Product Construction of Affine Codes

Yeow Meng Chee*, Han Mao Kiah§, Punarbasu Purkayastha*, Patrick Solé†‡
*School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
§Coordinated Science Lab, University of Illinois at Urbana-Champaign, USA
†Institut Mines-Télécom, Télécom ParisTech, CNRS LTCI, France
‡Department of Mathematics, King Abdulaziz University, Saudi Arabia
Emails: ymchee@ntu.edu.sg, hmkiah@illinois.edu, punarbasu@ntu.edu.sg, patrick.sole@telecom-paristech.fr

***Abstract*—Binary matrix codes with restricted row and column weights are a desirable method of coded modulation for power line communication. In this work, we construct such matrix codes that are obtained as products of affine codes - cosets of binary linear codes. Additionally, the constructions have the property that they are systematic. Subsequently, we generalize our construction to irregular product of affine codes, where the component codes are affine codes of different rates.**

***Index Terms*—Product codes, Affine codes, Irregular product codes, Power line communications.**

1. Introduction

Product codes were introduced by Elias [1] and subsequently generalized by Forney [2] to concatenated codes. Product codes are a method of constructing larger codes from smaller codes while retaining the good rates and good decoding complexity from the smaller codes. The codewords of a product code can be written as matrices with the rows belonging to the row component code and the columns belonging to the column component code. List decoding algorithms have also been studied in this context in Barg and Zemor [3] where the min-sum algorithm was shown to be amenable to list decoding of product codes.

Product codes have been subsequently generalized to yield codes obtained from product of nonlinear codes by Amrani [4], and to multilevel product codes by Zyablov *et al.* [5]. Amrani [4] gave the construction of product codes from component nonlinear codes which are binary and systematic. The construction guarantees that all the columns of any codeword belong to the column component code; however only the first few rows corresponding to the systematic part of the column code are guaranteed to belong to the row code. In the case where one of the component codes is linear, Amrani [4] proposed two soft-decision decoding algorithms. Irregular product codes, introduced by Alipour *et al.* [7], are yet another generalization of product codes where each row and column code can be a code of different rate. Irregular product codes were introduced to address the need for unequal error protection from bursty noise when some parts of the codeword are more vulnerable to burst errors than others.

In this work we study constructions of binary systematic nonlinear product codes which are obtained as products of affine codes – cosets of linear codes. In contrast to the work of Amrani [4], our construction guarantees that all the rows belong to the (affine) row code and all the columns belong to the (affine) column code. One primary motivation for studying such class of codes arises from a previous study on coded modulation for power line channels by Chee *et al.* [8] that proposed a generalization of the coded modulation scheme of Vinck [9].

Chee *et al.* [8] showed that binary matrix codes with bounded column weights, in conjunction with multitone frequency shift keying, can be used to counter the harsh noise characteristics of the power line channel. Concatenated codes obtained from the concatenation of constant weight inner codes with Reed-Solomon outer codes were used to obtain families of efficiently decodable codes with good rates and good relative distances. In this work, we continue this line of investigation and introduce systematic product codes with the additional restriction that the row weights are also bounded. The restriction on the column weight arises from the desire to be able to detect and correct impulse noise that is present in the power line channel. The restriction on the row weights allows one to detect and correct narrowband noise. It is quite evident that product codes obtained from the product of linear codes do not satisfy these restrictions. The nonlinear codes studied in this paper are constructed to satisfy these properties. The efficient decoding algorithms of product codes are directly applicable to the constructions presented in this work. As a first step to the decoding process, we subtract the coset representative that is used in the construction. The coset representative is explicitly described, as explained in the following sections.

The rest of the paper is organized as follows. In the next section we introduce the basic definitions and notation that are used throughout the rest of this paper. Section 3 discusses the general construction of systematic codes which are products of affine codes. Section 4 uses the construction in Section 3 to give constructions of product codes with restricted row and column weights. This is of interest because of its application to coded modulation for power line channels. In Section 5, we extend this construction to product codes which can provide unequal error protection, where different rows and columns belong to different row and column codes. This section generalizes the irregular product code construction of Alipour *et al.* [7], where the component codes are linear codes, to irregular product codes where the component codes are affine codes.

2. Notation and Definitions

Denote the finite field of order two by $\mathbb{F}_2$. A *binary code* $\mathcal{C}$ of length n is a subset of $\mathbb{F}_2^n$, while a *binary linear code* $\mathcal{C}$ of length n is a linear subspace of $\mathbb{F}_2^n$. The *dimension* of a linear code $\mathcal{C}$ is given by the dimension of $\mathcal{C}$ as a linear subspace of $\mathbb{F}_2^n$. Elements of $\mathcal{C}$ are called *codewords*. Endow the space $\mathbb{F}_2^n$ with the *Hamming distance* metric and for $\mathbf{u} \in \mathbb{F}_2^n$, the *Hamming weight* of $\mathbf{u}$ is the distance of $\mathbf{u}$ from the all-zero codeword. A code $\mathcal{C} \subseteq \mathbb{F}_2^n$ is said to have distance d if the (Hamming) distance between any two distinct codewords of $\mathcal{C}$ is at least d. Moreover, a linear code $\mathcal{C}$ has distance d if the weight of all nonzero codewords in $\mathcal{C}$ is at least d. A code of length n and distance d is denoted as an (n, d) code. We use the notation $[n, k, d]$ to denote a linear code of length n, dimension k and distance d.

