Tensor Product And Linear Error Block Codes

Soukaina Belabssir and Nadir Sahlal

***Abstract*—The codes generated using tensor product and called tensor codes have properties and composition similar to Linear Error Block codes (LEB codes). In this paper we study in depth the construction of new LEB codes using tensor product (TP). We also show that the TP code formed by two LEB codes is also an LEB code. We prove that the TP of two Hamming codes is not a Hamming code with minimum distance 3, besides, it's a non- perfect LEB code. We show that the TP code formed by two π-cyclic codes (resp. simplex LEB codes) is a π-cyclic code (resp. simplex LEB code).**

***Index Terms*—Linear Error-Block codes, Tensor product, Hamming codes.**

I. Introduction

LINEAR error-block (LEB) codes were introduced by Feng, Xu and Hickernell [1] in 2006 as a natural generalization of linear error correction codes. They summarized that these codes have mixed-level orthogonal arrays and can be used in experimental design and high-dimensional numerical integration. Like their classical counterpart, these codes may also be used in cryptography. Dariti and Souidi [2], in their paper, proved that using LEB codes in public key cryptography can reduce the size of the used keys while keeping the same level of security as in the classical case. The same authors in [3] showed the practicality of using LEB codes in steganography as it can help to increase the embedding capacity.

As a generalization of the classical case, we extend the notion of tensor product into the LEB codes case. Tensor codes were first introduced by J.K Wolf in [4] and were later generalized in [5], they are the result of the tensor product of the parity check of two constituent codes. These particular codes have found application in digital storage systems and digital recording systems [6], [7].

TP codes have many particular properties derived from the constituent codes, but the main motivation behind our work is that their structure reminds us of LEB codes. This pushed us to formally study the relation between LEB codes and tensor codes. We verify if tensor product codes are themselves LEB. We try to construct new LEB codes based on the tensor product of two constituent LEB codes and see if some of the properties are kept in place.

This paper is organized as follows: In Section 2, we present the preliminaries and introduce all the definitions that we will need for the rest. In Section 3, we verify if TP codes are also LEB codes. In Section 4, we give a construction of new LEB codes based on the tensor product of different constituent codes. In Section 5, we study the properties of the LEB constituted by TP of Hamming LEB codes. The Tensor product of simplex and cyclic LEB codes is studied in Section 6. A perspective of this work is discussed in Section 7.

Manuscript received September 18, 2020; revised November 11, 2020.

Soukaina Belabssir, and Nadir Sahlal are PHD students in Mohammed V University in Rabat. Faculty of sciences, BP 1014 Rabat Morocco. Laboratory of Mathematics, Computer Science, Applications and Information Security with the respective emails: soukainabelabssir@gmail.com, and SAHLLAL.NADIR@gmail.com

II. Preliminaries

A partition π of a positive integer n, is given by $n = n_1 + n_2 + \ldots + n_s$, where $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$, and s is an integer ≥ 1, and is denoted by $\pi = [n_1][n_2]\ldots[n_s]$. Furthermore, if $n = \sum_{i=1}^{s} n_i = l_1 m_1 + l_2 m_2 + \ldots + l_r m_r$ where $m_1 > m_2 > \ldots > m_r \geq 1$, then π will be rewritten as $\pi = [m_1]^{l_1}[m_2]^{l_2}\ldots[m_r]^{l_r}$.

Let $\pi = [n_1]\ldots[n_s]$ $(s \geq 1)$ be a partition of an integer n, set $V_i = \mathbb{F}_q^{n_i} (1 \leq i \leq s)$, and

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_s = \mathbb{F}_q^n. \tag{1}$$

Then each vector in V can be written uniquely as $v = (v_1, v_2, \ldots, v_s)$, where v_i is in V_i (for $1 \leq i \leq s$). For any $u = (u_1, u_2, \ldots, u_s)$ and $v = (v_1, v_2, \ldots, v_s)$ in V, the π-weight $w_\pi(u)$ and respectively the π-distance $d_\pi(u,v)$ of u and v are defined by:

$$w_\pi(u) = \#\{i / 1 \leq i \leq s,\ 0 \neq u_i \in V_i\} \tag{2}$$

and

$$d_\pi(u,v) = w_\pi(u-v) = \#\{i / 1 \leq i \leq s,\ u_i \neq v_i\}. \tag{3}$$

An $\mathbb{F}_q$-linear subspace C of V is called an $[n,k,d]_q$ linear error-block code over $\mathbb{F}_q$ of type π, where $k = dim_{\mathbb{F}_q}$ and $d = d_\pi$ is the minimum π-distance of C, which is defined as:

$$d = \min\{d_\pi(c,c') / c, c' \in C, c \neq c'\} \tag{4}$$

$$d = \min\{w_\pi(c) / c \in C,\ c \neq 0\}. \tag{5}$$

A classical linear error-correcting code is a linear error-block code of type $\pi = [1]^n$.

