Gulf Journal of Mathematics
Vol 3, Issue 2 (2015) 44-48

MATRIX PRODUCT CODES OVER $\mathbb{F}_p$

MOHAMED BOUYE[1*] AND MOHAMED SAÏD[2]

Abstract. We will present in this paper the concept of matrix-product code $[C_1, C_2, \cdots, C_s]A$ where $C_1, C_2, \cdots, C_s$ are linear codes and matrix A has full rank. The purpose of this paper is to give some properties of these codes that will be useful later, the two main points being the existence of a MacWilliams identity (which is one reason the existence of the phenomenon of duality formal) and the structure of the matrix-product code on $\mathbf{Z}_{p^k}$.

1. Introduction

In the coding theory an interesting and important approach is to construct a new codes from known ones. In [1], Blackmore and *all.* introduced the notion of matrix product codes over finite fields for generalize some construction known in the coding theory. For example, the Plotkin's well-known $(u|u+v)$-construction, the ternary $(u+v+w|2u+v|u)$-construction, the $(a+x|b+x|a+b+x)$-construction, and the $(u+v|u-v)$-construction and etc. But the challenge problem is to determine the parameters of the new codes (length, dimension, minimal Hamming distance, $\cdots$,) from the initial codes. To answer this question there are some other articles focusing on the study of decoding and the construction of matrix product codes ([3, 5]) have appeared.

2. Matrix Product Codes

Definition 2.1. Let $C_1, C_2, \cdots, C_s$ be linear codes of length m over $\mathbb{F}_q$ and $A = (a_{ij})$ in $M_{s\times l}(\mathbb{F}_q)$ with $s \leq l$. A matrix product codes C_A associated to $C_1, C_2, \cdots, C_s$ and A is the linear code over $\mathbb{F}_q$ of length ml defined by :

$$C_A = \{(\textstyle\sum_{i=1}^{s} a_{i1}x_i, \sum_{i=1}^{s} a_{i2}x_i, \cdots, a_{il}x_i)|x_i \in C_i\}$$

2.1. **Description of C_A.** If

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \vdots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{pmatrix}$$

Then :

Date: Received: Feb 28, 2015.

* Corresponding author.

2010 *Mathematics Subject Classification.* 94B05, 94B65, 15B33.

Key words and phrases. Error corrcting codes, linear codes, matrix product codes.

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{s1} \\ a_{12} & a_{22} & \cdots & a_{s2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1l} & a_{2l} & \cdots & a_{sl} \end{pmatrix}$$

$$C := [C_1, C_2, \cdots, C_s] = \{(x_1 x_2 \cdots x_s) \in M_{m\times s}(\mathbb{F}_q) | x_i^t \in C_i\}$$

We define :

$$C^t := \{X^t | X \in C\} \text{ and } A^t C^t := \{A^t.Y | Y \in C^t\}$$

Take Z element of the A^tC^t, so $\exists Y \in C^t : Z = A^tY$, $Y \in C^t \Leftrightarrow \exists X \in C; X^t = Y$

on the other hand $X \in C \Leftrightarrow \exists x_i : x_i^t \in C_i$ and $X = (x_1 x_2 \cdots x_s)$ so

$$Z = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{s1} \\ a_{12} & a_{22} & \cdots & a_{s2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1l} & a_{2l} & \cdots & a_{sl} \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_s \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^s a_{i1} x_i \\ \sum_{i=1}^s a_{i2} x_i \\ \vdots \\ \sum_{i=1}^s a_{il} x_i \end{pmatrix}$$

$Z^t = (\sum_{i=1}^s a_{i1}x_i, \sum_{i=1}^s a_{i2}x_i, \cdots, a_{il}x_i) \in C_A$, so $(A^tC^t)^t = C_A$ that means $C.A = C_A$

Example 2.2. Let $C_1 = \{000, 111\}$ and $C_2 = \{000, 011\}$ two linear codes of length $m = 3$ and $s = 2$ and consider the two matrix $A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

$$[C_1C_2] := \{(x_1x_2) | x_i \in C_i\} = \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \}.$$