Let m, n be positive integers and let $\mathbb{F}_2^{m\times n}$ denote the set of m by n matrices over $\mathbb{F}_2$. The *transpose* of a matrix $\mathbf{M}$ is denoted by $\mathbf{M}^T$ and we regard the vector $\mathbf{u} \in \mathbb{F}_2^n$ as a row vector or a matrix $\mathbf{u}$ in $\mathbb{F}_2^{1\times n}$. Hence, $\mathbf{u}^T$ denotes a column vector in $\mathbb{F}_2^{n\times 1}$. In addition, let $\mathbf{0}_n$ and $\mathbf{j}_n$ denote the all-zero and all-one vectors of length n respectively, while $\mathbf{I}_n$ and $\mathbf{0}_{m\times n}$ denote the $(n \times n)$ identity and $(m \times n)$ all-zero matrix respectively.

Let $\mathcal{C}$ be a linear $[n, k, d]$ code. After a permutation of coordinates, there exists a matrix $\mathbf{A} \in \mathbb{F}_2^{k\times(n-k)}$ such that each codeword in $\mathcal{C}$ can be written as $(\mathbf{x}, \mathbf{x}\mathbf{A})$, where $\mathbf{x} \in \mathbb{F}_2^k$ is called the *information vector*. The matrix $(\mathbf{I}_k|\mathbf{A})$ is said to be a *systematic encoder* of $\mathcal{C}$.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be linear $[n, k_1, d_1]$ and $[n, k_2, d_2]$ codes respectively. Suppose $\mathcal{C}_1 \subseteq \mathcal{C}_2$ and pick $\mathbf{u} \in \mathcal{C}_2$. Then the set of codewords $\mathcal{C}_1 + \mathbf{u}$ is a *coset of* $\mathcal{C}_1$ *in* $\mathcal{C}_2$. The collection of all cosets of $\mathcal{C}_1$ in $\mathcal{C}_2$ is denoted by $\mathcal{C}_2/\mathcal{C}_1$. Moreover, any coset in $\mathcal{C}_2/\mathcal{C}_1$ is a (n, d_1) code of size 2^{k_1}, and we call the coset an *affine* $[n, k_1, d_1]$ code.

Observe that if $(\mathbf{I}_{k_1}|\mathbf{A}_1)$ is a systematic encoder for $\mathcal{C}_1$ and $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2)$ where $\mathbf{u}_1$ is of length k, then $\mathcal{C}_1 + \mathbf{u} = \mathcal{C}_1 + (\mathbf{0}_k, \mathbf{u}_2 - \mathbf{u}_1\mathbf{A}_1)$. On the other hand, every coset in $\mathcal{C}_2/\mathcal{C}_1$ contains at most one element of the form $(\mathbf{0}_k, \mathbf{a})$. Hence, for every coset $\mathcal{C}_1 + \mathbf{u}$, there is exactly one element of the form $(\mathbf{0}_k, \mathbf{a})$, and in this paper, we refer to this element as the *coset representative of* $\mathcal{C}_1 + \mathbf{u}$. The set of all coset representatives of cosets in $\mathcal{C}_2/\mathcal{C}_1$ is denoted $(\mathcal{C}_2/\mathcal{C}_1)_{\rm rep}$.

We also consider the notion of systematicity for nonlinear codes. Let $\mathcal{C}$ be a (matrix) code of size 2^k. Then $\mathcal{C}$ is said to be *systematic of size* 2^k if there exists k coordinates such that $\mathcal{C}$ when restricted to these k coordinates is $\mathbb{F}_2^k$. Observe that if $\mathcal{C}$ is a linear $[n, k, d]$ code, then any affine code $\mathcal{C} + \mathbf{u}$ is systematic of size 2^k.

A. Binary Matrix Codes

A binary $(m \times n)$*-matrix code* $\mathcal{C}$ is a subset of $\mathbb{F}_2^{m\times n}$, while a *binary linear* $(m \times n)$*-matrix code* $\mathcal{C}$ is a linear subspace of $\mathbb{F}_2^{m\times n}$, when considered as a vector space of dimension mn. Regarding each matrix in $\mathbb{F}_2^{m\times n}$ as a vector of length mn, we have the definitions of Hamming distance, Hamming weight and dimension. A linear $(m \times n)$-matrix code of dimension K and distance d is denoted by $[m \times n, K, d]$.