An LEB code is completely defined by a generator matrix or a parity check matrix.

As in the classical case, the minimum π-distance of a linear error-block code is straightforwardly determined using a parity-check matrix as follows:

Proposition 2.1 ([1]): Let $H = [H_1, H_2, \ldots, H_s]$ be a parity-check matrix for an $[n,k,d_\pi]$ code C over $\mathbb{F}_q$ of type $\pi = [n_1][n_2]\ldots[n_s]$. Then $d_\pi(C) = d$ if and only if

- The union of columns of any $d-1$ blocks of H are $\mathbb{F}_q$-linearly independent;
- There exist d_π blocks of H of which the columns are linearly dependent.

The Hamming and singleton Bounds for LEB codes are given by Feng *et al.* [1], as follows:

Theorem 2.2: [1] Let C be an $[n,k,d_\pi]_q$ LEB code over $\mathbb{F}_q$ of type $\pi = [n_1][n_2]\ldots[n_s]$ where $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$. Then (the Hamming bound):

$$q^{n-k} \geq \begin{cases} b_\pi(l) & \text{if } d_\pi = 2l+1, \\ b'_\pi(l) & \text{if } d_\pi = 2l \geq 2. \end{cases} \tag{6}$$

where

$$b_\pi(l) = 1 + \sum_{\alpha=1}^{l} \sum_{1\le i_1\le i_2\le \ldots\le i_\alpha\le s} (q^{n_{i_1}}-1)(q^{n_{i_2}}-1)\ldots(q^{n_{i_\alpha}}-1) \quad (7)$$

and

$$b'_\pi(l) = q^{n_1} \left(1 + \sum_{\alpha=1}^{l-1} \sum_{2\le i_1\le i_2\le \ldots\le i_\alpha\le s} (q^{n_{i_1}}-1)(q^{n_{i_2}}-1)\ldots(q^{n_{i_\alpha}}-1)\right) \quad (8)$$

and (the Singleton bound) :

$$n-k \ge n_1+n_2+\ldots+n_{d-1}. \quad (9)$$

Definition 2.3: An $[n,k,d_\pi]_q$ LEB code of type π is said to be perfect if it attains the Hamming bound and is said to be MDS if it attains the Singleton bound.
Thus, perfect LEB codes verify the following equations :

$$q^{n-k} = \begin{cases} b_\pi(l) & \text{if } d_\pi = 2l+1, \\ b'_\pi(l) & \text{if } d_\pi = 2l \ge 2. \end{cases} \quad (10)$$

and MDS LEB codes verify the equation

$$n-k = n_1+n_2+\ldots+n_{d-1}. \quad (11)$$

The binary Hamming single-error-correcting codes are an important family of codes which were invented by Richard Hamming in 1950 [8] to be codes of length $n = 2^r-1$ $(r \ge 2)$ and have parity check matrix H whose columns consist of all nonzero binary vectors of length r, each used once, these are $[n = 2r-1, k = 2r-1-r, d = 3]$ codes.

Hamming LEB codes of type $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ with $r = \lambda m \ge 2$ were introduced by Belabssir. *et al.* in [9]. The authors defined $\pi - ham(r,q)$ codes to be codes of type $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ and whose parity check matrix H is an $r \times n$ matrix for which the union of columns of any two blocks is linearly independent. they also chowed that the $\pi - ham(r,q)$ codes are perfect and defined its parity check matrix as follows:

$$H_2 = \left(\begin{array}{c|c|c|c|c} I_m & E_1 & \ldots\ldots & E_{q^m-1} & 0_m \\ 0_{m-1} & I_m & \ldots\ldots & I_m & I_m \end{array} \right) \quad (12)$$

and for $\lambda \ge 3$

$$H_\lambda = \left(\begin{array}{c|c|c|c|c} I_m & A_1 & \ldots\ldots & A_{q^m-1} & A_0 \\ 0_{m(\lambda-1)} & H_{\lambda-1} & \ldots\ldots & H_{\lambda-1} & H_{\lambda-1} \end{array} \right) \quad (13)$$

where

- I_m is the identity matrix of size m.
- $E_1, \ldots, E_{q^m-1}$ are the extensions of non-zero vectors in $\mathbb{F}_q^m$.
- For all $1 \le i \le q^m-1$, $A_i = (\underbrace{E_i, \ldots, E_i}_{s_{\lambda-1} \text{ time}})$ where $s_{\lambda-1} = \frac{q^{(\lambda-1)m}-1}{q^m-1}$.
- $A_0 = (\underbrace{0_m, \ldots, 0_m}_{s_{\lambda-1} \text{ time}})$ where 0_m is the $m \times m$ null matrix.

