{D}| = |\mathbb{F}|^{sn} |\mathcal{D}| = |\mathcal{S}'|$. Therefore, (X, J) is also a perfect compression. \square

Theorem 4.2 (Existence of Parent Matrix). *Given a compression (H_1, \dots, H_s) , \exists a surjective parent matrix P of \mathcal{S} satisfying (2.18) and (2.19) with $\text{null}H_i \subset \text{null}Q_i$ for all i . Moreover, if H_i are surjective for all i , then P is an $(M-n) \times sn$ matrix such that for finite \mathbb{F} , $P|_{\mathcal{D}}$ is bijective if and only if (H_1, \dots, H_s) is a perfect compression.*

Proof. Lemma 4.2 tells us that the corresponding (X, J) defined in (4.4) and (4.5) is a compression of \mathcal{S}' (c.f. (4.6)). By Theorem 4.1, any two matrices with null spaces $\{0\}$ and $\text{null}X \oplus \text{null}J$ also forms a compression for \mathcal{S}' . Therefore, $(I_{sn \times sn}, P)$ is a compression of \mathcal{S}' , where P is an $r \times sn$ surjective matrix with $\text{null}P = \text{null}X \oplus \text{null}J$. It follows that

$$r = sn - \dim \text{null}X - \dim \text{null}J. \quad (4.13)$$

To see P is the parent matrix that we are looking for, we partition P into $P = [Q_1, \dots, Q_s]$, where Q_i are $r \times n$ matrices for all i . We have $Q_1 + Q_2 + \dots + Q_s = 0$ since

$$\text{null}X = \left\{ \begin{pmatrix} \mathbf{v} \\ \vdots \\ \mathbf{v} \end{pmatrix} \middle| \mathbf{v} \in \mathbb{F}^n \right\} \subset \text{null}P. \quad (4.14)$$

Thus P satisfies (2.19). Moreover,

$$\text{null}J = \left\{ \begin{pmatrix} \mathbf{n}_1 \\ \vdots \\ \mathbf{n}_s \end{pmatrix} \middle| \mathbf{n}_i \in \text{null}H_i \text{ for } 1 \leq i \leq s \right\} \subset \text{null}P \quad (4.15)$$

implies

$$\text{null}H_i \subset \text{null}Q_i \text{ for all } i. \quad (4.16)$$

To prove $P|_{\tilde{\mathcal{D}}}$ is injective (c.f. (2.18)), we let $\mathbf{d}', \mathbf{f}' \in \tilde{\mathcal{D}}$. Suppose $P\mathbf{d}' = P\mathbf{f}'$. We have

$$(I_{sn \times sn} \mathbf{0}, P(\mathbf{0} + \mathbf{d}')) = (I_{sn \times sn} \mathbf{0}, P(\mathbf{0} + \mathbf{f}')). \quad (4.17)$$

Since both $(\mathbf{0}, \mathbf{0} + \mathbf{d}')$ and $(\mathbf{0}, \mathbf{0} + \mathbf{f}')$ belong to \mathcal{S}' and $(I_{sn \times sn}, P)|_{\mathcal{S}'}$ is injective, we get $\mathbf{d}' = \mathbf{f}'$ and hence P satisfies (2.18).

Next if H_i are surjective for all i , then

$$M + \dim \text{null}(H_1, \dots, H_s) = sn \quad (4.18)$$

$$M + \dim \text{null}J = sn$$

$$M - n = sn - \dim \text{null}J - \dim \text{null}X$$

because $\dim \text{null}X = n$. Hence (4.13) becomes

$$r = M - n \quad (4.19)$$

that P is an $(M - n) \times sn$ matrix. Lastly for finite \mathbb{F} , (H_1, \dots, H_s) is a perfect compression iff $|\mathbb{F}|^{M-n} = |\tilde{\mathcal{D}}|$ by (3.1), iff $P|_{\tilde{\mathcal{D}}}$ is bijective as we have already shown $P|_{\tilde{\mathcal{D}}}$ is injective. \square

Theorem 4.3 (Uniqueness of Partition Codes). *Every linear lossless compression of a source with deviation symmetry is a Pre-Matrix Partition Code with a parent matrix obtained in Theorem 4.2. If the compression is linear-optimal or perfect, then the code is a Matrix Partition Code.*

