The Weight Enumerator of Some Families of Linear Error-Block Codes

S. Belabssir

Abstract—**In this paper, we introduce the notion of π-weight distribution for linear error-Block (LEB) codes. We compute the π-weight enumerator of simplex and Hamming LEB codes. We also show that some cosets have uniquely determined distributions. We prove that if the weight distribution of the cosets is known, and that the dimension of the LEB code is increased by one, then, the π-weight can be explicitly determined. Thereafter, we compute the π-weight enumerator of the direct sum of two LEB codes. Finally, we compute the π-weight enumerator of punctured and shortened LEB codes.**

Index Terms—**Weight distribution, Hamming Codes, Simplex Codes, Linear Error-Block Codes, Weight Enumerator, coset, Direct Sum Codes, Puncturing, Shortening.**

I. Introduction

LINEAR error-block codes (LEB) were introduced by Feng et al. in [1]. They are a generalization of classical codes (linear block codes), and they have application in experimental design since they yield mixed-level orthogonal arrays, and in high-dimensional numerical integration. [1] gives some algebraic aspects and fields of applications of linear error-block codes, and some open problems are stated in its concluding section. So far, there is a limited number of publications that deal with LEB codes. Alves et al. [2] have studied combinations between the π-metric (used with linear error-block codes) and the poset metric. A generalization of some results on packing and covering radii to the LEB case is made, and some bounds on packing and covering radii of these codes are given in [3]. Optimal linear error-block codes are discussed in [4]. In [5], the authors constructed new families of perfect linear error-block codes of minimum π-distance 3, 4 and 5. In [6], an algebraic study of cyclic LEB codes and some relevant results are discussed. In [7], the authors gives the existence conditions of infinite families of perfect LEB codes, and expended the notions of Hamming and simplex codes to linear error-block codes. In [9], the authors constructed new LEB codes using the tensor product of two codes, and claimed that some optimal LEB codes can be constructed from known optimal LEB codes. In order to allow the application of LEB codes in cryptography, especially in a McEliece-like cryptosystem, Dariti et al. [11] presented a method for decoding linear error-block codes inspired from the standard array classical method. The same authors presented in [8] some solutions on the use of LEB codes in codes-based cryptosystems, namely, the McEliece-like and Niederreiter cryptosystems, and realized that this solutions keep the size of the public key unchanged while it preserves, or even enhance, security parameters of the cryptosystem. They also used LEB codes in CFS signature scheme [8], and discovered that the use of LEB codes in CFS signature provide an improvement in the matter of density of decodable words with the π-metric, which will be grater. In the same work [8], a channel model which enables LEB codes to be used in correcting errors raised from transmission over a noisy channel was designed. LEB codes have also application in the field of steganography, where Dariti and Souidi [13] have introduced a protocol of steganography based on LEB codes. They have shown that employing convenient codes enhances the reliability of that protocol compared to other known steganography protocols. This steganographic protocol generalizes the idea of matrix encoding to be used with several bit planes. The scheme was ameliorated in [12].

The weight enumerator of a linear code is a classifying polynomial associated with the code. Besides its intrinsic importance as a mathematical object, it is used in the probability theory around codes. For example, the weight enumerator of a binary code is very useful to study the probability that a received message is closer to a different codeword than to the codeword sent (Or, rephrased: the probability that a maximum likelihood decoder makes a decoding error). The weight distribution of a linear code is one of the most important characteristics of a code. In some special cases, the weight distribution can uniquely identify a linear code. Among the most remarkable properties of weight distributions is how they relate to the dual code. In fact, MacWilliams [10] showed that the Hamming weight enumerator of the dual code is uniquely determined by the Hamming weight enumerator of a code over a finite field. In [1], Feng *et al.* generalized the definition of the homogeneous π-weight enumerator and the MacWilliams Identity to the LEB case.

In this paper, we extend the definition of the weight enumerator to linear error-block codes case, and give a simple formula for the π-weight for some families of LEB codes, namely the Hamming and the Simplex codes, cosets leaders of LEB codes, and the direct sum of two LEB codes as well as the puncturing and the Shortening techniques. This paper is organized as follows. In Section 2, we give an overview about LEB codes. In Section 3, a definition of the π-weight enumerator and some related results are reached. In Section 4, we give the π-weight enumerator of simplex codes. In Section 5, the study is focused on the π-weight enumerator for cosets of an LEB codes. In Section 6, we determine the π-weight distribution of LEB codes generated from the direct sum of two LEB codes. The π-weight distribution of LEB codes generated from the puncturing and shortening techniques is determined in Section 7. Finally, the conclusion and the perspective of this work are given in Section 8.

Manuscript received September 22, 2020; revised May 23, 2022.
Soukaina Belabssir is a PhD candidate of University Mohammed V, Rabat, Morocco, BP 1014, (e-mail: soukainabelabssir@gmail.com)

II. PRELIMINARIES

A partition π of a positive integer n, is defined by

$$n = n_1 + n_2 + \ldots + n_s$$

(with $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$, and s is an integer ≥ 1), and is denoted by $\pi = [n_1][n_2]\ldots[n_s]$. Furthermore, if

$$n = \sum_{i=1}^{s} n_i = \sum_{i=1}^{r} l_i m_i$$

where $m_1 > m_2 > \ldots > m_r \geq 1$, then π will be denoted by

$$\pi = [m_1]^{l_1}[m_2]^{l_2}\ldots[m_r]^{l_r}.$$

Let $\pi = [n_1][n_2]\ldots[n_s](s \geq 1)$ be a partition of an integer n and $V_i = \mathbb{F}_q^{n_i}$ $(1 \leq i \leq s)$, and

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

Where $\mathbb{F}_q$ is a finite field with q elements and q is a prime power.

