DOI: 10.24996/ijs.2021.62.11.22

ISSN: 0067-2904

Certain Types of Linear Codes over the Finite Field of Order Twenty-Five

Emad Bakr Al-Zangana*, Elaf Abdul Satar Shehab
Department of Mathematics, College of Science, Mustansiriyah University, Baghdad, Iraq

Received: 4/11/2020 Accepted: 24/1/2021

Abstract
The aim of the paper is to compute projective maximum distance separable codes, PG-MDS of two and three dimensions with certain lengths and Hamming weight distribution from the arcs in the projective line and plane over the finite field of order twenty-five. Also, the linear codes generated by an incidence matrix of points and lines of $PG(2,25)$ were studied over different finite fields.

Keywords: Linear code, MDS, Projective space, Incidence matrix.

أنواع معينة من الترميزات الخطية على الحقل من الرتبة خمسة وعشرون

عماد بكر الزنكنة *، ايلاف عبدالستار شهاب
قسم الرياضيات، كلية العلوم، الجامعه المستنصريه، بغداد، العراق

الخلاصة
الهدف من البحث هو حساب الترميزات الاسقاطية, $PG-$MDS ذات البعد الثاني والثالث مع توزيع الاوزان ذات اطوال واوزان هامنك معينين من الاقواس في الخط الاسقاطي والمستوي على الحقل من الرتبة خمسة وعشرين. كذلك, الترميزات الخطية المتولدة بواسطة مصفوفة الوقوع من نقاط وخط $PG(2,25)$ قد تم دراستها على حقول منتهية مختلفة.

1. Introduction

Let $GF(q) = F_q$ denotes the Galois field of q elements, q is a prime power, $F_q^+ = F_q$ is a plus point at infinity, and F_q^k is the vector space of row vectors of length n with entries in F_q. Let $PG(k-1,q)$ be the corresponding projective space of dimension $k-1$. As a special case, $PG(1,q)$ and $PG(2,q)$ are called projective line and projective plane, respectively. The points $P(x_1,\dots,x_k)$ of $PG(k-1,q)$ are the one dimensional subspaces of F_q^k. In $PG(k-1,q)$, the number of points is $\theta(k-1,q) = (q^k-1)/(q-1)$ and the number of lines is $(q^k-1)(q^{k-1}-1)/(q^2-1)(q-1)$. An $(n;r)$-arc with $n \geq r+1$ is a set of k points of a projective space, such that most r points are on the hyperplane, but with at least one set of r points are on the hyperplane. In the line, $(n;1)$-arc is just an n-set; that is, a set of n distinct points. An $(n;r)$-arc K is called complete if it is maximal with respect to inclusion; that is, there is no an $(n+1;r)$-arc containing K. The maximum size of an $(n;r)$-arc in $PG(k-1,q)$ is denoted by $m_r(k-1,q)$. In 1947, Bose [1] proved that

$$m_r(2,q) = q + 2 \; for\; q\; even, \quad m_r(2,q) = q + 1\; for\; q\; odd.$$

In the finite projective line, the value of $m_1(1,q)$ is just $q+1$.

*Email: emad77_kaka@yahoo.com

Definition 1. A conic $\mathcal{C}$ in $PG(2,q)$ is the set of rational points of a homogenous nonsingular form F of degree two over F_q.

Bose showed that: an $(m_2(2,q);2)$-arc in $PG(2,q), q$ odd, is just the conic, and that the conic plus its nucleus (the intersection point of its tangents) is an $(m_2(2,q);2)$-arc in $PG(2,q), q$ even.

The points $P(X,Y)$ of the projective line $PG(1,q)$ are identified by F_q^+ by sending the points $P(X,Y)$ to X/Y if $Y \neq 0$ and to ∞ if $Y=0$. The relation between the conic $\mathcal{C}^*(X^2-YZ)$ and F_q^+ exists by sending each point t of F_q^+ to $P(t^2,t,1)$ point on the conic $\mathcal{C}^*$.