Proof. Let (H_1, \dots, H_s) be a compression and P be the corresponding parent

matrix in Theorem 4.2. We have $\text{null} \begin{pmatrix} Q_1 \\ \vdots \\ Q_s \\ H_1 \\ \vdots \\ H_s \end{pmatrix} \subset \text{null} \begin{pmatrix} H_1 \\ \vdots \\ H_s \end{pmatrix} = \{\mathbf{0}\}$ by Lemma

4.1. Hence $\begin{pmatrix} Q_1 \\ \vdots \\ Q_s \\ H_1 \\ \vdots \\ H_s \end{pmatrix}$ is injective. By Theorem 2.1, (H'_1, \dots, H'_s) is a compression

of Pre-Matrix Partition Code if $\text{null}H'_i = \text{null} \begin{pmatrix} Q_i \\ H_i \end{pmatrix}$ for all i . In particular, (H_1, \dots, H_s) itself is such a compression because $\text{null}H_i \subset \text{null}Q_i$ (c.f. (4.16)).

If in addition that the compression code is linear-optimal or perfect, then it must be a Matrix Partition Code by the coronaries of Theorem 2.2. \square

Given an \mathcal{S} , there always exists a linear-optimal compression (H_1, \dots, H_s) for it. For finite field, if the compression is perfect, then $|\mathcal{S}| = |\mathcal{C}|$ and we could not extend \mathcal{S} without compromising the minimal compression sum-ratio. Otherwise, we have room to add more elements to \mathcal{S} without changing the compression. We can enlarge (see the proof of Theorem 3.1) the corresponding set $\tilde{\mathcal{D}}$ (and hence the \mathcal{S} per se) until the surjective parent matrix P (c.f. Theorem 4.2) we are working with becomes bijective when restricted to the extended $\tilde{\mathcal{D}}$. The compression for the extended \mathcal{S} is now perfect and we cannot extend thing further. Hence the extended \mathcal{S} is one of the largest sets containing \mathcal{S} that admit the same minimal sum-ratio. Conversely, let $\mathcal{S}' \supset \mathcal{S}$ and both admit the same minimal sum-ratio. Let (H'_1, \dots, H'_s) be a linear-optimal compression for \mathcal{S}' . The compression must be perfect or \mathcal{S}' is not one of those largest by the same argument. Notices that the compression works for \mathcal{S} , a subset of \mathcal{S}' . Actually, it is a linear-optimal compression for \mathcal{S} .

This method does not work for infinite field. Even with both $(H_1, \dots, H_s)|_{\mathcal{S}}$ and $P|_{\tilde{\mathcal{D}}}$ being bijective, there can be another compression (H'_1, \dots, H'_s) with the same compression sum-ratio such that $(H'_1, \dots, H'_s)|_{\mathcal{S}}$ and $P'|_{\tilde{\mathcal{D}}}$ is merely injective. Thus, \mathcal{S} can still be extended without compromising the minimal sum-ratio. Here is an example. Let $\mathbb{F} = \mathbb{R}$, $s = 2$, $n = 2$ and

$$\mathcal{D} = \{(\mathbf{0}, a\mathbf{e}_1), (\mathbf{0}, b\mathbf{e}_2) \mid |a| \geq 1, |b| < 1\}. \quad (4.20)$$

Notice that the two dimensional vector space $\{(\mathbf{v}, \mathbf{v}) \mid \mathbf{v} \in \mathbb{R}^2\}$ is a proper subset of \mathcal{S} . Hence \mathcal{S} cannot be compressed into \mathcal{C} if $\dim \mathcal{C} \leq 2$. It is not difficult to see that $\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, (1 \ 1)\right)$ is a compression for \mathcal{S} and it is bijective when restricted to \mathcal{S} . The compression is linear-optimal as $\dim \mathcal{C} = 3$. The parent matrix $P = \begin{pmatrix} -1 & -1 & 1 & 1 \end{pmatrix}$ is also bijective when restricted to the corresponding $\tilde{\mathcal{D}}$. Now $\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, (2 \ 1)\right)$ is another compression for \mathcal{S} with parent matrix $P' = \begin{pmatrix} -2 & -1 & 2 & 1 \end{pmatrix}$. Neither $\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, (2 \ 1)\right)|_{\mathcal{S}}$ nor $P'|_{\tilde{\mathcal{D}}}$ is bijective.