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 $u = (u_1, u_2, \ldots, u_s)$ and $v = (v_1, v_2, \ldots, v_s)$ in V, the π-weight $w_\pi(u)$ and respectively the π-distance $d_\pi(u, v)$ are defined by:

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

and

$$\begin{aligned} d_\pi(u, v) &= w_\pi(u - v) \\ &= \sharp\{i/1 \leq i \leq s,\ u_i,\ v_i \in V_i \text{ and } u_i \neq v_i\}. \end{aligned}$$

A linear error-block code over $\mathbb{F}_q$ of type π is an $\mathbb{F}_q$-linear subspace C of V. The integer n is called the length of C, $k = dim_{\mathbb{F}_q} C$ is its dimension and

$$\begin{aligned} d_\pi &= \min\{d_\pi(c, c')/c, c' \in C, c \neq c'\} \\ &= \min\{w_\pi(c)/0 \neq c \in C\}, \end{aligned}$$

is its minimal π-distance. Such LEB code is denoted by $[n, k, d_\pi]_q$ code. Therefore, 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:

Theorem II.1 ([1]). *Let $H = [H_1, H_2, \ldots, H_s]$ be a parity-check matrix of an $[n, k, d_\pi]$ code C over $\mathbb{F}_q$ of type $\pi = [n_1][n_2]\ldots[n_s]$. Then the minimum π-distance is d_π if and only if the union of columns of any $d_\pi - 1$ blocks of H are $\mathbb{F}_q$-linearly independent and there exist d_π blocks columns of H which are linearly dependent.*

Example II.2. *Let C be a $[7, 2, 2]$ binary code of type $\pi = [3][2][1]^2$ over $\mathbb{F}_2$ defined as follows:*

$$C = \{000|00|0|0, 101|10|1|0, 011|11|0|0, 110|01|1|0\}.$$

Then C is generated by the matrix

$$G = \left(\begin{array}{ccc|cc|c|c} 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right).$$

If C is an $[n, k]$ code of type $\pi = [n_1][n_2]\ldots[n_s]$ where $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$, of generator matrix G and parity-check matrix H. The dual of C is an $[n, n-k]$ code of type π of generator matrix H and parity-check matrix G, and it is denoted by $C^\perp$.

III. π-WEIGHT ENUMERATOR OF AN LEB CODE

In this section, we introduce the notion of π-weight distribution for an LEB code, and we give some relevant results.

Definition III.1. *Let C be an $[n, k, d]_q$ code of type $\pi = [n_1][n_2]\ldots[n_s]$ where $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$ with $s \geq 1$ and $\sum_{i=1}^{s} n_i = n$. Let*

$$A_i(C) = \mid \{c \in C/w_\pi(c) = i\} \mid$$

be the number of codewords in C of π-weight i for $i = 0, 1, \ldots, s$.

The π-weight spectrum of C is defined as the following

$$S_\pi(C) = \{(i, A_i(C))/i = 1, \ldots, s\}.$$

And the weight distribution of a linear code C is the vector

$$A(C) = (A_0(C), \ldots, A_s(C)),$$

it simply shows the number of codewords of a particular π-weight in the code.

The so called π-weight enumerator is a convenient representation of the weight spectrum.

Definition III.2. *Let C be an $[n, k, d]_q$ code of type $\pi = [n_1][n_2]\ldots[n_s]$ where $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$ and $s \geq 1$ with $\sum_{i=1}^{s} n_i = n$.*

- *The π-weight enumerator of C is defined as the following polynomial*

$$w_{\pi,C}(Z) = \sum_{i=0}^{s} A_i(C) Z^i.$$

where $A_i(C)$ is the number of codewords in C of π-weight i.

- *The homogeneous π-weight enumerator of C is defined as*

$$\begin{aligned} W_{\pi,C}(X, Y) &= \sum_{c \in C} X^{s - w_\pi(c)} Y^{w_\pi(c)} \\ &= \sum_{i=0}^{s} A_i(C) X^{s-i} Y^i. \end{aligned}$$

where $A_i(C)$ is the number of codewords in C of π-weight i.

Remark III.3. Note that $w_{\pi,C}(Z)$ and $W_{\pi,C}(X, Y)$ are equivalent in representing the weight spectrum. They determine each other uniquely by the following equations:

$$w_{\pi,C}(Z) = W_{\pi,C}(1, Z)$$

and

$$W_{\pi,C}(X, Y) = X^s w_{\pi,C}(Y.X^{-1})$$

Proposition III.4. *Let C be an $[n, k, d]$ LEB code over $\mathbb{F}_q$. Then*

1. *$A_0 = 1$ and $A_j = 0$ for $0 < j < d$.*

2. $\sum_j A_j = q^k$

Proof: easy to prove by analogy to the classical case. ■

Example III.5. • *The zero code has one codeword of π-weight is zero. Then*

$$W_{\pi,C}(X,Y) = A_0(C)X^{s-0}Y^0 = X^s.$$

- *For an $[n,k,d]_q$ MDS code C of type $\pi = [m]^s$, the π-weight distribution of C is:*

$$A_i(C) = \binom{s}{i}(q^m-1)\sum_{j=0}^{i-d}\binom{i-1}{j}q^{m(i-d-j)}(-1)^j$$

for $d \leq i \leq s$.
$A_i = 0$ for $1 \leq i < d$, and $A_0 = 1$.
Thus, the π-weight distribution of C is

$$W_{\pi,C}(X,Y) = \sum_{i=0}^{s} A_i(C)X^{s-i}Y^i$$

The weight enumerator satisfies the MacWilliams Identity, which was showed for codes of type $\pi = [m]^s$ in [1] as follows:

Theorem III.6. *[1] Let C be a linear code over $\mathbb{F}_q$ of type $\pi = [m]^s$. Then*

$$W_{\pi,C^\perp}(X,Y) = \frac{1}{\mid C \mid} W_{\pi,C}(X+(q^m-1)Y, X-Y).$$

IV. π-WEIGHT ENUMERATOR OF HAMMING AND SIMPLEX CODES

Let C be an LEB code of type $\pi = [m]^s$ with $s = \frac{q^r-1}{q^m-1}$ where $r = \lambda m$, $\lambda \geq 2$ and $dim_{\mathbb{F}_q}(C) = n-r$. C is said to be a Hamming LEB code of type π and denoted by π-Ham(r,q) if and only if its parity-check matrix H_λ is an $r \times n$ matrix for which the union of columns of any blocks is linearly independent.