Denote that a block extension of $v \in \mathbb{F}_q^l$ is an $l \times l$ matrix M defined as follows

- The columns of M are linearly independent.
- The sum of all columns of M is equal to v^T (transpose of v).

In [10], the authors proved that the dual code (π-Ham(r,q))$^\perp$ is a simplex code and the common π-weight of its non-zero codewords is $w_\lambda = 2^{r-m} = 2^{(\lambda-1)m}$ where $\lambda = \frac{r}{m}$ is an integer ≥ 1.

A. Tensor Product codes

In this part, we introduce tensor product codes and some of their properties. To start with, we define what is the tensor product between two matrices.

Definition 2.4: Let $A = (a_{ij})$ be an m-by-n matrix and let $B = (b_{ij})$ be a p-by-q matrix. The tensor product of A and B is defined as

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{bmatrix} \quad (14)$$

Definition 2.5: The Tensor Product (TP) code is formed by combining two constituent codes in a particular way. The name tensor product comes from the fact that the parity check matrix of the new code is formed by taking the tensor product of the parity-check matrices or generator matrices of the two simpler codes [4].

III. Tensor Product of two linear block codes

In this section, we prove that the tensor product of any two codes is not an LEB codes.

Theorem 3.1: The tensor product code of two Hamming codes is not a Hamming code.

Proof: Let C_1 and C_2 be respectively an $[n_1 = 2^m - 1, 2^m-1-m, 3]$ and an $[n_2 = 2^l-1, 2^l-1-l, 3]$ (m and l are integers bigger than 2) Hamming codes and C the TP codes resulting from the tensor product of C_1 and C_2.

To be also a Hamming code, C needs to be written as $[N = 2^M-1, 2^M-1-M, 3]$ with M a positive integer bigger than 2.

C is the TP code generated using C_1 and C_2. Then by definition

$$\begin{aligned} N &= n_1 \times n_2 \\ 2^M-1 &= (2^m-1)\times(2^l-1) \\ 2^M-1 &= 2^{m+l}-2^m-2^l+1 \\ 2^M &= 2^{m+l}-2^m-2^l+2 \\ 2^{M-1} &= 2^{m+l-1}-2^{m-1}-2^{l-1}+1 \end{aligned}$$

the last equality is only possible if the integers m, l and M are equal to 1 which is absurd as we supposed that they are bigger or equal to 2. ■

There is an interesting property that is transmitted to the TP code formed by two Hamming codes, which is the columns of the check matrix of the generated codes are two by two linearly independent.

Remark 3.2: The minimal distance of the TP code formed by two Hamming codes is equal to 3.

Theorem 3.3: The TP code of minimum distance $d = 3,4$ formed from two linear block codes is not a linear error-block code.

Proof: We give the proof for the case $d = 3$ and the case $d = 4$ is done in the same way with some minor modifications. Let C_1 be an $[n_1,k_1,3]$ code of parity-check matrix H_1 and C_2 be an $[n_2,k_2,3]$ code of parity check matrix H_2. The parity-check matrix of the TP code C formed from these two codes is of size $r \times n$ where $r = (n_1-k_1)\times(n_2-k_2)$ and $n = n_1 \times n_2$. Set $r_1 = n_1-k_1$ and $r_2 = n_2-k_2$. If C is an LEB code with minimum $\pi-$distance $d = 3 = 2\times 1+1$

then $\pi = [n_1]^{n_2}$ and it satisfies the Hamming bounds defined as follows:

$$q^r \geq 1 + \sum_{i=1}^{s} (q^{n_i} - 1). \tag{15}$$

We have $q^r = q^{r_1 r_2}$ and $1 + \sum_{i=1}^{s}(q^{n_i}-1) = 1 + n_2(q^{n_1}-1)$. Since $n = n_1 n_2$, then $1 + n_2(q^{n_1}-1) >> q^{r_1 r_2}$. Therefore $1 + \sum_{i=1}^{s}(q^{n_i}-1) > q^r$ and this is a contradiction with (15). Thus C is not an LEB code. ■