5 Matrix Partition Codes for Hamming Sources

In this section, we will use Hamming sources described in (2.10) to give more concrete examples for Matrix Partition Codes. Moreover, we will discuss linear-optimal compression for Hamming sources over both finite and infinite fields.

5.1 Parent matrix P of a Matrix Partition Code for a Hamming Source

Recall a Hamming source \mathcal{S} described by (2.10). For $s \geq 3$, we have \mathcal{D} in (2.11). The corresponding

$$\tilde{\mathcal{D}} = \{a\mathbf{e}_i \mid a \in \mathbb{F}, 1 \leq i \leq sn\} \subset \mathbb{F}^{sn} \quad (\text{c.f. (2.16)}). \quad (5.1)$$

To have an $r \times sn$ matrix P satisfying (2.18), the necessary and sufficient condition is

$$\text{each column of } P \text{ can't be the multiple of the other.} \quad (5.2)$$

Say if $\mathbf{P}_i = a\mathbf{P}_j$, where \mathbf{P}_i and \mathbf{P}_j are the i -th and j -th column of P , respectively; and $a \in \mathbb{F}$. Then $P(\mathbf{e}_i) = P(a\mathbf{e}_j)$ and (2.18) implies $i = j$ and $a = 1$. Conversely if $P(a\mathbf{e}_i) = P(b\mathbf{e}_j)$, then $a\mathbf{P}_i = b\mathbf{P}_j$. Condition (5.2) will imply $a = b = 0$ or $a = b \neq 0$ and $i = j$, i.e., (2.18) will be fulfilled. As $sn \geq 3$, we have

$$r > 1. \quad (5.3)$$

For infinite \mathbb{F} , we can always achieve (5.2) with $r = 2$. Explicitly, P can be

$$P = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_{sn} \end{pmatrix}, \quad (5.4)$$

where a_1, a_2, \dots, a_{sn} are distinct. When \mathbb{F} is finite. The condition (5.2) becomes

$$sn \leq (|\mathbb{F}|^r - 1)/(|\mathbb{F}| - 1). \quad (5.5)$$

Take $r = 2$ and $\mathbb{F} = \mathbb{Z}_5$ as an example. Condition (5.5) gives $sn \leq 6$ and P can be any segment of

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{pmatrix} \quad (5.6)$$

Now we consider $s = 2$ with \mathcal{D} given by (2.14). The corresponding

$$\tilde{\mathcal{D}} = \{a\mathbf{e}_i | a \in \mathbb{F}, s < i \leq 2s\}. \quad (5.7)$$

Let $P = [Q_1 | Q_2]$ with Q_1 and Q_2 are $r \times n$ matrices. The necessary and sufficient condition for P to satisfy (2.18) become

$$Q_1 \text{ is arbitrary; each column of } Q_2 \text{ can't be the multiple of the other.} \quad (5.8)$$

Obviously, we can further set $Q_1 = -Q_2$ such that (2.19) will be satisfied. Again we can always achieve (5.8) with $r = 2$ if \mathbb{F} is infinite, e.g. we can set

$$Q_2 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}, \quad (5.9)$$

with distinct elements a_1, \dots, a_n of \mathbb{F} . For finite \mathbb{F} , the condition (5.8) become

$$n \leq (|\mathbb{F}|^r - 1)/(|\mathbb{F}| - 1). \quad (5.10)$$

5.2 Linear-Optimal compression for Hamming Source with $s = 2$

As in the last section (5.7)-(5.10) mentioned. We take

$$P = [-Q_2; Q_2]. \quad (5.11)$$

with Q_2 satisfying the condition (5.8). Let C_2 be a row basis matrix of Q_2 as in the Matrix Partition Code. Then C_2 also fulfills (5.8). For simplicity, we

