World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:7, No:4, 2013

Packing and Covering Radii of Linear Error-Block Codes

Rabiî DARITI and El Mamoun SOUIDI

Abstract—Linear error-block codes are a natural generalization of linear error correcting codes. The purpose of this paper is to generalize some results on the packing and the covering radii to the error-block case. We study their properties when a code undergoes some specific modifications and combinations with another code. We give a few bounds on the packing and the covering radii of these codes.

Keywords—Linear error-block codes, π-distance, Correction capacity, Packing radius, Covering radius.

I. Introduction

Linear error-block (LEB) codes were introduced in [1]. Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. The space $\mathbb{F}_q^n$ is considered as a direct sum of spaces $\mathbb{F}_q^{n_i}$ where $n = \sum_{i=1}^{s} n_i$. The vectors in $\mathbb{F}_q^n$ are seen as a concatenation of s blocks $v = (v_1, v_2, ..., v_s)$ where $v_i \in \mathbb{F}_q^{n_i}$. Any change that happens inside a block causes a single error in the vector regardless to its magnitude. Classical linear error correcting codes are a special family of LEB codes for which $n_i = 1$ for $i = 1, 2, ..., s$.

The packing radius t of a code $\mathcal{C}$ is defined as the biggest integer for which each vector of the space is within distance t of at most one codeword. It is directly related to the minimum distance d (the minimal distance between two different codewords) by the formula $t = \lfloor \frac{d-1}{2} \rfloor$.

The covering radius ρ of a code $\mathcal{C}$ is defined as the smallest integer such that all vectors of the space $\mathbb{F}_q^n$ are within distance at most ρ of some codeword. It is the maximum distance from any vector in $\mathbb{F}_q$ to the code.

There exist further equivalent definitions for the covering radius. It can be defined as the weight of a coset leader of greatest weight. Also, if H is any parity check matrix for $\mathcal{C}$, then ρ is the least integer such that every column vector of $\mathbb{F}_q^{n-k}$ (syndrome) is a sum of some ρ or fewer columns of H. The least integer w allowing such a sum for the syndrome s is the weight of a leader of the coset associated with s.

In this paper, we extend the definitions of packing and covering radii to linear error-block codes. Some proofs are omitted when the results can be found by direct analogy to the classical error correcting codes. In the other results, we study the properties of the packing and covering radii when a LEB code is modified by extension or puncture, or by some combination with another LEB code.

This paper is organized as follows. In Section II we recall basic definitions. Section III introduces the π-packing and the π-covering radii, and gives some of their essential properties. Sections IV and V study some construction of LEB codes from other LEB codes and give the bounds yielded on the π-packing and the π-covering radii. They involve respectively lower bounds and upper bounds. Perspective of this work is given in Section VI.

Rabiî DARITI and El Mamoun SOUIDI are with the Mathematics, Informatics and Applications Laboratory, Faculty of Science of Rabat, Mohammed V Agdal University, BP 1014 - Rabat - Morocco.

II. Preliminaries

A composition π of a positive integer n is given by $n = l_1m_1 + l_2m_2 + \cdots + l_rm_r$, where $r, l_1, l_2, \ldots, l_r, m_1, m_2, \ldots, m_r$ are integers ≥ 1, and is denoted

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

If moreover $m_1 > m_2 > \cdots > m_r \geq 1$ then π is called a partition.
If $\pi_1 = [n_1^1]...[n_{s_1}^1]$ and $\pi_2 = [n_1^2]...[n_{s_2}^2]$ are compositions of two integers n^1 and n^2, then we note $\pi = \pi_1\pi_2$ the composition of $n^1 + n^2$ given by

$$\pi = \pi_1\pi_2 = [n_1^1]\ldots[n_{s_1}^1][n_1^2]\ldots[n_{s_2}^2].$$

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Let $s, n_1, n_2, \ldots, n_s$ be the non negative integers given by a partition $\pi = [m_1]^{l_1}[m_2]^{l_2}\ldots[m_r]^{l_r}$ as follows

$$\begin{gathered} s = l_1 + \cdots + l_r, \\ n_1 = n_2 = \cdots = n_{l_1} = m_1 \\ n_{l_1+1} = n_{l_1+2} = \cdots = n_{l_1+l_2} = m_2 \\ \vdots \\ n_{l_1+\cdots+l_{r-1}+1} = n_{l_1+\cdots+l_{r-1}+2} = \cdots = n_s = m_r \end{gathered}$$