Example 3.4: The TP code formed from two binary Hamming codes of minimum distance $d = 3$ is not a linear error-block code. In fact, let C_1 be a Hamming $[n_1, k_1]$ code and C_2 be a Hamming $[n_2, k_2]$ code. Set $r_1 = n_1 - k_1$ and $r_2 = n_2 - k_2$. If C is an LEB code then $\pi = [n_1]^{n_2}$ and it reaches the Hamming bounds defined as follows:

$$2^r = 1 + \sum_{i=1}^{s} (2^{n_i} - 1). \tag{16}$$

We have $2^r - (1 + \sum_{i=1}^{s}(2^{n_i}-1)) = 2^{r_1 r_2} - 1 - n_2(2^{n_1}-1)$.

Since C_2 is a Hamming code then $2^{r_2} - 1 = n_2$. Therefore,

$$\begin{aligned} &2^r - (1 + \textstyle\sum_{i=1}^{s}(2^{n_i}-1)) \\ &= 2^{r_1 r_2} - 1 - (2^{r_2}-1)(2^{n_1}-1) \\ &= 2^{r_2}(-2^{r_1(r_2-1)}(2^{n_1 - r_2 - r_1(r_2-r_1)}(2^{r_2}-1)+1)+1) - 2. \end{aligned}$$

Obviously

$-2^{r_1(r_2-1)}[2^{n_1-r_2-r_1(r_2-r_1)}(2^{r_2}-1)+1]+1 < 0$, thus $2^r - (1 + \sum_{i=1}^{s}(2^{n_i}-1)) < 0$ and this is a contradiction with (16). Finally, C is not an LEB code.

Corollary 3.5: In general the TP code formed using two classical codes is not an LEB code.

IV. Construction of LEB codes using tensor Product by parity check-matrices

We have shown that the tensor product of two classical error correcting codes does not generate an LEB codes despite the similarity of the structures.

In this section, we are motivated to explore the other ways we can use the tensor product to produce LEB. To do, we explore two constructions which we will explain in more details.

A. The tensor product of two LEB codes

Our first construction is inspired from the construction of tensor codes in the classical case. It is the tensor product of two LEB codes. From different examples and some theoretical proof, we gathered that this product can produce another LEB code.

In general, we denote two LEB codes C_1 defined as $[n_1, k_1, d_1]$ and C_2 defined with $[n_2, k_2, d_2]$ with partitions $\pi_1 = [m_1]^{s_1}$ and $\pi_2 = [m_2]^{s_2}$ respectively.

We use the Hamming LEB code to illustrate the different cases, but we will always give the corresponding analogy to the general case.

As a reminder, here is the Hamming LEB code (binary of length $n_1 = 10$, dimension $k = 6$ and type $\pi = [2]^5$) control matrix:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{17}$$

When we do the tensor product of $H \otimes H$ the resulting matrix is a 16 by 100 matrix.

$$H \otimes H = \begin{bmatrix} H & 0 & 0 & 0 & 0 & H & H & 0 & H & H \\ 0 & H & 0 & 0 & H & 0 & H & H & 0 & H \\ 0 & 0 & 0 & H & 0 & H & 0 & H & 0 & H \\ 0 & 0 & H & 0 & H & 0 & H & 0 & H & 0 \end{bmatrix} \tag{18}$$

After doing the tensor product comes the choice of the partition which is one of the most important factors in a LEB code. There are two natural choices that seem worthy of trial.

(we have $n_1 = n_2 = 10,\ k_1 = k_2 = 6, s_1 = s_2 = 5$)

a) $\pi = [2]^{50}$ *($[m_1]^{s_1.m_2.s_2} = [m_1]^{s_1.n_2}$):* This choice does actually generate an LEB code, but it defies the purpose of the tensor construction. Also, we do not make use of the structure of the constituent codes.

b) $\pi = [10]^{10}$ *($[m_1.s_1]^{m_2.s_2} = [n_1]^{n_2}$):* The last choice is in our opinion the most suitable. We get 10 blocks of length 10 each, but also every underlying block keeps the structure of one of the constructing codes (that we hope to use to simplify the decoding procedure of the lengthy code). By definition it is still an LEB code.

In the following corollary, we prove the LEB structure of this tensor product.

Corollary 4.1: The TP code of two LEB codes is also an LEB code.