assume Q_2 itself is surjective and $C_2 = Q_2$. Notice that Q_2 also equal to the Y in (2.33) Let $T = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$ be the matrix that fulfills (2.34), we have

$$\left(U_1 \begin{pmatrix} G_1 \\ Q_2 \end{pmatrix}, U_2 \begin{pmatrix} G_2 \\ Q_2 \end{pmatrix} \right) \text{ forms a Matrix Partition Code for } \mathcal{S}, \quad (5.12)$$

for any invertible matrices U_1, U_2 with appropriate sizes. Notice that $\begin{pmatrix} T \\ Q_2 \end{pmatrix}$ is invertible by (2.34) with $Q_2 = Y$. Let U_1 be the inverse of $\begin{pmatrix} T \\ Q_2 \end{pmatrix}$ and U_2 be an identity matrix. Put $G_1 = T$ and G_2 as void, we get a compression

$$(I_{n \times n}, Q_2). \quad (5.13)$$

Let Q_2 be an $r' \times n$ matrix. The total code length for (5.13) and hence for (5.12) as well is

$$M = n + r' \quad (5.14)$$

For finite \mathbb{F} and a given n . We must have $|\mathcal{S}| \leq |\mathcal{C}|$, ie

$$\begin{aligned} |\mathcal{S}| &= |\mathbb{F}|^n (1 + n(|\mathbb{F}| - 1)) \leq |\mathbb{F}|^{n+r'} \\ n &\leq (|\mathbb{F}|^{r'} - 1) / (|\mathbb{F}| - 1). \end{aligned} \quad (5.15)$$

The total code length M will be minimized if r' is the smallest integer satisfying (5.15). Fortunately, such r' observes the sufficient condition (5.10) with $r = r'$. That means we can always pick a Q_2 with that r and get linear-optimal compressions.

For infinite \mathbb{F} and $n = 1$, $\{[1], [1]\}$ is a linear-optimal compression, since something like $\{[1], \text{void}\}$ would give the same output for $\{\mathbf{e}_1, \mathbf{e}_1\}$ and $\{\mathbf{e}_1, 2\mathbf{e}_1\}$. For $n \geq 2$, we can always pick $r = 2$ with Q_2 defined in (5.9) to get Matrix Partition Codes (5.12) with $M = n + 2$. The compression obtained is actually linear-optimal. Let (H'_1, H'_2) be another compression with another codeword space \mathcal{C}' . The proper subset

$$\mathcal{B} = \{(\mathbf{v}, \mathbf{v} + a\mathbf{e}_1) | \mathbf{v} \in \mathbb{F}^n, a \in \mathbb{F}\} \subset \mathcal{S} \quad (5.16)$$

is a vector space with dimension $n + 1$. Since all of the compressions considered are linear and injective within \mathcal{S} , the output of \mathcal{B} is a vector subspace of \mathcal{C}' with $\dim n + 1$. To accommodate the output of the $(\mathbf{0}, \mathbf{e}_2)$, which belongs to \mathcal{S} but not \mathcal{B} , $\dim \mathcal{C}'$ must be at least $n + 2$.

5.3 Optimal Lossless Compression for Hamming Source over Infinite Fields

We have found such a compression for $s = 2$ in the previous section. So let $s \geq 3$. For $n = 1$, the linear-optimal compression is $\{[1], \dots, [1]\}$. The reason is the same as the case of $s = 2$.

Now let $s \geq 3$ and $n \geq 2$. First we will deal with the compression ratio. By more or less the same argument of the two-source case (c.f. (5.16)), the

dimension of the codeword space \mathcal{C} cannot be less than $n + 2$. In addition, each column within any encoding matrix cannot be multiple of each other. Say if $(H_1)_i = a(H_1)_j$, then $(a\mathbf{e}_i, \mathbf{0}, \dots, \mathbf{0})$ and $(\mathbf{e}_j, \mathbf{0}, \dots, \mathbf{0})$ will share the same output. That means each encoding matrix has at least 2 rows since $n \geq 2$. Therefore we have