B. Classical Product Codes

The classical product code constructs binary matrix codes from two binary linear codes. Given a linear $[n, k, d_{\mathcal{C}}]$ code $\mathcal{C}$ and a linear $[m, l, d_{\mathcal{D}}]$ code $\mathcal{D}$, let $(\mathbf{I}_k|\mathbf{A})$ and $(\mathbf{I}_l|\mathbf{B})$ be their respective systematic encoders. The *product code*, denoted by $\mathcal{C} \otimes \mathcal{D}$, is then given by the $(m \times n)$-matrix code (see [6, p. 568])

$$\mathcal{C} \otimes \mathcal{D} \triangleq \left\{ \left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} \\ \hline \mathbf{B}^T\mathbf{M} & \mathbf{B}^T\mathbf{M}\mathbf{A} \end{array} \right) : \mathbf{M} \in \mathbb{F}_2^{l\times k} \right\},$$

where $\mathbf{M}$ corresponds to the information bits. It can be shown that $\mathcal{C}\otimes\mathcal{D}$ is a linear $[m\times n, kl, d_{\mathcal{D}}d_{\mathcal{C}}]$ code. Furthermore, $\mathcal{C}\otimes\mathcal{D}$ has the following property that depends on the *component codes* $\mathcal{C}$ *and* $\mathcal{D}$.

Property $(\mathcal{C}, \mathcal{D})$. For every $\mathbf{N} \in \mathcal{C} \otimes \mathcal{D}$,

(i) every row of $\mathbf{N}$ belongs to $\mathcal{C}$, and
(ii) every column of $\mathbf{N}$ belongs to $\mathcal{D}$.

In this paper, we consider nonlinear component codes. Specifically, let $\mathcal{C}'$ be a nonlinear code of length n and size 2^k and $\mathcal{D}'$ be a nonlinear code of length m and size 2^l. We aim to construct an $(m \times n)$-matrix code $\mathcal{C}' \otimes \mathcal{D}'$ of size 2^{kl} such that Property $(\mathcal{C}', \mathcal{D}')$ holds.

This construction differs from the nonlinear product code construction in Amrani [4] because we guarantee that *all* the rows in every codeword belong to the row code $\mathcal{C}'$.

3. Product Codes from Affine Codes

In this section, we provide the general construction of systematic matrix codes that are obtained as products of cosets of linear codes, i.e., as products of affine codes. Throughout this section, let $\mathcal{C}$ and $\mathcal{D}$ be binary linear $[n, k, d_{\mathcal{C}}]$ and $[m, l, d_{\mathcal{D}}]$ codes, respectively. We consider affine codes that are obtained as cosets of the codes $\mathcal{C}$ and $\mathcal{D}$, i.e., they are of the form $\mathcal{C} + \mathbf{u}$ and $\mathcal{D} + \mathbf{v}$, respectively, where $\mathbf{u}$ and $\mathbf{v}$ are of lengths n and m respectively. In particular, we show that if both $\mathcal{C}$ and $\mathcal{D}$ contain the all-one vector, then there exists an $(m\times n)$-matrix code, that is systematic of size 2^{kl} with Property $(\mathcal{C} + \mathbf{u}, \mathcal{D} + \mathbf{v})$.

Let $(\mathbf{I}_k|\mathbf{A})$ and $(\mathbf{I}_l|\mathbf{B})$ be systematic encoders for $\mathcal{C}$ and $\mathcal{D}$ respectively. Without loss of generality, pick $\mathbf{u} = (\mathbf{0}_k, \mathbf{a}) \in (\mathbb{F}_2^n/\mathcal{C})_{\rm rep}$ and $\mathbf{v} = (\mathbf{0}_l, \mathbf{b}) \in (\mathbb{F}_2^m/\mathcal{D})_{\rm rep}$. Then a typical element in $\mathcal{C} + \mathbf{u}$ is of the form $(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a})$ where $\mathbf{x}$ is the information vector of length k. Similarly, a typical element in $\mathcal{D} + \mathbf{v}$ is of the form $(\mathbf{x}, \mathbf{x}\mathbf{B} + \mathbf{b})$ where $\mathbf{x}$ is the information vector of length l.

Define $(\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v})$ to be the $(m\times n)$-matrix code given by (1). This is obtained by the encoding the first k columns by $\mathcal{D}+\mathbf{v}$, followed by encoding all the rows by $\mathcal{C}+\mathbf{u}$. We observe that for every $\mathbf{N} \in (\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v})$, each row of $\mathbf{N}$ belongs to $\mathcal{C}+\mathbf{u}$. However, we can guarantee only that the first k columns belong to $\mathcal{D}+\mathbf{v}$.

$$(\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v}) \triangleq \left\{ \left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A}+\mathbf{j}_l^T\mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M}+\mathbf{b}^T\mathbf{j}_k & (\mathbf{B}^T\mathbf{M}+\mathbf{b}^T\mathbf{j}_k)\mathbf{A}+\mathbf{j}_{m-l}^T\mathbf{a} \end{array} \right) : \mathbf{M}\in\mathbb{F}_2^{l\times k} \right\}. \quad (1)$$

$$(\mathcal{C}+\mathbf{u})\widetilde{\otimes}(\mathcal{D}+\mathbf{v}) \triangleq \left\{ \left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A}+\mathbf{j}_l^T\mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M}+\mathbf{b}^T\mathbf{j}_k & \mathbf{B}^T(\mathbf{M}\mathbf{A}+\mathbf{j}_l^T\mathbf{a})+\mathbf{b}^T\mathbf{j}_{n-k} \end{array} \right) : \mathbf{M}\in\mathbb{F}_2^{l\times k} \right\}. \quad (2)$$

On the other hand, if we alter the definition given in (1) to be (2), where we encode the first l rows by $\mathcal{C}+\mathbf{u}$, followed by encoding all the columns using $\mathcal{D}+\mathbf{v}$, we have that every column of $\mathbf{N}$ belongs to $\mathcal{D}+\mathbf{v}$ for each $\mathbf{N}\in(\mathcal{C}+\mathbf{u})\widetilde{\otimes}(\mathcal{D}+\mathbf{v})$.