Proof: To prove that the TP code C of two $[n,k,d]$ LEB codes C_1 and C_2 is an LEB code, we prove that C is a subspace of $\mathbb{F}_2^n$. Take c_1 and c_2 two codewords of C and α and λ two elements of $\mathbb{F}_2$. Since $c_i^t.H = 0$ for $i = 1,2$, then $(\alpha c_1 + \beta c_2)^t.H = 0$ and $\alpha c_1 + \beta c_2$ is a codeword of C. Since $(C,+)$ is an abelian group then C is a subspace of $\mathbb{F}_2^n$. ■

B. Classical code Tensor LEB

Unlike the previous construction this is more of an hybrid construction between LEB codes and classical codes. We will try both sides to see the resulting code if it is in fact an LEB code and what properties they hold.

For the construction we use the $[7,4,3]$ Hamming code and the $[10,6]$ LEB Hamming code (a code of H parity check matrix shown in (17)).

The parity check matrix of the Hamming code $[7,4,3]$

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{19}$$

The tensor product of H and A, will also give a 12 by 70 check matrix of an LEB code

$$H \otimes A = \begin{bmatrix} A & 0 & 0 & 0 & 0 & A & A & 0 & A & A \\ 0 & A & 0 & 0 & A & 0 & A & A & 0 & A \\ 0 & 0 & 0 & A & 0 & A & 0 & A & 0 & A \\ 0 & 0 & A & 0 & A & 0 & A & 0 & A & 0 \end{bmatrix} \tag{20}$$

We come back again to the choice of the partition π and the most suitable choice is $\pi = [7]^{10}$.

V. Tensor product code of LEB Hamming codes

In this section, we study the structure of the code generated from the tensor product of two LEB hamming codes.

Theorem 5.1: Let C_1 be an $[n_1,k_1,3]$ $\pi-Ham(r_1,q)$ code of type $\pi=[m_1]^{s_1}$ and C_2 be an $[n_2,k_2,3]$ $\pi-Ham(r_2,q)$ code of type $\pi=[m_2]^{s_2}$. The TP code C of C_1 and C_2 is an LEB code of type $\pi=[n_1]^{n_2}$. Besides, C is a non-perfect code of minimum π-distance 3.

Proof: Let C_1 and C_2 two LEB Hamming codes satisfying conditions of Theorem 5.1. Viewing the TP code C of C_1 and C_2 as an LEB code we get two constructions:

1) Code of type $\pi=[n_1]^{n_2}$.
2) Code of type $\pi=[m_1]^{n_2s_1}$.

Here we are interested by the first construction (i.e. code of type $\pi=[n_1]^{n_2}$). If C is an LEB code, then C verify the Hamming bound that is $q^r\geq 1+\sum_{i=1}^{n_2s_1}(q^{m_1}-1)$.

We have

$$\begin{aligned}1+\textstyle\sum_{i=1}^{n_2s_1}(q^{n_i}-1) &= 1+n_2s_1(q^{m_1}-1)\\ &= 1+s_1m_2\tfrac{q^{r_2}-1}{q^{m_2}-1}(q^{m_1}-1)\\ &= \tfrac{(q^{m_2}-1)+m_2(q^{r_2}-1)(q^{r_1}-1)}{q^{m_2}-1}\end{aligned}$$

and

$$\begin{aligned}q^r &= q^{r_1r_2}\\ &= [1+\tfrac{q^{r_2}-1}{q^{m_2}-1}(q^{m_2}-1)]^{r_1}\\ &= [\tfrac{(q^{m_2}-1)+(q^{r_2}-1)(q^{m_2}-1)}{q^{m_2}-1}]^{r_1}\end{aligned}$$

Therefore $q^r>1+\sum_{i=1}^{n_2}(q^{n_i}-1)$. Thus C is a non perfect LEB code of $d_\pi=3$ and the columns of it's parity check-matrix are pairwise independent. ■

Theorem 5.2: The TP code formed of two perfect LEB codes is in general not a perfect LEB code.

Proof: The same idea of proof of the Theorem 5.1. ■

VI. Construction of TP codes of LEB codes using generators matrices

We show in this section that the tensor product of two cyclic LEB codes is a cyclic LEB code and the tensor product of two simplex LEB codes is also a simplex LEB code.

Cyclic LEB codes were introduced by Dariti *et al.* in [2], and generalized by Belabssir *et al.* in [10]. Hereafter we recall the definition of π-cyclic codes proposed in [10] and we give a short over view about their properties.