A code C' is called a simplex code if all its non-zero codewords have the same weight.

In [7], we have proven that the dual code of C is a simplexe code and the comon π-weight of its codewords is

$$W_\lambda = q^{r-m} = q^{(\lambda-1)m}$$

where $\lambda = \frac{r}{m}$ is an integer ≥ 2. We have also shown that the parity check matrix of C is defined recursively as follows :

$$H_2 = \left(\begin{array}{c|c|c|c|c} I_m & E_1 & \ldots\ldots & E_{q^m-1} & 0_m \\ 0_{m-1} & I_m & \ldots\ldots & I_m & I_m \end{array} \right) \quad (2)$$

and for $\lambda \geq 3$

$$H_\lambda = \left(\begin{array}{c|c|c|c|c} I_m & A_1 & \ldots\ldots & A_{q^m-1} & A_0 \\ 0_{m(\lambda-1)} & H_{\lambda-1} & \ldots\ldots & H_{\lambda-1} & H_{\lambda-1} \end{array} \right) \quad (3)$$

where

- $E_1, \ldots, E_{q^m-1}$ are the blocks extensions of non-zero vectors in $\mathbb{F}_q^m$. (where a block extension of a vector $v = (v_1, \ldots, v_n)$ in $\mathbb{F}_q^n$ is an $n \times n$ matrix E for which the columns are linearly independent and the sum of all its columns is equal to v^T (transpose of v), note also that if E and E' are two blocks extensions of two different vectors v and v' in $\mathbb{F}_q^m$, then, the columns of the matrix
$$\left(\begin{array}{c|c} E & E' \\ I_m & I_m \end{array} \right)$$
are linearly independent with I_m is the matrix identity of size m.)
- For all $1 \leq i \leq q^m - 1$, $A_i = (\underbrace{E_i, \ldots, E_i}_{s_{\lambda-1}\ time})$ where $s_{\lambda-1} = \frac{q^{(\lambda-1)m}-1}{q^m-1}$.
- $A_0 = (\underbrace{0_m, \ldots, 0_m}_{s_{\lambda-1}\ time})$ where 0_m is the $m \times m$ null matrix.

In this section, we consider simplex codes of type $\pi = [m]^s$ with $s = \frac{q^r-1}{q^m-1}$ where $r = \lambda m$, $\lambda \geq 2$ and $dim_{\mathbb{F}_q}(C) = n-r$. These codes give interesting results about the π-weight enumerator described in Theorem IV.1 and Theorem IV.2.

Theorem IV.1. *Let C be an $[n,r,d=3]_q$ simplex LEB code over $\mathbb{F}_q$ of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$, $r = \lambda m$, $\lambda \geq 2$ and $r \geq 1$. Then, the homogeneous π-weight of C equals :*

$$W_{\pi,C}(X,Y) = X^s + (q^r-1)X^{s-r+m}Y^{r-m}$$

Proof: Let C be an $[n,r,3]_q$ simplex code over $\mathbb{F}_q$ of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$ and $r = n - dim_{\mathbb{F}_q}(C)$, then by Theorem 10 of [7] all non-zero codewords of C have the π-weight q^{r-m}. Therefore,

$$\begin{aligned} W_{\pi,C}(X,Y) &= \sum_{w_\pi=0}^{s} A_{w_\pi}(C)X^{s-w_\pi(c)}Y^{w_\pi(c)} \\ &= A_0(C)X^{s-0}Y^0 + A_{q^{r-m}}(C)X^{s-r+m}Y^{r-m} \\ &= X^s + (\mid C \mid -1)X^{s-r+m}Y^{r-m} \\ &= X^s + (q^r-1)X^{s-r+m}Y^{r-m} \end{aligned}$$

■

Theorem IV.2. *Let H_π be an $[n,k,d=3]_q$ perfect $\pi - ham(n-k,q)$ code of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$, $r = \lambda m$, $\lambda \geq 2$ and $k = n-r \geq 1$. Then the homogeneous π-weight of H_π equals :*

$$\begin{aligned} W_{\pi,H_\pi}(X,Y) = \frac{1}{q^k}[&(X+(q^m-1)Y)^s + (q^r-1) \\ &(X+(q^m-1)Y)^{s-r+m}(X-Y)^{r-m}] \end{aligned}$$

Proof: Let H_π be an $[n,k,3]_q$ perfect $\pi - ham(n-k,q)$ code of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$, r is a multiple of m and $r = n-k \geq 1$.

Then H_π is the dual code of an $[n,k,3]_q$ simplex code C of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$. Hence, the MacWilliams Identity states that

$$W_{\pi,H_\pi}(X,Y) = \frac{1}{\mid C \mid} W_{\pi,C}(X+(q^m-1)Y, X-Y)$$

Thanks to Theorem IV.1,

$$W_{\pi,C}(X,Y) = X^s + (q^r-1)X^{s-r+m}Y^{r-m}$$

Then,

$$W_{\pi,H_\pi}(X,Y) = \frac{1}{q^k}[(X+(q^m-1)Y)^s + (q^r-1)$$
$$(X+(q^m-1)Y)^{s-r+m}(X-Y)^{r-m}]$$

■

Example IV.3. *Let S be the simplex $[10,4,3]_2$ code of type $\pi=[2]^5$ generated by the matrix*

$$G = \left(\begin{array}{cc|cc|c|c|c} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$

Therefore,

$$W_{\pi,S}(X,Y) = X^5 + 15X^3Y^2$$

is the homogeneous π-weight of S, and

$$W_{\pi,H_\pi}(X,Y) = \frac{1}{16}[(X+15Y)^5 + 15(X+15Y)^3(X-Y)^2]$$

is the homogeneous π-weight of H_π, where H_π is the $\pi - Ham(6,2)$ LEB code of type $\pi=[2]^5$.