Let $V_i = \mathbb{F}_q^{n_i}$ $(1 \leq i \leq s)$ and $V_\pi = V_1 \oplus V_2 \oplus \ldots \oplus V_s = \mathbb{F}_q^n$. Each vector $v \in V_\pi$ can be written uniquely as $v = (v_1, \ldots, v_s)$, $v_i \in V_i$ $(1 \leq i \leq s)$. For any $u = (u_1, \ldots, u_s)$ and $v = (v_1, \ldots, v_s)$ in V_π, the π-weight $w_\pi(u)$ of u and the π-distance $d_\pi(u, v)$ between u and v are defined by

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

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

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

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

A LEB code is completely defined by a generator matrix or a parity check matrix, as these are defined in the classical case [9].

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

A LEB code with a composition type is equivalent to some LEB code with a partition type through a block permutation.

Up to date publications on LEB codes involve determining and constructing optimal codes [1], [2], [3], [4]. Also, the authors have introduced a standard decoding algorithm adapted to LEB codes [5]. Feng et al. claimed in [1] that LEB codes have application in experimental design, high-dimensional numerical integration and cryptography. The authors introduced in [6] a steganographic protocol based on LEB codes. Their construction advantages utilization of LEB codes with good covering properties, ideally perfect codes. So far, neither covering nor packing properties of LEB codes have been thoroughly studied. For classical codes, a rich survey is given in [7].

III. Packing and covering radii

It is worth noting that it is useless to consider LEB codes in the Binary Symmetric Channel model, since the crossover probability (the probability for a bit to be altered) would differ from a block to another. The most suitable model supposes that the crossover probability is the same for each block regardless to the number of bits it contains. In this model, a received word is corrected by determining the codeword which is within the least π-distance to it.

In the literature, there are many definitions that can analogously be generalized to the error-block case. We state in the following some definitions and characteristics of the π-packing and the π-covering radii.

Definition 1 (The π-packing radius): The π-packing radius of a code is the largest radius of spheres centered at codewords such that the spheres are pairwise disjoint.

Let $\mathcal{C}$ be an $[n, k, d_\pi]$ LEB code of type π and π-packing radius t_π. The following results come straightforward.

Proposition 1:

(i) The code $\mathcal{C}$ corrects all errors of π-weight t_π or less.

(ii) The π-packing radius of $\mathcal{C}$ equals

$$t_\pi = \lfloor (d_\pi - 1)/2 \rfloor. \tag{1}$$

The latter equation shows that the characteristics of the π-packing radius can be deuced from those of the minimum π-distance. Let H be a parity check matrix of $\mathcal{C}$ written in the block form as $H = [H_1, H_2, \ldots, H_s]$ where H_i is an $(n-k) \times n_i$ matrix corresponding to the i^{th} block of π for $i = 1, 2, \ldots, s$. The following results are also generalized by direct analogy from the classical case.

Proposition 2:

- The π-packing radius t_π is the biggest integer such that all coset leaders of π-weight t_π or less are unique.
- The minimum π-distance of $\mathcal{C}$ is d_π if and only if any columns issued from any $d_\pi - 1$ blocks of H are linearly independent and there exist columns issued from d_π blocks that are linearly dependent.

Definition 2 (The π-covering radius): The π-covering radius of a LEB code $\mathcal{C}$ is the smallest radius of spheres centered at codewords such that the space V_π is the union of these spheres.

To say V_π is the union of spheres of radius ρ_π centered at codewords means that for all $x \in V_\pi$ there exists a sphere, of radius ρ_π centered at some codeword, which contains x. This gives the following.

Proposition 3: The π-covering radius of a LEB code $\mathcal{C}$ is the smallest integer ρ_π such that all vectors of the space V_π are within π-distance at most ρ_π of some codeword of $\mathcal{C}$. It is also the maximum π-distance from any vector in V_π to the code. i.e.

$$\rho_\pi = max\{d_\pi(x, \mathcal{C}), x \in V_\pi\}. \tag{2}$$

Proposition 4: The π-covering radius is the π-weight of a coset leader of greatest π-weight.