Definition 6.1: [10] An $[n,k,d]$ code C of type $\pi=[m]^s$ is π-cyclic if for each $a\in C$ we have $\sigma_\pi(a)\in C$ where

$$\begin{array}{rccc}\sigma_\pi: & \underbrace{\mathbb{F}_q^m\oplus\ldots\oplus\mathbb{F}_q^m}_{s\ times} & \longrightarrow & \underbrace{\mathbb{F}_q^m\oplus\ldots\oplus\mathbb{F}_q^m}_{s\ times}\\ & (u_1,u_2,\ldots,u_s) & \mapsto & (u_s,u_1,\ldots,u_{s-1})\end{array}$$

σ_π is a cyclic shift of one block to the right.

Proposition 6.2: Let $\mathbb{F}_q$ be the finite field of q elements and $R_\pi=\frac{\mathbb{F}_q^n[X]}{<X^n-1>}$, then $(R_\pi,+,\star)$ where "$+$" is the classical addition and "$\star$" is the multiplication defined by

- For $i\in\mathbb{N}$; $X^i\star X^j=X^{i+m-1}.X^j=X^j\star X^i$ where "." is the classical multiplication.
- For $i,j,k\in\mathbb{N}$ $X^i\star(X^j\star X^k)=(X^i\star X^j)\star X^k$.

is a commutative ring, with $\mathbf{1}^\star=X^{n-m+1}$ is the unity element for the law $\star$.

we have the following results

1) A linear error-block code C is π-cyclic if and only if C is an ideal of $(R_\pi,+,\star)$.
2) There exist a unique unitary polynomial g in C, of minimal degrees and called the generator polynomial of the code C, such that $g(x)$ divides every word $c(x)$ in C and $g(x)$ divides X^n-1 in $\mathbb{F}_q[X]$.
3) If $g(X)=g_0(X)+X\star g_1(X)+\ldots+X^{\star r}\star g_r(X)$ is the generator polynomial of C where $g_0,g_1,\ldots,g_r$ are non-zero polynomials in $\frac{\mathbb{F}q[X]}{<X^m-1>}$. Then $\dim C=k=l-r$ and C is generated by the matrix

$$G=\begin{pmatrix}g(X)\\ X\star g(X)\\ \ldots\\ X^{\star(l-1)}\star g(X)\end{pmatrix}=$$

$$\begin{pmatrix}g_0(x) & \ldots & g_r(x) & 0 & \ldots & 0 & 0\\ 0 & g_0(x) & \ldots & g_r(x) & 0 & \ldots & 0\\ \vdots & & & & & & \\ 0 & 0 & \ldots & 0 & g_0(x) & \ldots & g_r(x)\end{pmatrix}$$

A. Tensor Product of two Cyclic linear error-block codes

Theorem 6.3: Let C_1 and C_2 be respectively $[n_1,k_1,d_1]$ and $[n_2,k_2,d_2]$ cyclic LEB codes of types $\pi_1=[m_1]^{s_1}$ and $\pi_2=[m_2]^{s_2}$ where $s_1\wedge s_2=1$, then the code $C=C_1\otimes C_2$ of type $\pi=[n_1m_2]^{s_2}$ is an $[n_1n_2,k_1k_2,d_1]$ cyclic LEB code.

Proof: Assume C_1 and C_2 are two π-cyclic codes of types $\pi_1=[m_1]^{s_1}$ and $\pi_2=[m_2]^{s_2}$ respectively. The code $C=C_1\otimes C_2$ is defined by its generator matrix

$G=G_1\otimes G_2=$

$$\left(\begin{array}{c|c|c|c|c|c}\gamma_0 & \ldots & \gamma_r & 0 & \ldots\ldots & 0\\ 0 & \gamma_0 & \ldots & \gamma_r & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & \gamma_0 & \ldots & \gamma_r\end{array}\right).$$

where $\gamma_i=g_i(x)\star G_2$

A codeword $c(X,Y)$ of $C=C_1\otimes C_2$ can be obtained from the matrix representation $(\alpha_{ij})_{0\leq i<s_1-10\leq j<s_2-1}$ as follows

$$c(X,Y)=\sum_{i=0}^{s_1-1}\sum_{i=0}^{s_2-1}\alpha_{ij}\star X^{\star i}\star Y^{\star j}mod(X^{m_1m_2}-1).$$

If we suppose $X^{n_1}=1$ and $Y^{n_2}=1$, then $X\star c(X,Y)$ and $Y\star c(X,Y)$ represent cyclic shifts of the rows and the columns, and also belong to $C=C_1\otimes C_2$. Therefore C is an ideal of $(\frac{\mathbb{F}q[X]}{<X^{m_1m_2-1}>},\star)$. To represent $C(X,Y)$ as univariate polynomial $\tilde{C}(X)$, we suppose s_1 and s_2 are relatively prime. Then by the Chinese remainder for each pair i,j where $0\leq i<s_1-1$ and $0\leq j<s_2-1$, there is a unique integer $0\leq I(i_1,i_2)<s_1s_2$ such that $I(i,j)\equiv i\ mod[s_1]$ and $I(i,j)\equiv j\ mod[s_2]$ and

$$\tilde{C}(Z)=\sum_{i=0}^{s_1-1}\sum_{i=0}^{s_2-1}\alpha_{ij}\star Z^{\star I(i,j)}mod(Z^{m_1m_2-1}).$$

where $Z=X\star Y$.