For details and basic results on the projective space and the essential subsets of the projective space, see [2].

The Hamming weight of a vector $x \in F_q^n$ is the number of non-zero coordinates of x, denoted by $wt(x)$. A q-ary $[n,k,d]$-code C over F_q is a k-dimensional subspace of F_q^n, all of whose non-zero vectors (codewords) have a weight of at least $d=d(C)$. A q-ary $[n,k,d]$-code that corrects $e=\left\lfloor\frac{d-1}{2}\right\rfloor$ errors is called e-error correcting code, where $\lfloor x\rfloor$ denotes the floor function. Let A_i denotes the number of codewords with Hamming weight i in a code C of length n. The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of the code C. The dual code of q-ary $[n,k,d]$-code C over F_q, denoted by $C^\perp$, is defined by

$$C^\perp = \left\{x=(x_1,\ldots,x_n)\in F_q^n : \sum_{i=1}^{n} x_i c_i = 0, \forall c=(c_1,\ldots,c_n)\in C\right\}.$$

Any q-ary $[n,k,d]$-code C can be defined by a $(k\times n)$ matrix $G=[I_k A]$ (standard form), where A is a nonsingular $(k\times n)$ matrix with entries from F_q, called the generator matrix, whose rows form a basis. Also, the dual code $C^\perp$ can be defined by a $(n-k)\times n$ matrix $H=\left[-A^T I_{(n-k)}\right]$. Two linear codes are isomorphic (equivalent) if the generator matrices are equivalent after doing a sequence of row (column) operations.

A sphere-packing bound of a q-ary $[n,k,d=2e+1]$-code C over F_q is

$$q^k\left\{\sum_{i=0}^{e}\binom{n}{i}(q-1)^i\right\}\leq q^n.$$

A code which achieves the sphere-packing bound is called a perfect code, see [3].

Definition 2 [4]**.** A q-ary $[n,k,d]$-code C over F_q at $d=n-k+1$ (the maximum value of d) is called a maximum distance separable code, or MDS code for short. The code C is called projective if the columns of a generator matrix are pairwise linearly independent and denoted by PG-MDS.

Theorem 3 [4]

A q-ary $[n,k,d]$-code C over F_q is MDS if and only if its dual $C^\perp$ is MDS; that is, $d(C)=n-k+1$ if and only if $d(C^\perp)=k+1$.

Therefore, A q-ary $[n,k,d]$-code C over F_q is PG-MDS if and only if its dual $C^\perp$ is PG-MDS, since the standard generator matrix of both are depending on the base matrix A.

It is well known that there is equivalence between the existence of a PG-MDS and an arc in the projective space, where this equivalence comes from the fact that the matrix in which each column is a point of an arc has formed a generator matrix of PG-MDS.

The full prove of this relation is presented elsewhere [4] and the statement of the theorem is as follows.

Theorem 4: There exists a PG-MDS q-ary $[n,k,d]$-code if and only if an $(n;n-d)$-arc exists in $PG(k-1,q)$. As special cases:

(i) If $k = 2$, then every r-set, that is $(r; 1)$-arc, in $PG(1, q)$ gives a generator matrix of PG-MDS q-ary $[r, 2, r - 1]$-code over F_q.
(ii) If $k = 3$, then every $(r; 2)$-arc in $PG(2, q)$ gives a generator matrix of PG-MDS q-ary $[r, 3, r - 2]$-code over F_q.
The weight enumerator of an MDS (PG-MDS) q-ary $[n, k, d]$-code C over F_q is unique, and the weight distribution of the code C is $(A_0 = 1, A_1, A_2, \ldots, A_n)$, where
$A_j = 0$ for $0 < j < d$, and

$$A_j = (q-1)\binom{n}{j}\sum_{l=0}^{j-d}(-1)^l\binom{j-1}{l}\, q^{j-d-l}, \tag{1}$$