This can be seen by noting that the π-distance between a V_π vector x and the code $\mathcal{C}$ is the π-weight of the leader of the coset $x + \mathcal{C}$. From Equation 2 it follows

$$\rho_\pi = \max_{x \in V_\pi}\{w_\pi(e), e \text{ is a coset leader of } x + \mathcal{C}\}. \tag{3}$$

The following result is yielded by noting that any syndrome (vector of $\mathbb{F}_q^{n-k}$) can be written as product of H and some coset leader of $\mathcal{C}$.

Proposition 5: If H is any parity check matrix for $\mathcal{C}$, then ρ_π is the least integer such that every syndrome is a sum of columns of some ρ_π or fewer blocks of H.

An $[n, k]_q$ LEB code of type π has q^k codewords. Although the type does not affect the cardinality, it is a major factor in the topological properties of the code. This can be clearly seen within the sphere packing and the sphere covering problems. We generalize the sphere packing problem as follows. "Given a length n, a type π, a vector space V_π and a radius t_π, determine the maximum number of pairwise disjoint balls of π-radius t_π in the space V_π". In an equivalent statement, "Find the maximum cardinality of a code in V_π with length n and π-packing radius t_π".

The sphere covering problem is generalized by the following statement."Given a length n, a type π, a vector space V_π and a radius ρ_π, determine the minimum number of balls of π-radius ρ_π which cover the whole space V_π". An equivalent statement is "Find the minimum cardinality of a code in V_π with length n and π-covering radius ρ_π".

Now by finding out the cardinality of a ball of radius r in V_π, we determine the sphere packing and the sphere covering bounds for LEB codes. Let b_π be cardinality of a ball of radius r. Combinatoric calculations show that

$$b_\pi(r) = 1 + \sum_{\alpha=1}^{r} \sum_{1 \le i_1 < \cdots < i_\alpha \le s} (q^{n_{i_1}} - 1) \ldots (q^{n_{i_\alpha}} - 1). \tag{4}$$

Proposition 6: For any q-ary $[n, k]$ LEB code of packing radius t and covering radius ρ

$$b_\pi(t) \le q^{n-k} \le b_\pi(\rho), \tag{5}$$

where $b_\pi(.)$ is given by Equation 4.

The left side inequation is called the Hamming bound. Further to it, there was given in [1] another Hamming bound that holds only for LEB codes of even minimum π-distance.

Proposition 7: Let $\mathcal{C}$ be an $[n,k,d]_q$ LEB code of type $\pi = [n_1],[n_2],...,[n_s]$, $n_1 \geq n_2 \geq \cdots \geq n_s$ where $d = 2r$, $r \geq 1$. We have the following Hamming bound

$$q^{n-k} \geq b'_\pi(r), \tag{6}$$

where

$$b'_\pi(r) = q^{n_1}\left[1 + \sum_{\alpha=1}^{r-1} \sum_{2\leq i_1<\cdots<i_\alpha\leq s} (q^{n_{i_1}}-1)\ldots(q^{n_{i_\alpha}}-1)\right].$$

The advantage of this bound is that it is more precise than the usual Hamming bound, since $b'_\pi(r) \geq b_\pi(r)$. Actually, $b'_\pi(r)$ is the cardinality of any set $B'_\pi(c,r)$ defined for a codeword c and a positif integer $r > 0$ by

$$B'_\pi(c,r) = B_\pi(c,r-1) \cup \{x \in V / d_\pi(c,x) = r \text{ and } x_1 \neq c_1\}.$$

This gives the possibility to a LEB code to correct up to $d/2$ errors if d is even. However, we cannot consider $t = d/2$ as a sphere packing radius since the sets B' are not balls, and the balls of radius $d/2$ are not disjoint.

A particularly interesting solution to the sphere packing and the sphere covering problems is when the balls of radius, say r, are at the same time pairwise disjoint and their union covers the whole space V_π. The codes verifying this property are called perfect codes; their packing radius is equal to their covering radius. If a code is not perfect, then either the balls of radius ρ_π are not pairwise disjoint or the balls of radius t_π do not cover the whole space V_π. As a direct result of Proposition 6 we have the following.