Then the matrix product codes of C_1 , C_2 and A :

$$C_A = [C_1C_2].A :$$

- $\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \times A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = (000, 000, 000, 000) = \alpha_1$
- $\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \times A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = (000, 011, 000, 011) = \alpha_2$
- $\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} \times A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} = (111, 000, 000, 111) = \alpha_3$
- $\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \times A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = (111, 011, 000, 100) = \alpha_4$
- $$C_A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$$

$$C_B = [C_1 C_2].B:$$

- $\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \times B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = (000, 000, 000, 000) = \alpha_1$
- $\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \times B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} = (000, 011, 011, 000) = \beta_1$
- $\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} \times B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} = (111, 000, 111, 000) = \beta_2$
- $\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \times B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = (111, 011, 000, 100) = \beta_3$
-

$$C_B = \{\alpha_1, \beta_1, \beta_2, \beta_3\}.$$

3. Parameters of Matrix-product code

Proposition 3.1. *Let $G_1, G_2, \cdots, G_s$ be the generator matrix of the code $C_1, C_2, \cdots, C_s$ respectively and $A = (a_{ij}) \in M(\mathbb{F}_q, s \times l)$. Then the generator matrix G of the matrix product code $C = [C_1, C_2, \cdots, C_s]A$ is given by :*

$$G = \begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \vdots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{pmatrix}$$

Proof. Let $c \in C = [C_1, C_2, \cdots, C_s]A$, the matrix-product code C by definition is the set of all matrix product $c = (c_1, c_2, \cdots, c_s)A$ where $c_i \in C_i$, then:

$$c = (c_1, c_2, \cdots, c_s)A = (c_1, c_2, \cdots, c_s) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \vdots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{pmatrix}$$

And the codewords can be viewed as vectors of length ml,

$$c = (\sum_{j=1}^{s} a_{j1}c_j, \sum_{j=1}^{s} a_{j2}c_j, \cdots, \sum_{j=1}^{s} a_{jl}c_j) \in \mathbb{F}_q^{ml} \tag{3.1}$$

or $c_i \in C_i$, then $c_1 = (u_1, u_2, \cdots, u_{k_1}).G_1$, $c_2 = (v_1, v_2, \cdots, v_{k_2}).G_2$, ... , $c_s = (h_1, h_2, \cdots, h_{k_s}).G_s$. If we replaced all c_i in (1) we have:

$$c = (\sum_{j=1}^{s} a_{j1}(u_1, u_2, \cdots, u_{k_j}).G_j, \sum_{j=1}^{s} a_{j2}(u_1, u_2, \cdots, u_{k_j}).G_j, \cdots, \sum_{j=1}^{s} a_{jl}(u_1, u_2, \cdots, u_{k_j}).G_j)$$

We can write this expression in matrix form:

$$c = (u_1, u_2, \cdots, u_{k_1}, v_1, v_2, \cdots, v_{k_2}, \cdots, h_1, h_2, \cdots, h_{k_s}).\begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \vdots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{pmatrix}$$

Therefore, the generator matrix G of the matrix product code C

$$G = \begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \vdots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{pmatrix}$$

□

Proposition 3.2. *Let C_i be a $[m, k_i, d_i]$ linear codes over $\mathbb{F}_q$, $i \in \{1, \cdots, s\}$ and $A = (a_{ij}) \in M(\mathbb{F}_q, s \times l)$. Then the matrix product code $C = [C_1, C_2, \cdots, C_s]A$ is a linear code over $\mathbb{F}_q$ with length lm and dimension.*

$$k < k_1 + k_2 + \cdots + k_s \tag{3.2}$$

If the matrix A has full rank the bound (2) is achieved, so the dimension of the matrix product code $C = [C_1, C_2, \cdots, C_s]A$ is

$$k = k_1 + k_2 + \cdots + k_s \tag{3.3}$$

Proof. Let $A = (a_{ij}) \in M(\mathbb{F}_q, s \times l)$ matrix with $s \leq l$ which has full rank. Any codeword of C is of the form $c = (c_1, c_2, \cdots, c_s)A$. Let us suppose that $(c_1, c_2, \cdots, c_s) \neq [0, 0, \cdots, 0]$ for $i = 1, 2, \cdots, s$ and $c_i \in C_i$. Since A has full rank and $s \leq l$, then rank of A is equal to s, then $c = (c_1, c_2, \cdots, c_s)A \neq [0, 0, \cdots, 0]$. Therefore $\#C = (\#C_1).(\#C_2).\cdots.(\#C_s) = q^{k_1+k_2+\cdots+k_s}$. □