V. π-Weight Enumerators and Cosets

Let C be an LEB code over $\mathbb{F}_q^n$ and v be any vector in $\mathbb{F}_q^n$. A coset of C is a set $v+C$ defined by

$$v+C = \{v+c, c \in C\}.$$

Just like codes, the cosets have a π-weight distribution and a minimum π-weight. A vector in a coset with minimum π-weight is called a coset leader. In this section, the π-weight distribution of cosets of an LEB codes are studied. We will show that some cosets have uniquely determined distributions. We will also prove that when the weight distribution of the cosets is known, and that the dimension of the LEB code is increased by one, the new resulting π-weight is explicitly determined.

Theorem V.1. *Let C be an $[n,k,d]$ LEB code over $\mathbb{F}_q^n$, of type $\pi=[n_1]\dots[n_s]$ ($n_1 \geq \dots \geq n_s \geq 1$, $s \geq 1$ and $n_1 = \sum_{i=0}^{s} n_i$) and with π-weight enumerator $W_{\pi,C}(X)$. Let u be a vector in $\mathbb{F}_q^n$ which is not in C (i.e. $u \in \mathbb{F}_q^n \setminus C$). Let C' be the $[n,k+1]$ LEB code generated by C and u, and $\alpha \in \mathbb{F}_q$. Then,*

i) *The weight distributions of $u+C$ and $\alpha u + C$ are identical, when $\alpha \neq 0$.*
ii) $W_{\pi,C'} = (q-1)W_{\pi,u+C} + W_{\pi,C}$.

Proof: Since $\alpha u + C = \alpha(u+C)$, the weight distributions of $\alpha u + C$ and $\alpha(u+C)$ are identical. Moreover, the π-weight $w_\pi(\alpha(u+c)) = w_\pi(u+c)$ for all $c \in C$. Thus, (i) is proven. Let $u \in \mathbb{F}_q^n \setminus C$, and C' be the $[n,k+1]$ LEB code generated by C and u. Then, the generator matrix of C' is the generator matrix G of C with the vector u appended as a new row, and so, C' is the same code as $C \cup (u+C)$. From Theorem 1.1. in [8], we state that $\mathbb{F}_q^n$ is just the union of q^{n-k} distinct cosets of C, and since C is the coset $0+C$, then, $C \cap \alpha u + C$ is empty for all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$. Thus, $A_i(C') = (q-1)A_i(\alpha u + C) + A_i(C)$. Since $A_i(\alpha u + C) = A_i(u+C)$ by (i) then, $A_i(C') = (q-1)A_i(u+C) + A_i(C)$ for all $i \in \{0,\dots,s\}$ and

$$\begin{aligned} W_{\pi,C'}(X) &= \sum_{i=0}^{s} A_i(C')X^i \\ &= \sum_{i=0}^{s}(A_i(C) + (q-1)A_i(u+C))X^i \\ &= \sum_{i=0}^{s} A_i(C)X^i + (q-1)\sum_{i=0}^{s} A_i(u+C)X^i \\ &= (q-1)W_{\pi,u+C} + W_{\pi,C} \end{aligned}$$

■

VI. π-Weight Enumerators and Direct Sum

Let C_1 and C_2 be $[n_1,k_1,d_1]_q$ and $[n_2,k_2,d_2]_q$ LEB codes types $\pi_1 = [n_1]\dots[n_{s_1}]$ ($n_1 \geq \dots \geq n_{s_1} \geq 1$ and $n_1 = \sum_{i=0}^{s_1} n_i$) and $\pi_2 = [m_1]\dots[m_{s_2}]$ ($m_1 \geq \dots \geq m_{s_2} \geq 1$ and $m_2 = \sum_{i=0}^{s_2} m_i$), and with generator matrices G_1 and G_2 respectively. We denote by $\pi_1\pi_2$ the partition defined by

$$\pi = \pi_1\pi_2 = [n_1]\dots[n_{s_1}]\,[m_1]\dots[m_{s_2}]$$

The direct sum of C_1 and C_2 is the

$$[n_1+n_2, k_1+k_2, min(d_1,d_2)]$$

LEB code C of type $\pi = [\pi_1][\pi_2]$ where

$$C = C_1 \oplus C_2 = \{(c_1,c_2)/c_1 \in C_1, c_2 \in C_2\}.$$

In the following theorem, we give the π-weight Enumerator of C:

Theorem VI.1. *Let C_1 and C_2 be $[n_1,k_1]_q$ and $[n_2,k_2]_q$ LEB codes types of π_1 and π_2, and with π-weights enumerators $W_{\pi_1,C_1}(X)$ and $W_{\pi_2,C_2}(X)$ respectively. The π-weight enumerator of the code $C = C_1 \oplus C_2$ is*

$$W_{\pi,C_1\oplus C_2}(X) = W_{\pi_1,C_1}(X).W_{\pi_2,C_2}(X),$$

where $\pi = [\pi_1][\pi_2]$.