$$\dim \mathcal{C} \geq \max(n + 2, 2s). \quad (5.17)$$

Now we are going to build a compression for S over \mathbb{F} with characteristic 0 and $\dim \mathcal{C} = \max(n + 2, 2s)$. By (5.17), that compression will be a linear-optimal compression. We construct a $2 \times sn$ matrix P , the parent matrix, through its component $P = [Q_1 | \dots | Q_s]$ (c.f. (2.19)). We will make use of the fact that \mathbb{F} contains all rational numbers as a subfield. Let p_1, p_2, \dots, p_s, q be prime numbers such that

$$0 < p_s = p_1 < p_2 < \dots < p_{s-1} < q. \quad (5.18)$$

Let

$$\begin{cases} t_{2i-1} &= p_i q \\ t_{2i} &= p_{i+1} \end{cases} \quad \text{for } 1 \leq i < s. \quad (5.19)$$

We define the j -th column of Q_i as

$$(Q_i)_j = \begin{pmatrix} t_{2i-1}^j \\ t_{2i}^j \end{pmatrix} = \begin{pmatrix} (p_i q)^j \\ p_{i+1}^j \end{pmatrix} \quad \text{for } 1 \leq i < s, 1 \leq j \leq n. \quad (5.20)$$

They are not multiplier of each other. Say if $(Q_i)_j$ is a multiplier of $(Q_k)_l$, then

$$(p_i q)^j p_{k+1}^l = (p_k q)^l p_{i+1}^j, \quad (5.21)$$

which gives $i = k$ and $l = j$. We put $Q_s = -(Q_1 + \dots + Q_{s-1})$ and get

$$(Q_s)_j = - \begin{pmatrix} q^j (p_1^j + p_2^j + \dots + p_{s-1}^j) \\ p_2^j + p_3^j + \dots + p_s^j \end{pmatrix} \quad \text{for } 1 \leq j \leq n, \quad (5.22)$$

which is a multiplier of $\begin{pmatrix} q^j \\ 1 \end{pmatrix}$ since $p_1 = p_s$. Obviously the vectors in (5.22) are not multipliers of the others nor multipliers of those in (5.20). Hence by (5.2), our P satisfies (2.18). It fulfils (2.19) by construction.

If $2(s-1) \geq n$, we let T' (c.f. (2.20)) be a void matrix and have an injective $2(s-1) \times n$ matrix

$$R = \begin{pmatrix} Q_1 \\ \vdots \\ Q_{s-1} \end{pmatrix} = \begin{pmatrix} t_1 & t_1^2 & \dots & t_1^n \\ t_2 & t_2^2 & \dots & t_2^n \\ \dots & \dots & \dots & \dots \\ t_{2(s-1)} & t_{2(s-1)}^2 & \dots & t_{2(s-1)}^n \end{pmatrix} \quad (5.23)$$

It is injective as it contains the minor

$$\begin{pmatrix} t_1 & t_1^2 & \dots & t_1^n \\ t_2 & t_2^2 & \dots & t_2^n \\ \dots & \dots & \dots & \dots \\ t_n & t_n^2 & \dots & t_n^n \end{pmatrix} \quad (5.24)$$

whose determinant is

$$t_1 t_2 \cdots t_n \prod_{i>j} (t_i - t_j) \neq 0 \text{ (c.f. (5.19))}. \quad (5.25)$$

By Theorem 2.1, (Q_1, \dots, Q_s) is a compression for \mathcal{S} , a linear-optimal compression (c.f. (5.17)). It is also a Matrix Partition Code with void T and $C_i = Q_i$ for all i .

For $2(s-1) < n$, we pick any nonzero t_{2s-1}, \dots, t_n such that $t_i \neq t_j$ for all $i \neq j$. We let

$$T' = \begin{pmatrix} t_{2s-1} & t_{2s-1}^2 & \cdots & t_{2s-1}^n \\ t_n & t_n^2 & \cdots & t_n^n \end{pmatrix}. \quad (5.26)$$

