Malaya Journal of Matematik, Vol. 9, No. 1, 399-401, 2021
https://doi.org/10.26637/MJM0901/0067

The q-ary intersecting for $(a,\ a+b)$ construction code

B. Rega[1]* and C. Durairajan[2]

Abstract
In this paper, we study the pairs of q-ary linear intersecting codes $C_i(n_i, k_i, d_i),\ i=1,2$, with the property that for any two non-zero codes have the intersecting supports. Some codes with high distances are shown to be intersecting.

Keywords
Intersecting codes, Self- complementary codes, Dual codes, Linearly independent codes.

AMS Subject Classification
94B05.

[1,2] *Department of Mathematics, Bharathidasan University, Tiruchirappalli - 620 024, Tamil Nadu, India.*
*Corresponding author: [1] boseregaramesh@bdu.ac.in; [2]cdurai66@bdu.ac.in
Article History: Received **20** December **2020**; Accepted **08** February **2021**
©2021 MJM.

Contents

1. Introduction

We consider a code $C \subseteq \mathbf{F_q}^n$, where $\mathbf{F_q}^n$ is the set of all codes of length n over $\mathbf{F_q}$. If q is a prime power, $\mathbf{F_q}$ will be the Galois field $\mathbf{GF(q)}$, otherwise, the set of integers modulo q. The Hamming distance $d(x,y)$ between two codewords $x,y \in \mathbf{F_q}^n$ is the number of co-ordinates where they differ. In 1975, Ian F. Blake[2] studied the linear codes over integer residue rings and these codes are analogs to Hamming, BCH and Reed-Solomon codes over finite fields. Linear codes with intersecting properties were first introduced by Miklos D. on his paper [10]. On the other hand, Cohen G. [3] introduced linear intersecting codes in such way that any pairs of binary linear codes C_1 and C_2 with the property that for any nonzero $c_1 \in C_1$ and $c_2 \in C_2$, there are co-ordinates in which both c_1 and c_2 are non-zero. Sloane N. J. A [11], presented the relation between the covering arrays and intersecting codes. Again, Cohen G. [4] studied the properties of intersecting codes and their applications in VLSI testing, derandomization, and defect correction, etc., and also constructing the t-independent families of vectors. Further, Ashikhmin A. et al. [1] presented the minimal vectors in binary linear codes that had several applications in linear secret sharing schemes and decoding algorithms. They also extended the minimal vectors to codes over rings. Encheva. S. B., et al. [8] developed the new construction of linear intersecting codes and they derived that intersecting codes are not self-complementary codes. Cohen. G et al.,[5] constructed the separating codes from the intersecting linear codes through feasible sets. Again Cohen. G et al., [6] presented the construction of $(2,2)$- separating codes from error-correcting codes and also derived their bounds. These codes have applications in several areas like technical diagnosis, automata synthesis, and claiming the authenticating ownership. The coalition of codes was studied through separating codes by Cohen G. et al.,[7] with the motivation of digital fingerprinting and some e-commerce applications. The outlines of this paper are as follows. Section 2 deals with some basic definitions and results and in Section 3, we present some properties of q-ary intersecting codes. Finally, in Section 4, we derive that the construction codes that are shown to be intersecting in the q-ary level.

2. Preliminaries

Consider the linear code C over the finite field $\mathbf{GF(q)}^n$. Assume that length n, dimension k, minimum distance d and the intersecting t is denoted by $[n,k,d,t]$. The generator matrix and weight distribution are denoted by G and $(W_i)_0^n$ respectively, where W_i denotes the number of codewords of weight i. If $x,y \in C$, then $x-y \in C$. Let us consider the minimum distance of C

$$\begin{aligned} d &= \min\{d(x,y) \mid x,y \in C \text{ and } x \neq y\} \\ &= \min\{w(x-y) \mid x,y \in C \text{ and } x \neq y\}. \end{aligned}$$

Since C is $\mathbb{Z}_q$-linear code and $x, y \in C$, $x-y \in C$. Since $x \neq y$, $\min\{w(x-y) \mid x,y \in C \text{ and } x \neq y\} = \min\{w(c) \mid c \in C \text{ and } c \neq 0\}$. Thus, the lemma follows.