Proof: Let C_1 and C_2 be two LEB codes as defined above, with generator matrices G_1 and G_2 respectively. Then, the generator matrix of $C = C_1 \oplus C_2$ is

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

Let $A(C_1)$, $A(C_2)$ and $A(C)$ be the weight distributions for C_1, C_2 and C respectively. Furthermore, let $A_i(C_1)$, $A_i(C_2)$ and $A_i(C)$ be the number of codewords of C_1, C_2 and C of π-weight i respectively. Let c_1 and c_2 two codewords of C_1 and C_2 respectively and such that $w_\pi(c_1) = i$ and $w_\pi(c_2) = j$. The vectors $(c_1,0)$, $(0,c_2)$ and (c_1,c_2) are codewords of C, with π-weights i, j and $i+j$ respectively. Thus, $A_k = A_i(C_1) \times A_j(C_2)$ for all i,j such that $k = i+j$.

$A(C)$ being the result of a convolution of π-weights distribution vectors $A(C_1)$ and $A(C_2)$, we get

$$\begin{aligned} W_{\pi,C}(X) &= \sum_{k=0}^{s_1+s_2} A_k(C)X^k \\ &= \sum_{j+i=k} A_i(C_1)X^i A_j(C_2)X^j \\ &= \sum_{j+i=k} A_i(C_1)A_j(C_2)X^{i+j} \\ &= W_{\pi_1,C_1}(X).W_{\pi_2,C_2}(X) \end{aligned}$$

■

Example VI.2. *Let C_1 and C_2 be $[4,3,1]_2$ and $[3,1,1]$ LEB code of types $\pi_1 = [2][1]^2$ and $\pi_2 = [3]^1$, and defined using their generator matrices*

$$G_1 = \left(\begin{array}{cc|c|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

and

$$G_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

respectively. Then, C_1 have the weight distribution $A_0(C_1) = 1$, $A_1(C_1) = 1$, $A_2(C_1) = 5$ and $A_3(C_1) = 1$, and C_2 have the weight distribution $A_0(C_2) = 1$ and $A_1(C_2) = 1$. Thus,

$$W_{\pi,C_1}(X) = 1 + X + 5X^2 + X^3$$

and

$$W_{\pi,C_2}(X) = 1 + X$$

. Hence, $C = C_1 \oplus C_2$ is a $[7,4,1]$ code with generator matrix

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

Moreover, the π-weights enumerator of C is

$$\begin{aligned} W_{\pi,C}(X) &= W_{\pi_1,C_1}(X).W_{\pi_2,C_2}(X) \\ &= 1 + 2X + 6X^2 + 6X^3 + X^4. \end{aligned}$$

VII. π-Weight Enumerators of Punctured and Shortened LEB Codes

An $[n,k,d]$ code over $\mathbb{F}_q$ is distance-optimal (respectively, dimension-optimal and length-optimal) if there is no $[n,k,d' \geq d+1]$ (respectively, $[n,k \geq k+1,d]$ and $[n' \leq n-1,k,d]$) linear code over $\mathbb{F}_q$. An optimal code is defined to be a code that is length-optimal, or dimension-optimal, or distance-optimal, or meets a bound for linear codes. An important problem in the theory and application of coding theory is the construction of optimal codes and codes with desirable parameters. To this end, one may construct a linear code with good or desirable parameters from a known linear code with optimal or good parameters.

The puncturing and shortening techniques are two important approaches to construct new linear codes from old ones, their principal role is to create new optimal codes from old known codes.

In this section, we aim to determine the π-weight enumerator of punctured and shortened LEB codes.

Firstly, we will define the technique of puncturing a LEB code.

Secondly, we will show that the resulting set after puncturing a LEB code is also an LEB code, and we will define its properties.

Thirdly, we will extend the notion shortening techniques to the LEB codes, we prove that this two technique yields an other LEB cods that we give their properties.

Finally, we will give the appropriate π-weight enumerator of both punctured and shortened LEB codes.

A. Puncturing LEB Codes

For the classical case, the puncturing technique consists on delete coordinates from all its codewords. However, there exit two ways to puncture an LEB code. In the following, we define the puncturing technique for the LEB case, and we give the properties of a punctured code.

Definition VII.1. *Let C be an $[n,k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\dots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$). For all $i = 1,\dots,s$, let consider $L_i = \{p_1,\dots,p_l\}$ be the set of any l coordinates locations in the i^{th} block of all codewords of C. Puncturing C on L_i consists on deleting entries of the i^{th} block of each codeword in C at locations in the set L_i.*

Definition VII.2. *Let C be an $[n,k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\dots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$), and let consider $L = \{p_1,\dots,p_l\}$, the set of any l block locations. Puncturing C on L consists on deleting blocks from each codeword in C at locations in the set L.*

According to Definition VII.1, puncturing an LEB code C on L_i consists on puncturing the i^{th} block of each codeword of C. However, for the Definition VII.2, puncture C is the fact of removing l blocks from a generator matrix of C. We use Definition VII.2 to specify the the puncturing technique thereafter. Thus, puncturing a code C means that we have removed some blocks in a generator matrix of C. In the following, we denote by C_p the resulting set after puncturing an LEB code C.

Lemma VII.3. *Let C be an $[n,k,d]_q$ LEB code over $\mathbb{F}_q$ of type $\pi = [n_1]\dots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$), and let consider $L = \{p_1,\dots,p_l\}$, the set of any l block locations. Then, the obtained set C_p after puncturing C on L, is a Linear error-block code of length $n_p = n - \sum_{i=1}^{l} n_{p_i}$ and of type*

$$\pi_p = [n_1]\dots[n_{p_1-1}][n_{p_1+1}]\dots[n_{p_2-1}][n_{p_2+1}]\dots[n_{p_l-1}]$$

$[n_{p_l+1}]\dots[n_s]$.

To prove this lemma, we consider the case when the set L contains one component. The general case yields similarly.