Proposition 3.3. *Let $R_i = (a_{i1}, a_{i2}, \cdots, a_{il})$ denote the i- row of the matrix A for $i = 1, 2, \cdots, s$ and denote by D_i the minimum distance of the code C_{R_i} code generated by $< R_1, \cdots, R_i >$ in $\mathbb{F}_q^l$. In [6] the following lower bound for the minimum distance of the matrix product code C is obtained*

$$d(C) = d = min\{d_1D_1, d_2D_2, \cdots, d_sD_s\} \tag{3.4}$$

where d_i is the minimum distance of C_i

Proof. Demonstration of this proposition is given in [6] □

Lemma 3.4. *If $C_1, C_2, \cdots, C_s$ are nested codes $C_1 \supset C_2 \supset \cdots \supset C_s$ the bound in (4) is sharp* [3]

Proof. The proof of this lemma is given in [3] □

Example 3.5. If C_1, C_2 are two linear codes over $\mathbb{F}_2$, with generator matrices respectively G_1, G_2 and $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then the matrix-product code

$$C = [C_1, C_2].A = \{(c_1|c_1 + c_2) : c_1 \in C_1, c_2 \in C_2\}$$

and the generator matrix G of the matrix product code C is $G = \begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$

Example 3.6. Consider the linear codes C_1, C_2, C_3 of length 3 over $\mathbb{F}_3$, with generator matrices respectively:

$$G_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}, G_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix}, G_3 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \text{ and } A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Then the matrix-product code $C = [C_1, C_2, C_3].A$ is given by its matrix generator

$$G = \begin{pmatrix} G_1 & G_1 & G_1 \\ 0 & 2G_2 & G_2 \\ 0 & 0 & G_3 \end{pmatrix}$$

The parameters of these codes are $[3, 3, 1], [3, 2, 2]$ and $[3, 1, 3]$, respectively, and the codes are nested, the matrix-product code $C = [C_1, C_2, C_3].A$ is a $[9, 6, 3]$ linear code.

As conclusion of this work, we aim to study the matrix-product code and give some Bound on the parameters of the matrix-product code where the codes $C_1, \cdots, C_s$ are linear and the matrix A has full rank.

References

1. T. Blackmore and G.H. Norton; *Matrix-product codes over* $\mathbb{F}_q$, Appl. Algebra Engrg. Comm. Comput. (2001), **1** 477-500.
2. Y. Fan; S. Ling; H. Liu; *Matrix product codes over finite commutative Frobenius rings*, (to appear in Des Codes Cryptogr). DOI: 10.1007/s10623-012-9726-y
3. F. Hernando; K. Lally and D. Ruano; *Construction and decoding of matrix-product codes from nested codes*, Appl. Algebra Engrg. Comm. Comput. (2009), **20** 497-507.
4. F. Hernando and D. Ruano; *New linear codes from matrix-product codes with polynomial units*, Appl. Algebra Engrg. Comm. Comput. (2010), **4** 363-367.
5. M. B. Ould Medeni and S. Mamoun; *Construction and bound on the performance of matrix-product codes*, Appl Math Sci (Ruse), (2011), **5** 929-934.
6. F. Özbudak and H. Stichtenoth; *Note on Niederreiter-Xing's propagation rule for linear codes*, Appl. Algebra Engrg. Comm. Comput. (2002), **13** no. 1, 53-56.

[1] Department of Mathematics, Faculty of Sciences, King Khaled University, PO Box 9004, Abha, Saudi Arabia.

E-mail address: medeni.doc@gmail.com

[2] Laboratoire of Algebra, Cryptography, Algebraic Geometry and Applications., Mathematic and Informatics Departement, University Cheikh Anta Diop-Senegal (UCAD).

E-mail address: ouldsaid@yahoo.fr