Since $C(X,Y)\in C$, $Y\star C(X,Y)\in C$, then $Z\star\tilde{C}(Z)=X\star Y\star C(X,Y)\in C$. Therefore C is an LEB π-cyclic code. ■

B. Tensor Product of two Simplex linear error-block codes

Theorem 6.4: The TP code C of two simplex codes C_1 and C_2 of types $\pi_1=[m_1]^{s_1}$ and $\pi=[m_2]^{s_2}$ is a simplex code

of type $\pi = [n_1 m_2]^{s_2}$ and the common π-weight of the non zero codewords of C is

$$w_{\lambda_2} = 2^{r_2 - m_2} = 2^{(\lambda_2 - 1)m_2}$$

where $\lambda_2 = \frac{r_2}{m_2}$ is an integer and for $i = 1, 2$ $s_i = \frac{q^{r_i}-1}{q^{m_i-1}-1}$ and $r_i = n_i - k_i$.

Proof: Suppose C_1 and C_2 are simplex, then the LEB code of type $\pi = [n_1 m_2]^{s_2}$ is an $[n_1 n_2, k_1 k_2, d_1]$ defined by its generator matrix $H_2 = G_{1,\lambda=2} \otimes G_{2,\lambda=2} =$

$$\left(\begin{array}{c|c|c|c|c} I_{m_2} \otimes G_1 & E_1 \otimes G_1 & \ldots\ldots & E_{q^{m_2}-1} \otimes G_1 & 0_{m_2} \otimes G_1 \\ 0_{m_2} \otimes G_1 & I_{m_2} \otimes G_1 & \ldots\ldots & I_{m_2} \otimes G_1 & I_{m_2} \otimes G_1 \end{array} \right)$$

and for $\lambda_2 \geq 3$, define inductively H_{λ_2} by: $H_{\lambda_2} = G_{1,\lambda} \otimes G_{2,\lambda} =$

$$\left(\begin{array}{c|c|c|c|c} I_{m_2} \otimes G_1 & A_1 \otimes G_1 & \ldots & A_{q^{m_2}-1} \otimes G_1 & A_0 \otimes G_1 \\ 0_{m_2(\lambda_2-1)} \otimes G_1 & H_{\lambda_2-1} \otimes G_1 & \ldots & H_{\lambda_2-1} \otimes G_1 & H_{\lambda_2-1} \otimes G_1 \end{array} \right)$$

where $G_{1,\lambda}$ with $(\lambda \geq 3)$ and $G_{2,\lambda}$ are respectively generator matrices of C_1 and C_2 with the form defined in Equations (12) and (13).

- Set s_{λ_2} and w_{λ_2} where $r_2 = n_2 - k_2 = m_2\lambda$ respectively the number of blocks of H_{λ_2} and the weight of a codeword c in S_{λ_2}.
- The non-zero codewords generated by H_2, have the weight

  $$w_2 = s_{2,\lambda_2=2} - 1 = \frac{q^{2m_2}-1}{q^{m_2}-1} - 1 = q^{m_2} - 1 + 1 = q^{(2-1)m_2}.$$

  In fact, each non-zero codeword generated by H_2 is defined by one of the following forms of matrices :

  $$c = (e \otimes G_1 \mid a_1 \otimes G_1 \mid a_2 \otimes G_1 \mid \ldots \mid a_{q^{m_2}} \otimes G_1 \mid 0 \otimes G_1)$$

  or

  $$c = (0 \otimes G_1 \mid e_1 \otimes G_1 \mid e_2 \otimes G_1 \mid \ldots \mid e_{q^{m_2}} \otimes G_1)$$

  where for all $i = 1, \ldots, q^{m_2}$, a_i is a codeword generated by H_{λ_2-1}, e_i is in $\mathbb{F}_q^{m_2}$ and e is an element of the canonic basis of $\mathbb{F}_q^{m_2}$.
- We suppose the non-zero codewords generated by H_{λ_2-1} have the weight $w_{\lambda_2-1} = q^{r_2-2m_2} = q^{r_2(\lambda_2-2)}$.
- Then, the non-zero codewords of the sub-code generated by the last $(r_2 - m_2)$ rows of H_{λ_2} are defined by the matrix $c = (0 \otimes G_1 \mid a_1 \otimes G_1 \mid a_2 \otimes G_1 \mid \ldots \mid a_{q^m} \otimes G_1)$ where for all $i = 1, \ldots, q^m$, a_i is a codeword generated by H_{λ_2-1}. Therefore,

  $$w_{\lambda_2} = q^{m_2}.w_{\lambda_2-1} = q^{m_2}(q^{r_2-2m_2}) = q^{r_2-m_2}.$$