Lemma 2.1. *In a linear code, the minimum distance is the same as the minimum weight.*

Let C be an q-ary linear code. Then, the $supp(C) = \{q$ such that $\exists(c_1, c_2, \cdots, c_n), c_q \neq 0\}$ and is denoted by $\chi(C)$.

The support weight $w_s(C)$ is defined as the cardinality of $|supp(C)|$. The t-intersecting for two codes C_1 and C_2 is the support of $|c_1 * c_2| \geq t$.

Example 2.2. *For* $q=4$, *the Code* $C = \{(0000, 1232, 2020, 3212\}$ *is a* $[4,3,2,2]$ *code.*

The code C is said to be self-complementary if $W_i = 1$. Note that the self-complementary codes are not intersecting.

Denote $B(n,d)$ is the greatest number of the codewords in any linear code of length n and distance d.

Proposition 2.3. *[3] If two linear codes* $C_1(n_1,k_1,d_1)$ *and* $C_2(n_2,k_2,d_2)$ *are r-intersecting, then* $k_1 \leq \log B(d_2,r)$ *and* $k_2 \leq \log B(d_1,r)$.

Proposition 2.4. *[10]* $[(a,a+b)$ *construction* $]$ *Let* C_i *be an* $[n,k_i,d_i]$ *linear q-ary code for* $i=1,2$. *Then, the code C defined by*

$$C = \{(a, a+b) \text{ such that } a \in C_1, b \in C_2\}$$

is a $[2n, k_1+k_2, \min(2d'_1, d'_2)]$ *linear q-ary code.*

Using the above results, we will arrive the following proposition.

3. Some properties of q-ary intersecting codes

Proposition 3.1. *If the two linear q-ary codes* $C_i(n_i,\ k_i,\ d_i)$, $i=1,2$ *are t-intersecting, then* k_1 *and* k_2 *satisfy the following estimates* $k_1 \leq \log_q B(d_2,t)$ *and* $k_2 \leq \log_q B(d_1,t)$

Proof. Assume that $c'_2 \in C_2$ and $|c'_2| = d_2$. Define the set $I_1 = \{n * c'_2$ such that $n \in C_1\}$. Construct the mapping f defined on C_1 such that $f(n) = n * c'_2$, where $n \in C_1$. The mapping is linear and injective, since the non-zero elements c_1 in $ker f$ would permit $c_1 * c'_2 = 0$, which is contradiction to C_1 intersecting C_2. Hence, $|I_1| = q^{k_1}$ and $\chi(c'_2) = d_2$. Therefore, I_1 is a (d_2, k_1, t) code. Similarly, we can also prove that the set $I_2 = \{n' * c_2$ such that $n' \in C_1,\ c_2 \in C_2\}$ is (d_1, k_2, t) code. □

Corollary 3.2. *Let* C_i, $i=1,2$ *be t-intersecting codes, then* $d_1 \geq k_2 + r - 1$ *and* $d_2 \geq k_1 + r - 1$.

4. Construction of intersecting codes

In this section, we present some results on the q-ary intersecting codes and $(a,\ a+b)$ construction of the code.

Proposition 4.1. *Assume* C_i, $i=1,2$ *be* $[n,\ k_i,\ d_i]$ *linear q-ary codes and the* $[a,\ a+b]$ *construction of the code* $C = [2n,\ k_1+k_2, \min(2d_1,\ d_2)]$ *is linear code. Then C is t-intersecting with* $t \geq 3d - \frac{w}{2}$.