Then

$$R = \begin{pmatrix} Q_1 \\ \vdots \\ Q_{s-1} \\ T' \end{pmatrix} = \begin{pmatrix} t_1 & t_1^2 & \cdots & t_1^n \\ t_2 & t_2^2 & \cdots & t_2^n \\ \vdots & \vdots & \ddots & \vdots \\ t_n & t_n^2 & \cdots & t_n^n \end{pmatrix}, \quad (5.27)$$

whose determinant is not zero as all t_i are distinct. Hence R is injective (actually bijective) and by Theorem 2.1, $\begin{pmatrix} G_1 \\ Q_1 \end{pmatrix}, \dots, \begin{pmatrix} G_s \\ Q_s \end{pmatrix}$ is a compression

of S , a linear-optimal compression again, where $\begin{pmatrix} G_1 \\ \vdots \\ G_s \end{pmatrix} = T'$. It is a Matrix

Partition Code with $T = T'$, $Y = \begin{pmatrix} Q_1 \\ \vdots \\ Q_{s-1} \end{pmatrix}$ and $C_i = Q_i$ for all i .

Actually, for infinite field \mathbb{F} with any characteristic, the chance for two randomly picked vectors (with more than one entry) to be multipliers of the others are virtually zero. So one may just pick Q_1, Q_2, \dots, Q_{s-1} randomly, instead of (5.20). Then define Q_s as $-(Q_1 + Q_2 + \dots + Q_{s-1})$. The chance to have a pair of columns in $P = [Q_1 | \dots | Q_s]$ that are multipliers of the others are

again virtually zero. Moreover, $\begin{pmatrix} Q_1 \\ \vdots \\ Q_{s-1} \end{pmatrix}$ should have full rank as its entries are

randomly selected. So if $2(s-1) \geq n$, then $\begin{pmatrix} Q_1 \\ \vdots \\ Q_{s-1} \end{pmatrix}$ should be injective and

(Q_1, \dots, Q_s) forms a linear-optimal compression like the aforementioned exam-

ple. For $2(s-1) < n$, we should be able to augment $\begin{pmatrix} Q_1 \\ \vdots \\ Q_{s-1} \end{pmatrix}$ to a bijective

$\begin{pmatrix} Q_1 \\ \vdots \\ Q_{s-1} \\ T \end{pmatrix}$. Then $\begin{pmatrix} G_1 \\ Q_1 \end{pmatrix}, \dots, \begin{pmatrix} G_s \\ Q_s \end{pmatrix}$ will forms an linear-optimal compression for

S as before.

6 Structure of Deviation Symmetry

Given n, s, \mathbb{F} , let Σ be the set of sources with deviation symmetry. For any $\mathcal{S} \in \Sigma$, we pick a representative set $\mathcal{D}(\mathcal{S})$ of it. Notice that we have n degree of freedom in choosing a particular $\delta \in \mathcal{D}(\mathcal{S})$. Therefore it is possible to fix a certain component to be a constant within the whole $\mathcal{D}(\mathcal{S})$. Say if we want to fix the last component to be zero, then we simply replace $\delta = (\mathbf{d}_1, \dots, \mathbf{d}_s)$ with $(\mathbf{d}_1, \dots, \mathbf{d}_s) - (\mathbf{d}_s, \dots, \mathbf{d}_s), \forall (\mathbf{d}_1, \dots, \mathbf{d}_s) \in \mathcal{D}(\mathcal{S})$. We call such fixing as component-fixing. Since each component contains n entries, the component-fixing eliminates all n degrees of freedom in choosing δ .

Let us impose a component-fixing throughout the Σ . It can be shown that $\mathcal{S}_1 \subset \mathcal{S}_2$ if and only if $\mathcal{D}(\mathcal{S}_1) \subset \mathcal{D}(\mathcal{S}_2)$. Now \mathcal{D} can be viewed as an injective mapping. It is more than that. More specifically, after fixing the last component to be zero, then $\mathcal{D} : \Sigma \rightarrow \text{power set of } \underbrace{\mathbb{F}^n \times \dots \times \mathbb{F}^n}_{s-1 \text{ terms}} \times \{\mathbf{0}\}$ becomes a bijective

mapping. Power set of a set is a σ -algebra for sure. Actually, we can show by definition (2.1) that Σ is also a σ -algebra. The bijective mapping \mathcal{D} preserves their structures in sense that $\mathcal{D}(\bigcup_{i=1}^{\infty} \mathcal{S}_i) = \bigcup_{i=1}^{\infty} \mathcal{D}(\mathcal{S}_i)$, $\mathcal{D}(\mathcal{S}^c) = \mathcal{D}(\mathcal{S})^c$ and $\mathcal{D}(\emptyset) = \emptyset$, where c stands for complement.