Proposition 8: If t_π is the π-packing radius and ρ_π is the covering radius of an $[n,k]$ code of type π, then $t_\pi \leq \rho_\pi$.

Definition 3: Let n be a positif integer and Π_n be the set of all possible partitions of n. We define a partial order relation "$\preceq$" between two elements $\pi = [n_1][n_2]...[n_s]$ and $\pi' = [n'_1][n'_2]...[n'_{s'}]$ of Π_n as follows,
$\pi \preceq \pi'$ if and only if there exists an ordered sequence $(l_i)_{0\leq i\leq s'}$ such that for all $i = 1,2,...,s'$ we have

$$n'_i = \sum_{j=l_{i-1}+1}^{l_i} n_j \text{ with } l_0 = 0 \text{ and } l_{s'} = s.$$

This means each component of π' is a union of one or more consecutive components of π.

Corollary 1: We keep the notations of Definition 3. We have the following results

- $\forall \pi \in \Pi_n$; $[1]^n \preceq \pi \preceq [n]$.
- $\pi \preceq \pi'$ if and only if $\pi = \pi_1\pi_2...\pi_{s'}$ where $\pi_i \in \Pi_{n'_i}$, $i = 1,...,s'$. i.e. each π_i is a partition of n'_i. π is a concatenation of partitions of n'_i.
- If $\pi \preceq \pi'$ then $t_{\pi'} \leq t_\pi$ and $\rho_{\pi'} \leq \rho_\pi$.

Proof: The first and the second assertions are direct results of Definition 3. Let x and y be two codewords of $\mathcal{C}$. If $\pi \preceq \pi'$ then $d_{\pi'}(x,y) \leq d_\pi(x,y)$. Definition 2 proves the third assertion. ■

In the remainder of this paper, if a partition π is clear from the context, we omit the symbol π when referring to code parameters. We shall denote the π-covering radius, the π-packing radius and the π-minimum distance as ρ, t and d respectively. For simplicity we focus our study on the binary case. In the following, we show how the π-packing and the π-covering radii are related to the type of the code when the length and the dimension are fixed.

IV. Lower bounds

For the next two sections, we adopt the following notation. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be, respectively, an $[n_1,k_1,d_1]$ LEB code of type π_1, packing radius t_1, covering radius ρ_1 and generator matrix G_1, and an $[n_2,k_2,d_2]$ LEB code of type π_2, packing radius t_2, covering radius ρ_2 and generator matrix G_2. Concatenation of partitions π_1 and π_2 is in general a composition, denoted by $\pi = \pi_1\pi_2$ (see Section II).

In this section, we study lower bounds on the π-packing and the π-covering radii of a LEB code which is constructed from other LEB codes. Note that these constructions can be made, in a particular case, using classical error correcting codes.

A. The direct sum

Let $\mathcal{C}$ be the code defined by

$$\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 = \{(c_1,c_2)/c_1 \in \mathcal{C}_1 \text{ and } c_2 \in \mathcal{C}_2\}$$

Proposition 9: The code $\mathcal{C}$ is an $[n_1+n_2, k_1+k_2]$ code of type $\pi = \pi_1\pi_2$ and it has packing radius

$$t = min(t_1,t_2) \tag{7}$$

and covering radius

$$\rho = \rho_1 + \rho_2. \tag{8}$$

A generator matrix of $\mathcal{C}$ has the form

$$\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}.$$

Proof: Codewords of $\mathcal{C}$ have the form (c_1,c_2). Let e_1 and e_2 be two codewords of minimum weight of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. So $(e_1,0)$ and $(0,e_2)$ are codewords of $\mathcal{C}$. Hence $d = min(d_1,d_2)$. If l_1 and l_2 are two coset leaders of maximum weight of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively, then a maximum weight coset leader of $\mathcal{C}$ is (l_1,l_2). ■

B. The concatenation lower bound

Suppose we have $k_1 > k_2$, and let $\hat{G}_2$ be the $k_1 \times n_2$ matrix $\begin{bmatrix} G_2 \\ 0 \end{bmatrix}$ where 0 is the $(k_1-k_2)\times n_2$ null matrix.