Proof: Let C be an LEB code satisfying conditions of Lemma VII.3, and i an integer such that $1 \leq i \leq s$. Let C_p be the set obtained by puncturing C on the i^{th} block. Clearly, $(C_p,+)$ is an abelian group. Let $x = (x_1,\dots,x_s)$ and $y = (y_1,\dots,y_s)$ two codewords in C, then for all $\lambda \in \mathbb{F}_q$, $x + \lambda y = (x_1 + \lambda y_1,\dots,x_s\lambda y_s) \in C$. Besides, $\hat{x} = (x_1,\dots,x_{i-1},x_{i+1},\dots,x_s)$ and $\hat{y} = (y_1,\dots,y_{i-1},y_{i+1},\dots,y_s)$ are in C_p, and we have also $\hat{x} + \lambda\hat{y} = (x_1 + \lambda y_1,\dots,x_{i-1} + \lambda y_{i-1},x_{i+1} + \lambda y_{i+1},\dots,x_s\lambda y_s) \in C_p$. By construction of C_p, C and

C_p have the same neutral element for the usual multiplication low. Therefore, C_p is an $\mathbb{F}_q$-linear subspace of $V_p = \mathbb{F}_q^{n_1} \oplus \ldots \oplus \mathbb{F}_q^{n_{i-1}} \oplus \mathbb{F}_q^{n_{i+1}} \oplus \ldots \oplus \mathbb{F}_q^{n_s}$ of length $n_p = n - n_i$, and since we have deleted the i^{th} block from each codeword in C, then C_p is an LEB code of type $\pi_p = [n_1] \ldots [n_{i-1}][n_{i+1}] \ldots [n_s]$. ■

Theorem VII.4. *Let C be an $[n, k, d]_q$ LEB code of type $\pi = [n_1] \ldots [n_s]$ where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \ldots \geq n_s \geq 1$, and let consider $L = \{i\}$ the set of one block locations. let C_p be the $[n_p, k_p, d_p]_q$ code obtained from puncturing C on L. Then, we have the following:*

1) *When $d = 1$, if there is no codeword in C of minimumn π-weight 1 whose i^{th} block is not nul, then $d_p = 1$ and $k_p = k$. Otherwise, if $k > 1$, then C_p is an $[n - n_i, k - 1, d_p \geq 1]_q$ LEB code of type $\pi_p = [n_1] \ldots [n_{i-1}][n_{i+1}] \ldots [n_s]$.*
2) *When $d > 1$, if there is a minimum π-weight whose i^{th} block is not null, then $d_p = d - 1$. Otherwise, $d_p = d$.*

This means that $d_p \geq d - 1$ and $k_p \geq k - 1$.

Proof: Let C and C_p be two LEB codes satisfying conditions of Theorem VII.4. Therefore, when $d = 1$, suppose that there exists a codeword $c \in C$ of minimum π-distance 1 whose i^{th} block is not null. Then, by removing the i^{th} block of c we will get a codeword of C_p which is zero in all blocks and of length $n - n_i$. Thus, the minimum π-distance d_p of C_p is at least d. Besides, $k_p = k - 1$. In fact, C contains q^k codewords and the only way that C_p could contain fewer codewords is when two codewords of C agree in all blocks but not in the i^{th} block. Now, if there is no codeword in C of minimumn π-weight 1 whose i^{th} block is not nul, then $d_p = 1$ and 1 is proven. Using the same idea of 1 we can prove the second statement. ■

Remark VII.5. If G is a generator matrix for C satisfying conditions of Theorem VII.4, then a generator matrix for C_p satisfying the same conditions as C is obtained from G by deleting the i^{th} block (and omitting a zero or duplicate a row that may occur).

Lemma VII.6. *Let C be an $[n, k, d]$ LEB code satisfying conditions of Lemma VII.3, $L = \{p_1, \ldots, p_l\}$ be the set of any l block locations, and let C_p be the $[n_p, k_p, d_p]_q$ code obtained from puncturing C on L. C_p is an $[n_p, k_p, d_p]$ LEB code with $k_p \geq k - l$ and $d_p \geq d - l$.*

We use induction reasoning (an induction on l) to prove this theorem as shown as follows.

Proof: Assuming conditions of Theorem VII.6. For $l = 1$, according to Theorem VII.4, $d_p \geq d-1$ and $k_p \geq k-1$. Let l be an integer ≥ 1, and assume that $k_p \geq k-l$ and $d_p \geq d-l$. Let $L' = L \cup \{p_{l+1}\}$ be a set of $l+1$ block locations and C'_p be the $[n'_p, k'_p, d'_p]$ LEB code obtained from puncturing C on L'. Let us prove that $k'_p \geq k-l-1$ and $d'_p \geq d-l-1$. Since C_p is the code obtained after puncturing C on L, then by the recurrence hypothesis we have $k_p \geq k - l$ and $d_p \geq d - l$. Let us now puncture C_p on the $(p_{l+1})^{th}$ block. Then, the obtained LEB code is exactly C'_p and according to Theorem VII.4, we have $k'_p \geq k_p - l$ and $d'_p \geq d_p - l$. Therefore $k'_p \geq k - l - 1$ and $d'_p \geq d - l - 1$, and by induction we deduce that $k_p \geq k - l$ and $d_p \geq d - l$. ■

Example VII.7. *Let C be the $[8, 2, 3]_2$ LEB code of type $\pi = [3][2][2][1]$ and defined by $C = \{000 \mid 00 \mid 00 \mid 0, 101 \mid 01 \mid 10 \mid 1, 100 \mid 00 \mid 01 \mid 1, 001 \mid 01 \mid 11 \mid 0\}$, and let $L = \{2, 4\}$. Then, the obtained code after puncturing C on L is an $[5, 2, 2]_2$ LEB code of type $\pi_p = [3][2]$ and defined by $C_p = \{000 \mid 00, 101 \mid 10, 100 \mid 01, 001 \mid 11\}$.*