Throughout the paper, we say \mathcal{S} can be compressed by the encoding matrices (H_1, \dots, H_s) if $(H_1, \dots, H_s)|_{\mathcal{S}}$ is injective, which does not specify if the source actually is compressed into a smaller space. To distinguish thing, we will say \mathcal{S} is compressible if and only if it can be compressed by (H_1, \dots, H_s) into a lower dimensional space (i.e. $\dim \mathcal{C} < sn$). We will make use of the component-fixing to determine the necessary and sufficient condition for \mathcal{S} to be compressible.

Theorem 6.1. *\mathcal{S} is compressible if and only if there exists a subset \mathcal{D}_- of $\mathbb{F}^{n-1} \times \underbrace{\mathbb{F}^n \times \dots \times \mathbb{F}^n}_{s-2 \text{ terms}}$ such that the representative set \mathcal{D} can be expressed as*

$$\mathcal{D} = \left\{ \pi \left(B \begin{bmatrix} f(\mathbf{d}_1, \dots, \mathbf{d}_{s-1}) \\ \mathbf{d}_1 \end{bmatrix}, \mathbf{d}_2, \dots, \mathbf{d}_{s-1}, \mathbf{0} \right) \mid (\mathbf{d}_1, \dots, \mathbf{d}_{s-1}) \in \mathcal{D}_- \right\}, \quad (6.1)$$

where π is a position permutation of the \mathbb{F}^n -vectors, B is an $n \times n$ invertible matrix and f is a well-defined function from \mathcal{D}_- to \mathbb{F} .

Proof. " \Rightarrow " Suppose \mathcal{S} can be compressed by (H_1, \dots, H_s) into a lower dimensional space. One of the H_i , say $i = 1$ WLOG, must have a nonzero null space. So let $\mathbf{0} \neq \mathbf{v} \in \text{null} H_1$. Also let A be an $(n-1) \times n$ matrix with $\text{null } A = \text{span}\{\mathbf{v}\}$. Then \mathcal{S} can also be compressed by $(A, \underbrace{I_n, \dots, I_n}_{s-1 \text{ terms}})$ whose null space is a

subspace of (H_1, \dots, H_s) 's. Fix the last component of every $\delta \in \mathcal{D}$ to be zero. For any $\sigma \in \mathcal{S}$, \exists a unique $\mathbf{v} \in \mathbb{F}^n$ and a unique $(\mathbf{d}, \mathbf{d}_2, \dots, \mathbf{d}_s, \mathbf{0}) \in \mathcal{D}$ such that $\sigma = (\mathbf{v} + \mathbf{d}, \mathbf{v} + \mathbf{d}_2, \dots, \mathbf{v} + \mathbf{d}_{s-1}, \mathbf{v})$. We have

$$(A, \underbrace{I_n, \dots, I_n}_{s-1 \text{ terms}})\sigma = ([\mathbf{0}|I_{n-1}]B^{-1}(\mathbf{v} + \mathbf{d}), \mathbf{v} + \mathbf{d}_2, \dots, \mathbf{v} + \mathbf{d}_{s-1}, \mathbf{v}), \quad (6.2)$$

where B is an $n \times n$ invertible matrix such that $AB = [\mathbf{0}|I_{n-1}]$. Therefore, we get everything back directly, except for the first entry of $B^{-1}\mathbf{d}$. Since the \mathcal{S} can

be compressed by $(A, \underbrace{I_n, \dots, I_n}_{s-1 \text{ terms}})$ (losslessly), we must be able to retrieve the

lost part from the output. Mathematically, the first entry of $B^{-1}\mathbf{d}$ has to be a function of $[\mathbf{0}|I_{n-1}]B^{-1}\mathbf{d}, \mathbf{d}_2, \dots, \mathbf{d}_{s-1}$ and \mathbf{v} . However, we are talking about deviation symmetry that \mathcal{D} does not depend on \mathbf{v} . Therefore \mathcal{D} has the form of (6.1) with $\pi = 1$ and $\mathbf{d}_1 = [\mathbf{0}|I_{n-1}]B^{-1}\mathbf{d}$.