for $d \leq j \leq n$. If $d = n - k + 1$, then

$$A_d = (q-1)\binom{n}{d}. \tag{2}$$

For details and descriptions of equations (1) and (2), see [3].
Ezerman *et al.* [5] determined the weight spectra of certain linear MDS codes, namely those that satisfy the MDS Conjecture. Alderson [6] discussed the weight distribution of MDS q-ary $[n, k, d]$-code and showed that all k weights from n to $n - k + 1$ are realized.
One of the important questions for a code with parameters n, k, d and q, is: how many non-isomorphic codes are there having these parameters? Many researches discussed this question directly by working on the code, see for example [7, 8], or indirectly through projective space, both in general cases and for a certain q, see for example [9,10,11].
The first objective of this paper is to present a class of non-isomorphic error-correcting PG-MDS codes over F_{25} of two and three dimensions with their weight distributions. The second objective is to construct linear codes from the incidence matrix of lines and points of $PG(2,25)$ by giving details of generator matrices over distinct finite fields.
The GAP programming was used to perform the calculations required for achieving the desired results [12].

2. Non-Isomorphic Error-Correcting PG-MDS Codes over F_{25}

Al-Zangana and Shehab [13] gave full details of the classification of projectively inequivalent k-subsets in the projective line over F_{25}, such that each k-subset contains the standard frame $\Gamma_{25}(3) = \{\infty, 0,1\}$. These results are summarized in Table 1. Let n_k denotes the number of projectively inequivalent k-subsets of $PG(1,25)$.

Table 1- Projectively inequivalent k-subsets of PG(1,25).

k	4	5	6	7	8	9	10	11	12	13
n_k	5	8	28	54	131	225	398	531	692	714

Theorem 5. Over F_{25}, the non-isomorphic PG-MDS codes with parameters n, k, d, e, and no zero weight distributions A_i are listed in Table 2.

Table 2- Non-isomorphic PG-MDS codes of dimension 2.

$\hat{m}$	n	k	d	e	A_0	A_{n-1}	A_n
5	4	2	3	1	1	96	528
8	5	2	4	1	1	120	504
28	6	2	5	2	1	144	480
54	7	2	6	2	1	168	456
131	8	2	7	3	1	192	432
225	9	2	8	3	1	216	408
398	10	2	9	4	1	240	384
531	11	2	10	4	1	264	360
692	12	2	11	5	1	288	336
714	13	2	12	5	1	312	312

692	14	2	13	6	1	336	288
531	15	2	14	6	1	360	264
398	16	2	15	7	1	384	240
225	17	2	16	7	1	408	216
131	18	2	17	8	1	432	192
54	19	2	18	8	1	456	168
28	20	2	19	9	1	480	144
8	21	2	20	9	1	504	120
5	22	2	21	10	1	528	96
1	23	2	22	10	1	552	72
1	24	2	23	11	1	576	48
1	25	2	24	11	1	600	24
1	26	2	25	12	1	624	---

Here $\widehat{m}$ denotes the number of non-isomorphic PG-MDS codes of specific parameters.

Proof. First of all, since each n-subset computed in [13] contains the points of the standard frame, then the constructed $(2\times n)$ matrix G from the points of n-subset will be in a standard form and the second row of G takes the form $0\ 1\ 1 \ldots 1$; that is, $G=[I_2A]$ and a $2\times(n-2)$ matrix A has now zero coordinate in each row (column) vector. According to the construction of points of the projective line, the second coordinate is 1 and, hence, the second row of A is always a vector with one in each coordinate. Hence, it is enough to give the first row of the matrix A to refer to the generator matrix. Secondly, from Theorem 4, every n-subset formed a PG-MDS q-$[n,2,n-1]$-code. For each n, the GAP program was used to compute the weight distributions A_i, $i=n-1,n$. Let β be the primitive element of F_{25}.

$n=4$.