Proposition 10: The code $\mathcal{C}$ defined by the generator matrix

$$G = [G_1\hat{G}_2]$$

is an $[n_1+n_2, k_1]$ code of type $\pi = \pi_1\pi_2$ and it has packing radius

$$t \geq t_1 \tag{9}$$

and covering radius

$$\rho \geq \rho_1 + \rho_2. \tag{10}$$

Proof: Codewords of $\mathcal{C}$ have the form $c = (c_1, c_2)$ where $c_1 \in \mathcal{C}_1$ and $c_2 \in \mathcal{C}_2$. If c is non null then c_1 cannot be null as G_1 is of rank k_1. Hence $w_\pi(c) = w_{\pi_1}(c_1) + w_{\pi_2}(c_2) \geq d_1$. Let l_1 and l_2 be two coset leaders of maximum weight of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. Then (l_1, l_2) is a coset leader of $\mathcal{C}$ of weight $\rho_1 + \rho_2$. ∎

C. The $(u, u + v)$ construction

Assume that $n_1 = n_2$, $\pi_1 = \pi_2$ and $\mathcal{C}_2 \subseteq \mathcal{C}_1$. Let $\mathcal{C}$ be the code defined by

$$\mathcal{C} = \{(u, u + v)/u \in \mathcal{C}_1, v \in \mathcal{C}_2\}.$$

Proposition 11: The code $\mathcal{C}$ is a $[2n_1, k_1 + k_2]$ code of type $\pi = \pi_1 = \pi_2$ and it has packing radius

$$t = min(2t_1, t_2) \tag{11}$$

and covering radius

$$\rho \geq 2\rho_1. \tag{12}$$

A generator matrix of $\mathcal{C}$ has the form

$$\begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}.$$

Proof: Let e_1 be a codeword of minimum weight of $\mathcal{C}_1$. Then (e_1, e_1) is a codeword of $\mathcal{C}$ of weight $2d_1$. Let e_2 be a codeword of minimum weight of $\mathcal{C}_2$. Then $(0, e_2)$ is a codeword of $\mathcal{C}$ of weight d_2. Hence $d = min(2d_1, d_2)$ this implies 11. Let l be a coset leader of $\mathcal{C}_1$ of weight ρ_1. Then (l, l) is a coset leader of $\mathcal{C}$ with π-weight $2\rho_1$. ∎

D. The supercode lower bound

Proposition 12: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two codes of length n and type π such that $\mathcal{C}_2 \subset \mathcal{C}_1$. We define two quantities associated with these codes:

$$m(\mathcal{C}_1, \mathcal{C}_2) = \min\{w_\pi(x), x \in \mathcal{C}_1 - \mathcal{C}_2\},$$

$$M(\mathcal{C}_1, \mathcal{C}_2) = \max_{x \in \mathcal{C}_1} \min\{w_\pi(x - y), y \in \mathcal{C}_2\}.$$

Then we have the following inequalities

$$\rho_2 \geq M(\mathcal{C}_1, \mathcal{C}_2) \geq m(\mathcal{C}_1, \mathcal{C}_2) \geq d_1. \tag{13}$$

Proof: ρ_2 is defined by $\rho_2 = \max\{w_\pi(x + \mathcal{C}_2), x \in \mathbb{F}_2^n\}$. Since $w_\pi(x + \mathcal{C}_2) = \min\{w_\pi(x + c_2), c_2 \in \mathcal{C}_2\}$, it follows $\rho_2 = \max_{x \in \mathbb{F}_2^n} \min_{c_2 \in \mathcal{C}_2}\{w_\pi(x + c_2)\}$. Hence

$$\rho_2 = M(\mathbb{F}_2^n, \mathcal{C}_2) \geq M(\mathcal{C}_1, \mathcal{C}_2).$$

This yields

$$\begin{aligned} m(\mathcal{C}_1, \mathcal{C}_2) &= \min\{d_\pi(c_1, c_2), c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2\} \\ &\geq \min\{d_\pi(c_1, x), c_1 \in \mathcal{C}_1, x \in \mathbb{F}_2^n\} = d_1. \end{aligned}$$