Therefore, the matrix code $(\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v})$ meets our requirements if

$$(\mathbf{B}^T\mathbf{M}+\mathbf{b}^T\mathbf{j}_k)\mathbf{A}+\mathbf{j}_{m-l}^T\mathbf{a} = \mathbf{B}^T(\mathbf{M}\mathbf{A}+\mathbf{j}_l^T\mathbf{a})+\mathbf{b}^T\mathbf{j}_{n-k}, \text{that is,}$$

$$\mathbf{b}^T(\mathbf{j}_k\mathbf{A}+\mathbf{j}_{n-k}) = (\mathbf{B}^T\mathbf{j}_l^T+\mathbf{j}_{m-l}^T)\mathbf{a} \quad (3)$$

If (3) holds, then $(\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v})$ (or equivalently, $(\mathcal{C}+\mathbf{u})\widetilde{\otimes}(\mathcal{D}+\mathbf{v})$) is a coset of $\mathcal{C}\otimes\mathcal{D}$. That is, $(\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v}) = (\mathcal{C}\otimes\mathcal{D})+\mathbf{U}$, where

$$\mathbf{U} \triangleq \left(\begin{array}{c|c} \mathbf{0}_{l\times k} & \mathbf{j}_l^T\mathbf{a} \\ \hline \mathbf{b}^T\mathbf{j}_k & \mathbf{b}^T\mathbf{j}_k\mathbf{A}+\mathbf{j}_{m-l}^T\mathbf{a} \end{array} \right). \quad (4)$$

Theorem 3.1. Let $\mathcal{C}$ and $\mathcal{D}$ be binary linear $[n,k,d_{\mathcal{C}}]$ and $[m,l,d_{\mathcal{D}}]$ codes, respectively and $(\mathbf{I}_k|\mathbf{A})$ and $(\mathbf{I}_l|\mathbf{B})$ be their corresponding systematic encoders. Pick $\mathbf{u}=(\mathbf{0}_k,\mathbf{a})\in(\mathbb{F}_2^n/\mathcal{C})_{\rm rep}$ and $\mathbf{v}=(\mathbf{0}_l,\mathbf{b})\in(\mathbb{F}_2^m/\mathcal{D})_{\rm rep}$. If in addition (3) holds, then $(\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v})$ defined by (1) is equal to $(\mathcal{C}+\mathbf{u})\widetilde{\otimes}(\mathcal{D}+\mathbf{v})$ defined by (2). Moreover, the code is systematic of size 2^{kl} and is a coset of $\mathcal{C}\otimes\mathcal{D}$ with Property $(\mathcal{C}+\mathbf{u},\mathcal{D}+\mathbf{v})$.

We now provide a sufficient condition for (3) to hold. Observe that $\mathbf{j}_n\in\mathcal{C}$ if and only if $\mathbf{j}_k\mathbf{A}=\mathbf{j}_{n-k}$, since $\mathbf{j}_k(\mathbf{I}_k|\mathbf{A})$ is necessarily $\mathbf{j}_n$. Hence, $\mathbf{j}_k\mathbf{A}+\mathbf{j}_{n-k}=\mathbf{0}_{n-k}$ and $\mathbf{b}^T(\mathbf{j}_k\mathbf{A}+\mathbf{j}_{n-k})=\mathbf{0}_{(m-l)\times(n-k)}$. Similar argument holds for $\mathbf{B}^T\mathbf{j}_l^T+\mathbf{j}_{m-l}^T$. Hence, (3) holds and the coset representative $\mathbf{U}$ given by (4) is

$$\mathbf{U} = \left(\begin{array}{c|c} \mathbf{0}_{l\times k} & \mathbf{j}_l^T\mathbf{a} \\ \hline \mathbf{b}^T\mathbf{j}_k & \mathbf{b}^T\mathbf{j}_{n-k}+\mathbf{j}_{m-l}^T\mathbf{a} \end{array} \right),$$

and is independent of matrices $\mathbf{A}$ and $\mathbf{B}$. The following corollary, that we refer to as *Construction I*, is now immediate.

Corollary 3.1 (*Construction I*)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be binary linear $[n,k,d_{\mathcal{C}}]$ and $[m,l,d_{\mathcal{D}}]$ codes, respectively and $(\mathbf{I}_k|\mathbf{A})$ and $(\mathbf{I}_l|\mathbf{B})$ be their corresponding systematic encoders. Pick $\mathbf{u}=(\mathbf{0}_k,\mathbf{a})\in(\mathbb{F}_2^n/\mathcal{C})_{\rm rep}$ and $\mathbf{v}=(\mathbf{0}_l,\mathbf{b})\in(\mathbb{F}_2^m/\mathcal{D})_{\rm rep}$. If in addition $\mathbf{j}_n\in\mathcal{C}$ and $\mathbf{j}_m\in\mathcal{D}$, then $(\mathcal{C}+\mathbf{u})\otimes(\mathcal{D}+\mathbf{v})$ defined by (1) is systematic of size 2^{kl} and is a coset of $\mathcal{C}\otimes\mathcal{D}$ with Property $(\mathcal{C}+\mathbf{u},\mathcal{D}+\mathbf{v})$.