Proof. If $c_1,\ c_2 \in C$ be two non-zero codewords. Let $x \in c_1$ and $y \in c_2$ such that $x \neq 0 \neq y$ with weight d. Consider

$$\begin{aligned} w(x,\ x+y) = w(x) + w(x+y) &\geq 2w(x) + w(y) - 2w(x \cap y) \\ &= 2d + d - 2w(x \cap y) \\ &= 3d - 2w(x \cap y) \\ w(x \cap y) &= 3d - \frac{w(x,\ x+y)}{2} \\ t &\geq 3d - \frac{w}{2}, \end{aligned}$$

where $w(x \cap y) = t$ and $w(x, x+y) = w$. □

Proposition 4.2. *If* C_1 *and* C_2 *are t-intersecting with minimum distances d and D, respectively, then the minimum distance of the concatenated codes is at least dD.*

Proof. Consider M be an array contains the q-ary vectors u_1 and u_2 for the code C_1 and C_2 whose minimal weights are d and D, respectively. But every component of i of u_1 will appear multiplied by every component of j of u_2 at least dD. Hence, the proposition holds good. □

Proposition 4.3. *If C is the q-ary intersecting code, then the code C satisfies* $d \geq k$.

Proof. Let $u_1 = 11\cdots111, 00\cdots000, \cdots, qq\cdots qqq$ be weight d and
$u_2 = 00\cdots000, 11\cdots111, \cdots, qq\cdots qqq$
$u_3 = 00\cdots000, 22\cdots222, \cdots, qq\cdots qqq$
$\vdots$
$u_k = 00\cdots000, 22\cdots222, \cdots, qq\cdots qqq$ in which $u_2, \cdots, u_k$ begin with 0. Since each of $u_2, \cdots, u_k$ must intersect u_1. Therefore, $k-1 < d-1$ which implies that $k \leq d$. □

Theorem 4.4. *If* $C = [2n,\ k = k_1+k_2,\ d = \min(2d'_1, d'_2)]$, *then C is intersecting for positive distance d and dimension k greater than or equal to* 3.

Proof. We will prove the theorem by using self-complementary codes. So that, consider the two cases such that the codes are intersecting.

Case 1: $\min(2d'_1, d'_2) = 2d'_1$.

If possible, the code C is non-intersecting, there exists two self-complementary codewords $c'_1,\ c'_2 \in C$ with same weight $2d'_1$. Suppose that, c'_3 in C, is not any linear combination of c'_1 and c'_2, then $w(c'_1 + c'_3) \geq 2d'_1$. This implies $|c'_2 \cap c'_3| \geq |c'_1 \cap c'_3|$. In similar way, we can also prove that $|c'_1 \cap c'_3| \geq |c'_2 \cap c'_3|$. Thus, we arrive the equality. Hence,

$w(c_3') = d > 2d_1'$, where d is an even integer. Consequence of the above argument, the complement of c_3' is a codeword whose weight is less than $2d_1'$, which is a contradiction. Hence, we proved that the code C is intersecting.

Case 2: $\min(2d_1', d_2') = d_2'$.

Suppose that, the code C is non-intersecting, there exists two self-complementary codewords c_1', $c_2' \in C$ with same weight $2d_2'$. Suppose that, c_3' in C, is not any linear combination of $\{c_1', c_2'\}$, then $w(c_1' + c_3') \geq 2d_1'$. This implies $|c_2' \cap c_3'| \geq |c_1' \cap c_3'|$. In similar way, we can also prove that $|c_1' \cap c_3'| \geq |c_2' \cap c_3'|$. Thus, we arrive the equality. Hence, $w(c_3') = d > 2d_2'$, where d is an odd integer. Consequence of the above argument, the complement of c_3' is a codeword of weight less than $2d_2'$, which is a contradiction. Hence, we proved that the C is intersecting. The proof is similar to the above case except the weight of the codeword is an odd integer strictly greater than d_2', which is a contradiction.
Hence, in both cases, the code is intersecting. □

Proposition 4.5. *Assume, C be a* $[qd+1,\ k \geq 4,\ d = qp+1]$ *code with* $p > 0$, *then C is intersecting if and only if* $A_{qd+1} = 0$.

Proof. If $A_{qd+1} = 1$, then the code is self-complementary and hence non-intersecting.