Lemma VII.8. *Assuming conditions of Theorem VII.6 hold and that $d > 1$. When puncturing C on L, the deleted blocks of each codeword can be also viewed as vectors. So let S be the set of vectors deleted in the puncturing technique. Then, S is also an LEB and $d_p = d - d_{\pi'}(S)$ where $d_{\pi'}(S)$ is the minimum π-distance of S and $\pi' = [n_{p_1}] \ldots [n_{p_l}]$.*

Proof: Easy to proof, just noticing that S is exactly the code obtained from the puncturing C on C_L^E the complement of L in C (where $E = \{1, \ldots, s\}$), and then applying Theorems VII.4 and VII.6. ■

Example VII.9. *Continuing with the Example VII.7, we have $S = \{00 \mid 0, 01 \mid 1, 00 \mid 1, 01 \mid 0\}$ and $d_{\pi'}(S) = 2$ where $\pi' = [2][1]$. Therefore, $d_p = d - d_{\pi'}(S) = 1$.*

B. Shortening LEB Codes

In the following, we define the shortening technique for the LEB case, and we give some properties of a shortened code.

Definition VII.10. *Let C and L be as defined in Definition VII.2. Then the shortening operation on C at block locations in the set L consists of two steps. The first one, consider the set W of codewords in C that have zeros at the locations in the set L. The second one, the puncturing operation is performed on W at block locations in the set L.*

Remark VII.11. The code obtained after the above mentioned shortening operation is an LEB code of length $n - \sum_{i=1}^{l} n_{p_i}$, called the shortened code and denoted by C_s.

Example VII.12. *Let C be the $[9, 3, 1]$ binary LEB code with generator matrix*

$$G = \left(\begin{array}{cccc|ccc|cc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{array} \right).$$

Let $L = \{3\}$. A Generator matrix for the shortened code C_s is

$$G_s = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right).$$

Theorem VII.13. *Let C and L be as defined in Definition VII.2. and Let C_p and C_s are respectively the resulting codes after puncturing and shortening C. Then*

$$(C^{\perp})_s = (C_p)^{\perp} \tag{4}$$

and

$$(C^{\perp})_p = (C_s)^{\perp} \tag{5}$$

Proof: Let c be a codeword of $C^{\perp}$ which is 0 on L and c^* the codeword with the block locations in L removed. So $c^* \in (C^{\perp})_s$. If $x \in C$, then $0 = x.c = x^*.c^*$, where x^* is the codeword x punctured on L. Thus $(C^{\perp})_s \subseteq (C_p)^{\perp}$. Any vector $c \in (C_p)^{\perp}$ can be extended to a vector c' by inserting $0s$ in the block positions of L. If $x \in C$, puncture x on L to obtain x^*. As $0 = x^*.c = x.c'$, $c \in (C_p)^{\perp}$. Thus

$(C^\perp)_s = (C_p)^\perp$. Replacing C by $C^\perp$ gives $(C^\perp)_p = (C_s)^\perp$. ■

Example VII.14. *Let C be an $[8,2,2]_2$ LEB codes of type $\pi = [3][2]^2[1]$ defined as follows:*
$C = \{000 \mid 00 \mid 00 \mid 0; 101 \mid 11 \mid 00 \mid 0; 000 \mid 00 \mid 01 \mid 1; 101 \mid 11 \mid 01 \mid 1\}$.

Let $i = 3$, the punctured and the shortened codes in the i^{th} block location are respectively the codes

$$C_p = \{000 \mid 00 \mid 0; 101 \mid 11 \mid 0; 000 \mid 00 \mid 1; 101 \mid 11 \mid 1\},$$

and

$$C_s = \{000 \mid 00 \mid 0; 101 \mid 11 \mid 0\}.$$

C. π-Weight Enumerators of Punctured and Shortened LEB Codes

The π-weight distribution of an LEB code obtained from a known LEB code by either puncturing or shortening techniques is in general not determined by the π-weight distribution of the original code. But, after adding some conformity conditions, thus, our original LEB code can determine the π-weight distribution of the punctured and shortened LEB codes. One of these conditions, is the homogeneity of an LEB code that we define bellow.

Definition VII.15 (Homogenous LEB Code)**.** *Let C be an $[n,k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\ldots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \ldots \geq n_s \geq 1$). Let M be a $q^k \times n$ matrix whose rows consisting on all codewords of C, and for $i = 1,\ldots,s$ such that $A_i(C) \neq 0$, let consider M_i, the sub-matrix of M, consisting of all codewords with π-weight i.*

C is said to be homogeneous if and only if all blocks of M_i have the same π-weight. (Note that to have the π-weight of a block we should take this block as a vector in blocks.)

Example VII.16. *The code of the Example VII.14, is a homogeneous LEB code. In fact, For*

$$M_0 = (000 \mid 00 \mid 00 \mid 0)$$

each block of M_0 is of π-weight 0. For

$$M_2 = \left(\begin{array}{c|c|c|c} 101 & 11 & 00 & 0 \\ 000 & 00 & 01 & 1 \end{array}\right),$$

each block of M_1 is of π-weight 1.

For

$$M_4 = (101 \mid 11 \mid 01 \mid 1),$$

each block of M_1 is of π-weight 1.