Binary codes that contain the all-one vector are also called *self-complementary codes*. Well-known examples of linear self-complementary codes include the primitive narrow-sense Bose-Chaudhuri-Hocquenghem codes, the extended Golay code and the Reed-Müller codes [6].

4. Variants of Construction I

In this section, we adopt Construction I to certain nonlinear component codes $\mathcal{C}'$, $\mathcal{D}'$ that are variants of cosets of linear codes. Several well-known families of nonlinear codes such as Nordstrom-Robinson, Delsarte-Goethals, Kerdock and Preparata can be obtained as unions of cosets of linear codes (see [6, Ch. 15]). In general, it is difficult to achieve a matrix code with Property $(\mathcal{C}',\mathcal{D}')$ of size $2^{\log|\mathcal{C}'|\log|\mathcal{D}'|}$. Instead we show that it is possible to achieve a size of $2^{\kappa\log|\mathcal{C}'|\log|\mathcal{D}'|}$ for some positive constant $\kappa<1$.

A straightforward generalization of Construction I to union of cosets of linear codes can be achieved as follows. Let $\mathcal{C}_1$ and $\mathcal{D}_1$ be binary linear $[n,k_1,d_{\mathcal{C}_1}]$ and $[m,l_1,d_{\mathcal{D}_1}]$ such that $\mathbf{j}_n\in\mathcal{C}_1$ and $\mathbf{j}_m\in\mathcal{D}_1$. Let $\mathcal{U}\subseteq(\mathbb{F}_2^n/\mathcal{C}_1)_{\rm rep}$ and $\mathcal{V}\subseteq(\mathbb{F}_2^m/\mathcal{D}_1)_{\rm rep}$. Then we consider the component codes $\mathcal{C}'$ and $\mathcal{D}'$, where

$$\mathcal{C}'=\bigcup_{\mathbf{u}\in\mathcal{U}}\mathcal{C}_1+\mathbf{u}, \text{ and } \mathcal{D}'=\bigcup_{\mathbf{v}\in\mathcal{V}}\mathcal{D}_1+\mathbf{v}.$$

Then the $(m\times n)$-matrix code defined by

$$\bigcup_{\mathbf{u}\in\mathcal{U}}\bigcup_{\mathbf{v}\in\mathcal{V}}(\mathcal{C}_1+\mathbf{u})\otimes(\mathcal{D}_1+\mathbf{v}). \quad (5)$$

has Property $(\mathcal{C}',\mathcal{D}')$. However, observe that the code has size $|\mathcal{U}||\mathcal{V}|2^{k_1l_1}=2^{k_1l_1+\log|\mathcal{U}|+\log|\mathcal{V}|}$, while the sizes of $\mathcal{C}'$ and $\mathcal{D}'$ are $|\mathcal{U}|2^{k_1}=2^{k_1+\log|\mathcal{U}|}$ and $|\mathcal{V}|2^{l_1}=2^{l_1+\log|\mathcal{V}|}$ respectively. Thus the size of the code obtained from (5) is less than $2^{\log|\mathcal{C}'|\log|\mathcal{D}'|}=2^{(k_1+\log|\mathcal{U}|)(l_1+\log|\mathcal{V}|)}$.

A. Product Construction of Expurgated Codes

We improve the size given by (5) when the union of cosets of product codes has a certain structure. Specifically, we consider the instance where the cosets form an expurgated code. We describe this formally below.

In addition to the codes $\mathcal{C}_1,\mathcal{D}_1$, assume that $\mathcal{C}_2$ and $\mathcal{D}_2$ are binary linear $[n,k_2,d_{\mathcal{C}_2}]$ and $[m,l_2,d_{\mathcal{D}_2}]$ codes such that $\mathcal{C}_1\subset\mathcal{C}_2$ and $\mathcal{D}_1\subset\mathcal{D}_2$. We consider nonlinear component codes that are obtained from expurgated codes $\mathcal{C}_2\setminus\mathcal{C}_1$ and $\mathcal{D}_2\setminus\mathcal{D}_1$. Our objective is therefore to construct an $(m\times n)$-matrix code such that Property $(\mathcal{C}_2\setminus\mathcal{C}_1,\mathcal{D}_2\setminus\mathcal{D}_1)$ holds.

Clearly, $\mathcal{C}_2\setminus\mathcal{C}_1$ and $\mathcal{D}_2\setminus\mathcal{D}_1$ are union of cosets of $\mathcal{C}_1$ and $\mathcal{D}_1$ with $\mathcal{U}=(\mathcal{C}_2/\mathcal{C}_1)_{\rm rep}\setminus\{\mathbf{0}_n\}$ and $\mathcal{V}=(\mathcal{D}_2/\mathcal{D}_1)_{\rm rep}\setminus\{\mathbf{0}_m\}$ respectively. Then the construction described in (5) gives a code with size $(2^{k_2-k_1}-1)(2^{l_2-l_1}-1)2^{k_1l_1}\approx 2^{k_2-k_1+l_2-l_1+k_1l_1}$.