1st row of generating matrix
$1\ 0\ 1\ \beta^{12}$
$1\ 0\ 1\ \beta^{4}$
$1\ 0\ 1\ \beta$
$1\ 0\ 1\ \beta^{22}$
$1\ 0\ 1\ \beta^{7}$

$n=5$.

1st row of generating matrix
$1\ 0\ 1\ \beta^{12}\ \beta^{6}$
$1\ 0\ 1\ \beta^{12}\ \beta$
$1\ 0\ 1\ \beta^{12}\ \beta^{2}$
$1\ 0\ 1\ \beta^{12}\ \beta^{3}$
$1\ 0\ 1\ \beta^{4}\ \beta^{2}$
$1\ 0\ 1\ \beta^{4}\ \beta^{5}$
$1\ 0\ 1\ \beta\ \beta^{2}$
$1\ 0\ 1\ \beta\ \beta^{8}$

$n=6$.

1st row of generating matrix
$1\ 0\ 1\ \beta^{12}\ \beta^{6}\ \beta^{18}$
$1\ 0\ 1\ \beta^{12}\beta^{6}\ \beta$
$1\ 0\ 1\ \beta^{12}\ \beta\ \beta^{2}$
$1\ 0\ 1\ \beta^{12}\ \beta\ \beta^{3}$
$1\ 0\ 1\ \beta^{12}\ \beta\ \beta^{4}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{5}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{7}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{8}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{9}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{10}$

$1\ 0\ 1\ \beta^{12}\beta\ \beta^{11}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{13}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{14}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{15}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{16}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{20}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{21}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{22}$
$1\ 0\ 1\ \beta^{12}\beta\ \beta^{23}$
$1\ 0\ 1\ \beta^{12}\ \beta^{2}\ \beta^{4}$
$1\ 0\ 1\ \beta^{12}\ \beta^{2}\ \beta^{9}$
$1\ 0\ 1\ \beta^{12}\ \beta^{2}\ \beta^{10}$
$1\ 0\ 1\ \beta^{12}\ \beta^{2}\ \beta^{14}$
$1\ 0\ 1\ \beta^{12}\ \beta^{3}\ \beta^{15}$
$1\ 0\ 1\ \beta^{12}\ \beta^{3}\ \beta^{16}$
$1\ 0\ 1\ \beta^{12}\ \beta^{3}\ \beta^{20}$
$1\ 0\ 1\ \beta\ \beta^{2}\ \beta^{3}$
$1\ 0\ 1\ \beta\ \beta^{8}\ \beta^{15}$

For $n = 7, \ldots 13$, the first rows of a one generating matrix are written below, since there is no enough space to write all here.

	1st row of generating matrix
$n = 7$	$1\ 0\ 1\ \beta^{12}\beta^{6}\ \beta^{18}\ \beta$
$n = 8$	$1\ 0\ 1\ \beta^{12}\beta^{6}\ \beta^{18}\ \beta^{2}$
$n = 9$	$1\ 0\ 1\ \beta^{12}\beta^{6}\beta\ \beta^{4}\ \beta^{5}\ \beta^{20}$
$n = 10$	$1\ 0\ 1\ \beta^{12}\beta^{6}\ \beta^{18}\beta\ \beta^{8}\ \beta^{9}\ \beta^{14}$
$n = 11$	$1\ 0\ 1\ \beta^{12}\beta^{6}\ \beta^{18}\beta\ \beta^{2}\ \beta^{4}\ \beta^{7}\ \beta^{16}$
$n = 12$	$1\ 0\ 1\ \beta^{12}\beta^{6}\ \beta^{18}\beta\ \beta^{2}\ \beta^{3}\ \beta^{9}\ \beta^{14}\ \beta^{19}$
$n = 13$	$1\ 0\ 1\ \beta^{12}\beta^{6}\ \beta\ \beta^{2}\ \beta^{3}\ \beta^{4}\ \beta^{11}\ \beta^{16}\ \beta^{17}\ \beta^{22}$