We have the following results:

Theorem VII.17. *Let C be a homogeneous $[n,k,d>1]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\ldots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \ldots \geq n_s \geq 1$). Let C_p and C_s respectively, the obtained LEB codes after puncturing C in the i^{th} block location. Then, for $i = 1,\ldots,s-1$ we have:*

1) $A_i(C_p) = \frac{s-i}{s}A_i(C) + \frac{i+1}{s}A_{i+1}(C)$
2) $A_i(C_s) = \frac{s-i}{s}A_i(C)$

Proof: Let C be a homogeneous $[n,k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\ldots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \ldots \geq n_s \geq 1$). Let C_p and C_s respectively, the obtained LEB codes after puncturing C in the i^{th} block location. Let $1 \leq i \leq s-1$, then a vector of π-weight i in C_p comes either from a vector of π-weight i in C with a zero in the punctured block, or a vector of π-weight $i+1$ in C with a nonzero block in the punctured block; as $d > 1$, then no vector in C_p could be found in both ways. On the other hand, the number of nonzero blocks in all rows of M_i is $sw_{\pi,i} = iA_i(C)$ where $w_{\pi,i}$ is the π-weight of a block of M_i. Since C is homogeneous, then the π-weight is independent of the block, and thus $w_{\pi,i} = \frac{i}{s}A_i$. Therefore, M_i has $\frac{s-i}{s}A_i(C)$ null block. Hence, 1) holds. Since, a vector of π-weight i in C_s comes from a vector of π-weight i in C with a zero on the shortened block, then 2) is yield. ■

Example VII.18. *Continuing with the Example VII.16, we have $s = 4$, $A_0(C) = 1$, $A_1(C) = 0$, $A_2(C) = 2$ and $A_4(C) = 1$, and*

$$\begin{aligned} A_0(C_p) &= \frac{s-0}{s}A_0(C) + \frac{0+1}{s}A_{0+1}(C) \\ &= 1, \end{aligned}$$

$$\begin{aligned} A_1(C_p) &= \frac{s-1}{s}A_1(C) + \frac{1+1}{s}A_{1+1}(C) \\ &= 1, \end{aligned}$$

$$\begin{aligned} A_2(C_p) &= \frac{s-2}{s}A_2(C) + \frac{2+1}{s}A_{2+1}(C) \\ &= 1, \end{aligned}$$

and

$$\begin{aligned} A_3(C_p) &= \frac{s-3}{s}A_3(C) + \frac{3+1}{s}A_{3+1}(C) \\ &= 1. \end{aligned}$$

we have also

$$\begin{aligned} A_0(C_s) &= \frac{s-0}{s}A_0(C) \\ &= 1, \end{aligned}$$

$$\begin{aligned} A_1(C_s) &= \frac{s-1}{s}A_1(C) \\ &= 0, \end{aligned}$$

$$\begin{aligned} A_2(C_s) &= \frac{s-2}{s}A_2(C) \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} A_3(C_s) &= \frac{s-3}{s}A_3(C) \\ &= 0. \end{aligned}$$

VIII. Conclusion

In this work, we aimed to extend the notion of π-weight enumerator to the LEB case, define its properties and determine the π-weight distribution of some families of LEB codes.

Firstly, thanks to the MacWilliams Identity, we have given a simple formula to the π-weight enumerator polynomial of both Hamming and simplex LEB codes.

Secondly, we have studied the notion of π-weight enumerator for the cosets of an LEB code, and we have proven that some cosets have uniquely determined distributions. We have also proven that when the weight distribution of the cosets is known, and that the dimension of the LEB code is increased by one, the new resulting π-weight is explicitly determined.

Thirdly, we have shown that the π-weight enumerator of the code obtained from the direct sum of two LEB codes, is the multiplication of the respective π-weight enumerators of these two codes.

Finally, we have defined the puncturing and shortening techniques for LEB codes, we have given the structure of the resulting codes, then, we have studied the π-distribution of punctured and shortened LEB codes.

Forthcoming work involves determining the π-weight enumerator polynomial of some other families of LEB codes scu as the family of LEB π-constacyclic codes.

REFERENCES

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

[2] M. F. M.M.S. Alves, L. Panek, "Error-block codes and poset metrics," *Advances in Mathematics of Communications*, vol. 2, no. 1, pp. 95–111, 2008.

[3] R. Dariti and E. M. Souidi, "Packing and covering radii of linear error block codes," *International Journal of Mathematical Sciences*, vol. 57, pp. 13–17, 2013.

[4] P. Udomkavanich and S. Jitman, "Bounds and modifications on linear error-block codes." *International Mathematical Forum*, vol. 5, pp. 35–50, 2010.

[5] R. Dariti and E. M. Souidi, "New families of perfect linear error-block codes," *International Journal of Information and Coding Theory*, vol. 2, no. 2, pp. 84–95, 2013.

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

[7] S. Belabssir, E. B. Ayebie, and E. M. Souidi, "Perfect, Hamming and simplex linear error-block codes with minimum p-distance 3," ser. *Lecture Notes in Computer Science, C. Carlet, S. Guilley, A. Nitaj, and E. M. Souidi, Eds.*, vol. 11445. Springer, 2019, pp. 288–306. https://doi.org/10.1007/978-3-030-16458-4 17

[8] Dariti, R., "Linear error-block codes and applications", Thèse de Doctorat, Université Mohammed V-Agdal, Faculté des Sciences, 2012.

[9] Belabssir, S. and Sahlal, N. , "Tensor Product And Linear Error Block Codes", *IAENG International Journal of Applied Mathematics*, vol 51, no. 2, pp. $279-283$, 2021.

[10] F. J. MacWilliams, "A theorem on the distribution of weight in a systematic code", *The Bell System Technical Journal*, vol 42, no. 1, 1963, pp. $79-94$.

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

[12] R. Dariti and E. M. Souidi. An application of linear error-block codes in steganography. International Journal of Digital Information and Wireless Communications, 1:426–433, 2012.

[13] Rabiî Dariti and El Mamoun Souidi. Improving code-based steganography with linear error-block codes. Communications in Computer and Information Science, Springer Berlin Heidelberg, 189:310–321, 2011. https://doi.org/10.1109/TIT.1978.1055873.