On the other hand, we improve this size via the following.

Construction IA. Consider two intermediary codes $\mathcal{C}_3$ and $\mathcal{D}_3$ of dimensions k_2-1 and l_2-1 respectively such that $\mathcal{C}_1\subseteq\mathcal{C}_3\subset\mathcal{C}_2$ and $\mathcal{D}_1\subseteq\mathcal{D}_3\subset\mathcal{D}_2$. Pick any $\mathbf{u}\in(\mathcal{C}_2\setminus\mathcal{C}_3)$ and $\mathbf{v}\in(\mathcal{D}_2\setminus\mathcal{D}_3)$ and observe that

$$\mathcal{C}_3+\mathbf{u}\subset\mathcal{C}_2\setminus\mathcal{C}_1 \text{ and } \mathcal{D}_3+\mathbf{v}\subset\mathcal{D}_2\setminus\mathcal{D}_1.$$

Applying Construction I to the cosets $\mathcal{C}_3+\mathbf{u}$ and $\mathcal{D}_3+\mathbf{v}$ yields a matrix code $(\mathcal{C}_3+\mathbf{u})\otimes(\mathcal{D}_3+\mathbf{v})$ with Property $(\mathcal{C}_3+\mathbf{u},\mathcal{D}_3+\mathbf{v})$, and hence the Property $(\mathcal{C}_2\setminus\mathcal{C}_1,\mathcal{D}_2\setminus\mathcal{D}_1)$. Furthermore, the size of this code is $2^{(k_2-1)(l_2-1)}$ and is significantly larger than the straightforward construction from (5).

B. Matrix Codes with Restricted Column and Row Weights

In this section, we apply Construction IA to obtain matrix codes with the additional property of bounded row and column weights. The motivation for studying such matrix codes arises from the application to coded modulation for power line communication channel. Consider a codeword $\mathbf{N}$ of a matrix code. Each row of the matrix corresponds to transmission over a particular frequency slot, while each column of the matrix corresponds to a discrete time instance. Transmision occurs at the frequency and time slots corresponding to a one in the matrix. The effect of the different types of noises in the powerline channel can be described briefly as follows. A narrowband noise turns an entire row of $\mathbf{N}$ to ones, an impulse noise turns an entire column of $\mathbf{N}$ to ones, a channel fade event turns an entire row of $\mathbf{N}$ to zeros, and a background noise flips an entry of $\mathbf{N}$. We refer to [10] for an expanded description of the types of noise that are present in the power line channel.

If any row of the matrix is an all-one vector then this row is not distinguishable from an all-one row introduced by the presence of narrowband noise. Similarly, an all-one column is not distinguishable from impulse noise. Additionally, the use of multi-tone frequency shift keying is adopted with the understanding that the energy is concentrated on a small fraction of the available frequencies (see [8]). Thus, it is desired that every row and every column of the matrix contain at least a single one, but it should not be an all-one vector. This requires the use of codes whose codewords are matrices with bounded column and row weights.

We use the following lemma that was crucial in proving the so-called low symbol weight property (see [11, Proposition 1]) for q-ary affine codes.

Lemma 4.1. Let $\mathcal{C}$ be binary linear $[n,k,d]$ code such that $\langle\mathbf{j}_n\rangle\subset\mathcal{C}$. Then the codewords in $\mathcal{C}\setminus\langle\mathbf{j}_n\rangle$ have Hamming weight bounded between d and $n-d$.

First, we illustrate via an example that the code obtained by straightforward expurgation does not satisfy the systematic property.

Example 4.1. Let $\mathcal{C}=\mathcal{D}$ be the binary linear $[4,3,2]$ code consisting of all even weight codewords. Observe that $\mathcal{C}\setminus\langle\mathbf{j}_4\rangle$ consists of six codewords of weight two and we are interested in constructing a (4×4)-matrix code whose matrices have row weight two and column weight two.

A naive approach is to look at the (3×3) information matrix and require all columns and rows to not belong to $\{\mathbf{0}_3,\mathbf{j}_3\}$. This approach fails as illustrated by the example codeword, $\begin{pmatrix}\mathbf{I}_3 & \mathbf{j}_3^T\\ \mathbf{j}_3 & 1\end{pmatrix}$ which contains an all-one row even though each of the component codewords in the first three rows and columns have weight exactly two.

On the other hand, consider the binary linear $[4,2,2]$ code $\mathcal{C}_3=\{\mathbf{0}_4,\mathbf{j}_4,(1,0,1,0),(0,1,0,1)\}$ and let $\mathbf{u}=(0,0,1,1)$. Then $(\mathcal{C}_3+\mathbf{u})\otimes(\mathcal{C}_3+\mathbf{u})$ yields a (4×4)-matrix code whose matrices have row weight two and column weight two. Furthermore, it is systematic of dimension four.