∎

E. Code lengthening

We can lengthen an $[n, k]$ LEB code of type $\pi_0 = [n_1][n_2]...[n_s]$ by adding some m new columns to its generator matrix $G = [G_1 G_2 ... G_s]$. This yields an $[n + m, k]$ code and modifies the type. Essentially there are two methods of lengthening a LEB code. We describe them in the following.

a) Lengthening a block: The columns are added to a block G_i of the generator matrix G. This increases the size of the i-th element of the partition, but the overall size of the partition (the integer s) remains unchanged. The produced code is of type $\pi = [n_1]...[n_i + m]...[n_s]$.

b) Inserting a block: In this case, the produced code is of type $\pi = [n_1]...[n_i][m][n_{i+1}]...[n_s]$. The size of the partition is now $s + 1$.

Proposition 13: The packing and the covering radii in each case are either unchanged or increased by 1. Combinations of these methods provide more lengthening situations. Each time a new block is modified (lengthened or inserted) the packing and the covering radii may be increased by 1 or remain unchanged.

V. Upper bounds

A. The Singleton and the redundancy bounds

A parity check matrix H of an $[n, k, d]$ LEB code has rank $n - k$, which means that there exist $n - k$ columns in H that are linearly independent. These columns are contained in at most $n - k$ blocks. By Proposition 2, the columns of the first $d - 1$ blocks are linearly independent. This proves the following bound which was first introduced in [1].

Proposition 14 (Singleton bound): An $[n, k, d]$ LEB code of type $\pi = [n_1][n_2] \ldots [n_s]$ verifies

$$n_1 + n_2 + \cdots + n_{d-1} \leq n - k. \tag{14}$$

This is an indirect bound on the packing radius. Also, by Proposition 5, every vector of length $n - k$ is a sum of columns of at most ρ blocks of H. This proves the following bound.

Proposition 15 (Redundancy bound): The covering radius ρ of any $[n, k]$ LEB code verifies

$$\rho < n - k. \tag{15}$$

We give in the following some bounds on the covering radius yielded by three constructions. We use the same notation as in Section IV.

B. The concatenation upper bound

Proposition 16: Let $\mathcal{C}$ be the concatenation of $\mathcal{C}_1$ and $\mathcal{C}_2$ as in Proposition IV-B. We have

$$\rho \leq \min(\rho_1 + n_2, \rho_2 + n_1). \tag{16}$$

Proof: Codewords of $\mathcal{C}$ have the form $c = (c_1, c_2)$. For all $x = (x_1, x_2) \in \mathbb{F}^{n_1} \oplus \mathbb{F}^{n_2}$ we have $d(x, c) = d(x_1, c_1) + d(x_2, c_2) \leq d(x_1, c_1) + n_2$. This yields $d(x, \mathcal{C}) \leq d(x_1, \mathcal{C}_1) + n_2$. Hence $\rho \leq \rho_1 + n_2$. Analogously we get $\rho \leq \rho_2 + n_1$ which yields the result. ∎

C. The supercode upper bound

Proposition 17: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two codes of length n and type π such that $\mathcal{C}_2 \subset \mathcal{C}_1$. We have

$$\rho_1 \leq \rho_2 + M(\mathcal{C}_1, \mathcal{C}_2). \tag{17}$$

Proof: Let $x \in \mathbb{F}_2^n$ such that $d_\pi(x, \mathcal{C}_2) = \rho_2$. Let a be the closest codeword of $\mathcal{C}_1$ to x. We have $d_\pi(x, a) \leq \rho_1$. Let b be the closest codeword of $\mathcal{C}_2$ to a. We have $d_\pi(a, b) \leq M(\mathcal{C}_1, \mathcal{C}_2)$. Thus,

$$\begin{aligned} \rho_1 &\leq d_\pi(b, x) \\ &\leq d_\pi(a, x) + d_\pi(a, b) \\ &\leq \rho_2 + M(\mathcal{C}_1, \mathcal{C}_2). \end{aligned}$$

■

D. The $\rho_1 + \rho_2$ Bound

The following bound is the generalization of the bound appeared in [8].