- The remaining non-zero codewords generated by H_{λ_2-1} is defined by the matrix $(e \otimes G_1 \mid a_1 \otimes G_1 \mid a_2 \otimes G_1 \mid \ldots \mid a_{q^m-1} \otimes G_1, \underbrace{0 \otimes G_1 \ldots 0 \otimes G_1}_{s_{\lambda_2-1} time})$ where for all $i = 1, \ldots, q^{m_2}$, $a_i \neq 0$ and e is an element of the canonic basis of $\mathbb{F}_q^{m_2}$. These codewords have the weight

  $$\begin{array}{rcl} w_{\lambda_2} & = & s_{2,\lambda_2} - s_{2,\lambda_2-1} \\ & = & \frac{q^{m_2\lambda_2}-1}{q^{m_2}-1} - \frac{q^{m_2(\lambda_2-1)}-1}{q^{m_2}-1} \\ & = & \frac{q^{m_2\lambda_2} - q^{m_2(\lambda_2-1)}}{q^{m_2}-1} \\ & = & q^{m_2(\lambda_2-1)}(\frac{q^{m_2}-1}{q^{m_2}-1}) \\ & = & q^{m_2(\lambda_2-1)} = q^{r_2-m_2} \end{array}$$

- Thus by induction, all the non-zero codewords of C' have the weight

  $$w_{\lambda_2} = q^{r_2-m_2} = q^{(\lambda_2-1)m_2}.$$

■

VII. Conclusion

In this paper where we have explored the different possibilities using tensor product and LEB codes, we have presented two different constructions of LEB codes using tensor product. We have shown that the tensor product of two block codes is not an LEB code and that the tensor product of two Hamming codes is in general not a perfect Hamming code. Besides, we have shown that the tensor product of two cyclic LEB codes is a cyclic LEB code and the tensor product of two Simplex LEB codes is also a simplex LEB code. In future projects, we plan to explore the tensor product on codes with partitions π of sub-blocks of different lengths. Also working on factoring the new construction to optimize the decoding of certain LEB codes.

References

[1] K. Feng, L. Xu, and F. J. Hickernell., "Linear error-block codes," *Finite Fields and Their Applications*, vol. 12, pp. 638–652, 2006.

[2] R. Dariti and E. M. Souidi, "Cyclicity and decoding of linear error-block codes." *Journal of Theorecal and Applied Information Technology*, vol. 25, pp. 39–42, 2011.

[3] ——, "An application of linear error-block codes in steganography." *International Journal of Digital Information and Wireless Communications*, vol. 1, pp. 426–433, 2012.

[4] J. K. Wolf, "An introduction to tensor product codes and applications to digital storage systems," *Information Theory Workshop*, pp. 6–10, 2006, iTW '06 Chengdu. IEEE.

[5] H. Imai and H. Fujiya, "Generalized tensor product codes,," *Transactions on Information Theory*, vol. 27, no. 2, pp. 181–187, 1981, iEEE.

[6] H. Alhussien and J. Moon, "An iteratively decodable tensor product code with application to data storage," *IEEE J. Sel. Areas Commun*, vol. 2, no. 28, p. 228–240, 2010.

[7] P. Chaichanavong and P. H. Siegel, "Tensor-product parity code for magnetic recording," *IEEE Trans. Magn.*, vol. 42, no. 2, p. 350–352, 2006.

[8] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Tech. J.*, vol. 29, pp. 147–160, 1950.

[9] S. Belabssir, E. B. Ayebie, and E. M. Souidi, "Perfect, hamming and simplex linear error-block codes with minimum π-distance 3," ser. Lecture Notes in Computer Science, vol. 11445. Springer, 2019, pp. 288–306.

[10] S. Belabssir, N. Sahllal, and E. M. Souidi, "Cyclic linear error-block codes," *AIP Conference Proceedings*, vol. 2074, no. 1, p. 020005, 2019.