" \Leftarrow " Conversely, given (6.1), we let $H_1 = [\mathbf{0}|I_{n-1}]B^{-1}$, $H_2 = H_3 = \dots = H_s = I_n$. Then \mathcal{S} can be compressed by $(H_{\pi(1)}, \dots, H_{\pi(s)})$ losslessly. \square

The argument in the theorem can be generalized until null $H_i \neq \{\mathbf{0}\}$ for all i , i.e. actual compression happens at each terminal.

7 Conclusion

In this paper, we study zero-error linear coding of a set of rather general sources known as sources with deviation symmetry. Matrix Partition Codes can be used to efficiently compress sources with deviation symmetry. We will conclude here by summarizing the construction procedure of a Matrix Partition Code in the following. Suppose we want to compress a source with deviation symmetry \mathcal{S} losslessly. We can simply search the compression within the framework of Theorem 2.1 because Theorem 4.3 tells us that there is no other way causing difference. So we need to fix a \mathcal{D} (c.f. (2.7), (2.5)) first. Theorem 2.3 ensures that the choice of \mathcal{D} does not affect the end results.

Then we have to find the parent matrix P , an $r \times sn$ matrix satisfying (2.18) and (2.19). Such P always exists as compression always exists. Precisely all encoding matrices are identity matrix forms a trivial compression and X (c.f. (4.4)) is the corresponding parent matrix. The problem is about the compression rate. Basically, P with lower r ends up with more efficient compression. On the other hand, it is easier to form the P with higher r . Once we get P , we can follow the mechanism of Matrix Partition Code to get a code of highest compression efficiency (with that P) in sense of Theorem 2.2 and its second corollary.

Acknowledgment

We would like to thank the associate editor and the anonymous reviewers for their times and constructive comments.

References

- [1] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. 19, pp. 471–480, Jul. 1973.
- [2] A. Wyner, "Recent results in the Shannon theory," *IEEE Trans. Inform. Theory*, vol. 20, pp. 2–10, Jan. 1974.
- [3] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction," in *Proc. DCC*, 1999, pp. 158–167.

- [4] V. Stankovic, A. D. Liveris, Z. Xiong, and C. N. Georgiades, "On code design for the Slepian-Wolf problem and lossless multiterminal networks," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1495–1507, 2006.
- [5] S. Pradhan and K. Ramchandran, "Generalized coset codes for distributed binning," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3457–3474, 2005.
- [6] 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.
- [7] A. Liveris, Z. Xiong, and C. Georgiades, "Nested convolutional/turbo codes for the binary Wyner-Ziv problem," in *Proc. ICIP'03*, Barcelona, Spain, Sep 2003.
- [8] 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.
- [9] P. Mitran and J. Bajcsy, "Coding for the Wyner-Ziv problem with turbo-like codes," in *Proc. ISIT'02*, Lausanne, Switzerland, Jun 2002.
- [10] 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.
- [11] S. Servetto, "Lattice quantization with side information," in *Proc. DCC'00*, Snowbird, UT, Mar 2000.
- [12] M. Zamani and F. Lahouti, "A flexible rate Slepian-Wolf code construction," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2301–2308, 2009.
- [13] A. Al Jabri and S. Al-Issa, "Zero-error codes for correlated information sources," *Cryptography and Coding*, pp. 17–22, 1997.
- [14] 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.
- [15] —, "On zero-error source coding with decoder side information," *IEEE Trans. Inform. Theory*, vol. 49, no. 1, pp. 99–111, 2003.
- [16] Y. Yan and T. Berger, "On instantaneous codes for zero-error coding of two correlated sources," in *Proc. ISIT. IEEE*, 2000, p. 344.
- [17] R. Ma and S. Cheng, "The universality of generalized hamming code for multiple sources," *Communications, IEEE Transactions on*, no. 99, pp. 1–7, 2011.
- [18] 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.
- [19] R. Ma and S. Cheng, "Hamming coding for multiple sources," in *Proc. ISIT'10*, Austin, TX, June 2010.