Proposition 18: Let $\mathcal{C}$ be an $[n, k]$ code of type π, and assume that there exists a parity check matrix H of $\mathcal{C}$ in the form $H = [I_r D]$ where D is an $r \times k$ matrix of rank j and $r = n - k$. Define $\mathcal{C}_1$, as the $[k, k-j]$ code of type π_1 such that D is a parity check matrix, and let ρ_1 be the covering radius of $\mathcal{C}_1$. Define $\mathcal{C}_2$ as the $[r, j]$ code of type π_2 spanned by the columns of D, and let ρ_2 be its covering radius. Assume that $\pi = \pi_1 \pi_2$.

$$\rho \leq \rho_1 + \rho_2 \leq n - k. \tag{18}$$

Proof: If x is any syndrome, then it is at π_2-distance ρ_2 or less from some vector c_2 in $\mathcal{C}_2$. Thus $x = c_2 + y$, where y is the sum of columns of at most ρ_2 blocks of I_r. The set of all subsets of columns of D with sum c_2 corresponds to a coset of $\mathcal{C}_1$. Thus c_2 is the sum of columns of at most ρ_1 blocks of D accordingly to π_1. Therefore, x is the sum of at most $\rho_1 + \rho_2$ columns of H. For the right hand side, Proposition 15 yields $\rho_1 \leq j$ and $\rho_2 \leq r - j$. Thus $\rho_1 + \rho_2 \leq r = n - k$.

■

E. Code puncturing

With the same notations as Section IV-E, we give in the following two main ways of puncturing a LEB code.

c) Puncturing a block: The columns are removed from a block G_i. This decreases the size of the i-th element of the partition, but the overall size of the partition remains unchanged. The produced code is of type $\pi = [n_1]...[n_i - m]...[n_s]$.

d) Removing a block: This produces a code of type $\pi = [n_1]...[n_i][n_{i+1}]...[n_s]$ and of generator matrix $[G_1 G_2 ... G_{i-1} G_{i+1} ... G_s]$.

Proposition 19: The packing and the covering radii in each case is either unchanged or decreased by 1. Combinations of these methods provide more puncturing situations. Each time a new block is modified (punctured or removed) the packing and the covering radii may be decreased by 1 or remain unchanged.

VI. Perspective

We defined π-covering radius of linear error-block (LEB) codes. We studied various types of constructions and gave bounds on the covering radius. Forthcoming work involves determining bounds in the general construction of "Matrix product codes". In this case, the code is written as $C = [C_1 \dots C_M].A$ where $C_1, \dots, C_M$ are LEB codes of length n over $\mathbb{F}_q$ and A is an $M \times N$ matrix over $\mathbb{F}_q$.

References

[1] K. Feng, L. Xu and F.J. Hickernell: *Linear error-block codes*. Finite Fields Appl. 12, 638–652 (2006).
[2] S. Ling, F. Özbudak: *Constructions and bounds on linear error-block codes*. Designs, Codes and Cryptography. 45, 297–316 (2007).
[3] M.M.S. Alves, L. Panek, M. Firer: *Error-block codes and poset metrics*. Advances in Mathematics of Communications. Vol. 2, No. 1,95–111 (2008).
[4] R. Dariti, E. M. Souidi, *New Families of Perfect Linear Error-Block Codes*, International Journal of Information and Coding Theory. Accepted for publication (2012).
[5] R. Dariti, E. M. Souidi,*Cyclicity and Decoding of Linear Error-Block Codes*, Journal of Theoretical and Applied Information Technology, 25, No. 1 (2011).
[6] R. Dariti, E.M. Souidi, *Improving Code-Based Steganography with Linear Error-Block Codes*. Digital Information Processing and Communications, Communications in Computer and Information Science, International Conference, ICDIPC 2011, Ostrava, Czech Republic, July 7-9, 2011, Proceedings, Part II, Springer Berlin Heidelberg. 189, 310–321 (2011).
[7] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein: *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.
[8] H.F. Mattson: *An Upper Bound on Covering Radius*. Combinatorial Mathematics, Proceedings of the International Colloquium on Graph Theory and Combinatorics, North-Holland, 75, 453 – 458 (1983).
[9] W.C. Huffman, V. Pless: *Fundamentals of Error-Correcting Codes*. Cambridge University Press (2003).