On the other hand, it can be obtained via computer search that there are exactly 90 matrices in $\mathcal{C}\otimes\mathcal{C}$ that have constant row weight two and constant column weight two. An exhaustive computer search shows that there do not exist five coordinates where a subset of these 90 matrices is systematic.

We proceed with the construction of matrix codes with restricted row and column weights. Let $\mathcal{C}$, $\mathcal{D}$ be binary linear $[n,k,d_{\mathcal{C}}]$, and $[m,l,d_{\mathcal{D}}]$ codes respectively. Suppose $\langle\mathbf{j}_n\rangle\subset\mathcal{C}$, and $\langle\mathbf{j}_m\rangle\subset\mathcal{D}$. Direct application of Construction IA yields a systematic binary $(m\times n)$-matrix code of dimension $(k-1)(l-1)$ whose matrices have

(i) row weight bounded between $d_{\mathcal{C}}$ and $n-d_{\mathcal{C}}$,
(ii) column weight bounded between $d_{\mathcal{D}}$ and $m-d_{\mathcal{D}}$.

In Example 4.1 we showed that this construction gives more desirable results and why naive methods of constructions do not work. Because of the narrowband and impulse noise present in the power line channel, we want codes with restricted column and row weights. The following proposition gives the condition under which the noises can be corrected.

Proposition 4.1. Let $\mathcal{C}$, $\mathcal{D}$ be binary linear $[n,k,d_{\mathcal{C}}]$, and $[m,l,d_{\mathcal{D}}]$ codes respectively. Suppose $\langle\mathbf{j}_n\rangle\subset\mathcal{C}$, and $\langle\mathbf{j}_m\rangle\subset\mathcal{D}$. Then $(\mathcal{C}\setminus\langle\mathbf{j}_n\rangle)\otimes(\mathcal{D}\setminus\langle\mathbf{j}_m\rangle)$ obtained using Construction IA yields a systematic binary $(m\times n)$-matrix code of dimension $(k-1)(l-1)$ whose matrices have

(i) row weight bounded between $d_{\mathcal{C}}$ and $n-d_{\mathcal{C}}$,
(ii) column weight bounded between $d_{\mathcal{D}}$ and $m-d_{\mathcal{D}}$.

Furthermore, $(\mathcal{C}\setminus\langle\mathbf{j}_n\rangle)\otimes(\mathcal{D}\setminus\langle\mathbf{j}_m\rangle)$ is a subcode of $\mathcal{C}\otimes\mathcal{D}$, and hence, is able to correct $e_{\sf NBD}$ narrowband errors and $e_{\sf IMP}$ impulse noise errors, provided

$$e_{\sf IMP}<d_{\mathcal{C}},\ \text{and } e_{\sf NBD}<d_{\mathcal{D}}.$$

5. Irregular Product of Affine Codes

The power line channel is known to be frequency selective (see [10]), i.e., the noise in different frequency slots are of different intensities. Thus, it is of interest to provide constructions of codes that can provide different levels of error correction over different frequencies. Such codes can be constructed as product codes where the rows of the matrix correspond to different row codes. Such codes have been studied earlier as "Generalized Concatenated Codes" or "Multilevel Concatenated Codes" (see Zyablov *et al.* [5] and Dumer [12]). The row codes, which correspond to the row encoding, in these constructions are defined over an extension field of the field of the column code. As a result, although the resulting matrix code is linear over the smaller field, the rows do not in general belong to the row code. This makes it difficult to extend the construction to product of affine codes.

Instead, we consider the case where the component codes for each row and column are different and they are defined over the binary field $\mathbb{F}_2$. Such product codes were termed *irregular product codes* and were studied by Alipour *et al.* [7]. Specifically, they demonstrated the following proposition. Denote the set of integers $\{1, 2, \ldots, n\}$ by $[n]$ for a positive integer n.

Proposition 5.1 (Alipour *et al.* [7])**.** Let $\mathcal{C}_i$ be linear codes of length n and dimension k_i for $i \in [m]$ and $\mathcal{D}_j$ be linear codes of length n and dimension l_j for $j \in [m]$. Suppose that $k_1 \le k_2 \le \cdots \le k_m$ and $l_1 \le l_2 \le \cdots \le l_n$. Then there exists a linear $(m \times n)$-matrix code of dimension K, where

$$K \le \sum_{j=1}^{n} \sum_{i=l_{j-1}+1}^{l_j} \max\{k_i - j + 1, 0\}, \text{ where } l_0 = 0, \quad (6)$$

and every codeword $\mathbf{N}$ satisfies the properties that

(i) the i-th row of $\mathbf{N}$ belongs to $\mathcal{C}_i$ for $i \in [m]$, and
(ii) the j-th column of $\mathbf{N}$ belongs to $\mathcal{D}_j$ for $j \in [n]$.

Furthermore, if $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_m$ and $\mathcal{D}_1 \subseteq \mathcal{D}_2 \subseteq \cdots \subseteq \mathcal{D}_n$, we achieve equality in (6).

We apply Construction I directly to Proposition 5.1 to obtain an irregular product of affine codes.