Conversely, if $A_{qd+1} = 0$, then the only possible non-intersecting codes $c_1, c_2 \in C$ with weights $w(c_1) = qd, w(c_2) = qd$, respectively. Therefore, $w(c_1 + c_2) = 2qd$. If c_3 is not spanned by c_1, c_2, implies that $w(c_1 + c_3) \geq qd + 1$.

Without loss of generality, we may assume that the supports of the two codewords c_1 and c_2 are having first and the last positions as qd. If the code c_3 is not linear combination of c_1 and c_2, then $w(c_1 + c_3) \geq qd + 1$.

The support of c_3 in the first d positions has size at most qp. since $w(c_2 + c_3) \geq qd + 1$, the support of c_3 in the last d positions has size at most qp too. Thus, $w(c_3) = qd$ and $A_d > 2$.

Similarly, we can construct a new code c_4 is not linear combination of $\{c_1, c_2, c_3\}$, we may assume that the first three rows of c_1, c_2, c_3 of the generator matrix of C are

$$111\cdots 11, q-1q-1q-1\cdots q-1q-1, 0, 000\cdots 00, 000\cdots 00$$

$$000\cdots 00, 000\cdots 00, 1, q-1q-1q-1\cdots q-1q-1, 111\cdots 11$$

$$000\cdots 00, q-1q-1q-1\cdots q-1q-1, 1, 111\cdots 11, 000\cdots 00,$$

we divide the positions of C into five sets, namely, E the first $q(p+1)$ positions, F the next qp positions, H the one position I the next $q(p+1)$ positions and J the last qp positions. The support of c_4 in E, F, H, I, J are e, f, h, i, j, respectively. All requirements for c_3 are valid for c_4 too. $w(c_4) = qd$. To find c_4, we have to determine the values of e and f. The support of $c_3 + c_4$ in the first qd positions shows that $e \geq f$. The support $c_1 + c_2 + c_3$ in the first qd positions shows that $f + 1 > e$, which implies $e = f$.

Hence, $w(c_3 + c_4) = 2qp < d$, which is a contradiction.
This implies C is intersecting. □

References

[1] Ashikhmin A., Barg A., Minimal vectors in linear codes, *IEEE Trans. Inform. Theory*, 44(5)(1998), 2010–2017.

[2] Blake I.F., Codes over integer residue rings, *Information and Control*, 29(1975), 295–300.

[3] Cohen G., Lempel A., Linear intersecting codes, *Discrete Math.*, 56(1985), 35–43.

[4] Cohen G., Zemor G., Intersecting codes and independent Families,*IEEE Trans. Inform. Theory*, 40(6), 1872–1881.

[5] Cohen G., Encheva S., Schaathun H.G., On separating codes, *Technical reports in informatics, the Centre National de la RechercheScientifique and Telecom Paris, Departement INF*, 2001.

[6] Cohen G., Encheva S., Schaathun H.G., More on (2; 2)-separating systems, *IEEE Trans. Inform. Theory*, 48(9)(2001), 2606–2609.

[7] Cohen G., Encheva S., Litsyn S., Schaathun H.G., Intersecting codes and separating codes, *Discrete Applied Mathematics*, 128(75)(2003), 75–83.

[8] Encheva S., Cohen Gerard D., Constructions of intersecting Codes, *IEEE Trans.Inform. Theory*, 45(4)(1999).

[9] Macwilliams F.J and Slone N.J.A., *The theory of error correcting codes*, North-Holland, New york, 1977.

[10] Miklos D., Linear binary codes with intersection properties, *Discrete Appl. Math.*, 9(2)(1984), 187–196.

[11] Sloane N.J.A., *Covering arrays and intersecting codes, J. Combinator. Designs*, Vol. 1(1993), 51–63.

⋆⋆⋆⋆⋆⋆⋆⋆⋆
ISSN(P):2319 − 3786
Malaya Journal of Matematik
ISSN(O):2321 − 5666
⋆⋆⋆⋆⋆⋆⋆⋆⋆