Proposition 5.2. In addition to the conditions of Prop. 5.1, let $\mathbf{j}_n \in C_i$ for $i \in [m]$ and $\mathbf{j}_m \in D_j$ for $j \in [n]$. Furthermore, suppose there exist linear codes $\mathcal{C}$ and $\mathcal{D}$ such that $\bigcup_{i=1}^m \mathcal{C}_i \subset \mathcal{C}$ and $\bigcup_{i=1}^m \mathcal{D}_i \subset \mathcal{D}$, respectively. Let $\mathbf{u} = (\mathbf{0}_{k_m}, \mathbf{a}) \in \mathcal{C} \setminus \bigcup_{i=1}^m \mathcal{C}_i$ and $\mathbf{v} = (\mathbf{0}_{l_n}, \mathbf{b}) \in \mathcal{D} \setminus \bigcup_{j=1}^n \mathcal{D}_j$.

Then there exists an affine $(m \times n)$-matrix code of size 2^K bounded by (6) and every codeword $\mathbf{N}$ in the code satisfies the properties that

(i) the i-th row of $\mathbf{N}$ belongs to $\mathcal{C}_i + \mathbf{u}$ for $i \in [m]$, and
(ii) the j-th column of $\mathbf{N}$ belongs to $\mathcal{D}_j + \mathbf{v}$ for $j \in [n]$.

Furthermore, if $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_m$ and $\mathcal{D}_1 \subseteq \mathcal{D}_2 \subseteq \cdots \subseteq \mathcal{D}_n$, we achieve equality in (6). Additionally, the weight of every row of any codeword is bounded between $d_{\mathcal{C}}$ and $n - d_{\mathcal{C}}$, and of every column between $d_{\mathcal{D}}$ and $m - d_{\mathcal{D}}$, where $d_{\mathcal{C}}$ and $d_{\mathcal{D}}$ are the minimum distances of $\mathcal{C}$ and $\mathcal{D}$ respectively.

6. CONCLUSION

We provide new constructions of systematic nonlinear product codes that are obtained by taking product of affine codes. The constructions have the property that every row and every column belongs to the row code and column code, respectively. Subsequently, we show that it is possible to construct matrix codes with restricted column and row weights. Although the primary motivation for studying such matrix codes is for coded modulation over power line channel, the constructions can potentially be adapted to address other problems where such codes are desired such as codes for memristor arrays and two-dimensional weight-constrained codes [13], [14].

ACKNOWLEDGEMENT

This work was done while H. M. Kiah was a graduate student at Nanyang Technological University.

The authors thank the anonymous reviewers and the TPC member for their constructive comments.

REFERENCES

[1] P. Elias, "Error-free coding," *Transactions of the IRE Professional Group on Information Theory*, vol. 4, no. 4, pp. 29–37, 1954.
[2] G. Forney Jr, "Concatenated codes. research monograph no. 37," 1966.
[3] A. Barg and G. Zemor, "List decoding of product codes by the minsum algorithm," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2011, pp. 1273–1277.
[4] O. Amrani, "Nonlinear codes: The product construction," *IEEE Trans. Commun.*, vol. 55, no. 10, pp. 1845–1851, October 2007.
[5] V. Zyablov, S. Shavgulidze, and M. Bossert, "An introduction to generalized concatenated codes," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 609–622, 1999.
[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland Publishing Co., 1977.
[7] M. Alipour, O. Etesami, G. Maatouk, and A. Shokrollahi, "Irregular product codes," in *IEEE Information Theory Workshop (ITW) 2012*, 2012, pp. 197–201.
[8] Y. M. Chee, H. Kiah, and P. Purkayastha, "Matrix codes and multitone frequency shift keying for power line communications," in *Proc. IEEE Intl. Symp. Inform. Theory*, 2013, pp. 2870–2874.
[9] A. J. H. Vinck, "Coded modulation for power line communications," *AEÜ - Int J. Electron. Commun.*, vol. 54, no. 1, pp. 45–49, 2000.
[10] M. Ardakani, G. Colavolpe, K. Dostert, H. C. Ferreira, D. Fertonani, T. G. Swart, A. M. Tonello, D. Umehara, and A. J. H. Vinck, "Digital transmission techniques," in *Power Line Commun. - Theory and Applicat. for Narrowband and Broadband Commun. over Power Lines*, H. Ferreira, L. Lampe, J. Newbury, and T. Swart, Eds. John Wiley & Sons, 2010, ch. 5, pp. 195–310.
[11] D. J. J. Versfeld, A. J. H. Vinck, J. N. Ridley, and H. C. Ferreira, "Constructing coset codes with optimal same-symbol weight for detecting narrowband interference in M-FSK systems," *IEEE Trans. Inform. Theory*, vol. 56, no. 12, pp. 6347–6353, 2010.
[12] I. Dumer, "Concatenated codes and their multilevel generalizations," *Handbook of coding theory*, vol. 2, pp. 1911–1988, 1998.
[13] E. Ordentlich and R. Roth, "Low complexity two-dimensional weight-constrained codes," in *IEEE International Symposium on Information Theory Proceedings (ISIT) 2011*, 2011, pp. 149–153.
[14] ——, "Two-dimensional weight-constrained codes through enumeration bounds," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1292–1301, 2000.