The complement subset $K^c$of each n-subset K formed an $(26-n)$-subset of $PG(1,25)$. Therefore, the number of inequivalent $(26-n)$-subsets and n-subsets of $PG(1,25)$ is equal. Thus, the number of non-isomorphic PG-MDS codes with length equal to $26-n$ and dimension 2 is equal to the number of non-isomorphic PG-MDS codes with length n and dimension 2, where $n = 4, \ldots, 12$. The number of non-isomorphic PG-MDS codes with lengths $23, 24, 25$ and dimension 2 is one, since all the 3-sets are equivalents. Also, there is only one non-isomorphism PG-MDS code of length 26 and dimension 2, since the 26-subset of $PG(1,25)$ is just the line. ■

Corollary 5. Over F_{25}, the dual codes $C^{\perp}$ of the PG-MDS codes C with parameters $\widehat{m}, n,$ shown in Table 2, formed PG-MDS codes with dimension $n-2, d = 3$ and $e = 1$.

Proof. From Theorem 3, each dual code $C^{\perp}$ of the PG-MDS q-ary $[n, 2, n-1]$-code C over F_{25} formed PG-MDS q-ary $[n, n-2, 3]$-code and $e = 1$ with $n = 4, \ldots, 26$. Since the dual code of $C^{\perp}$ is C, then the number of non-isomorphic code $C^{\perp}$ for certain length n is $\widehat{m}$, as in Table 2. The weight distributions $(A_3, \ldots, A_n)$ of $C^{\perp}$ for fixed n are as listed in Table 3.

Table 3- Weight distributions (A_3,…,A_n) of C^⊥ for n=4,…,14

n	$(A_3, \ldots, A_n)$
4	(96, 528)
5	(240, 2640, 12744)
6	(480, 7920, 76464, 305760)
7	(840, 18480, 267624, 2140320, 7338360)
8	(1344, 36960, 713664, 8561280, 58706880, 176120496)
9	(2016, 66528, 1605744, 25683840, 264180960, 1585084464, 4226892072)
10	(2880, 110880, 3211488, 64209600, 880603200, 7925422320, 42268920720, 101445409536)
11	(3960, 174240, 5887728, 141261120, 2421658800, 29059881840, 232479063960,

	1115899504896, 2434689829080)
12	(5280, 261360, 10093248, 282522240, 5811981120, 87179645520, 929916255840, 6695397029376, 29216277948960, 58432555897680)
13	(6864, 377520, 16401528, 524684160, 12592625760, 226667078352, 3022227831480, 29013387127296, 189905806668240, 759623226669840, 1402381341544584)
14	(8736, 528528, 25513488, 918197280, 25185251520, 528889849488, 8462237928144, 101546854945536, 886227097785120, 5317362586688880, 19633338781624176, 33657152197069728)
15	(10920, 720720, 38270232, 1530328800, 47222346600, 1133335391760, 21155594820360, 304640564836608, 3323351616694200, 26586812933444400, 147250040862181320, 504857282956045920, 807771652729673784)
16	(13440, 960960, 55665792, 2448526080, 83950838400, 2266670783520, 48355645303680, 812374839564288, 10634725173421440, 106347251733777600, 785333551264967040, 4038858263648367360, 12924346443674780544, 19386519665512170480)
17	(16320, 1256640, 78859872, 3784085760, 142716425280, 4281489257760, 102755746270320, 1972910324656128, 30131721324694080, 361580655894843840, 3337667592876109920, 22886863494007415040, 109856944771235634624, 329570834313706898160, 465276471972292091880)
18	(19584, 1615680, 109190592, 5676128640, 233535968640, 7706680663968, 205511492540640, 4439048230476288, 77481569120641920, 1084741967684531520, 12015603334353995712, 102990885723033367680, 659141668627413807744, 2966137508823362083440, 8374976495501257653840, 11166635327335010204736)
19	(23256, 2046528, 148187232, 8295880320, 369765283680, 13311539328672, 390471835827216, 9371324042116608, 184018726661524560, 2944299626572299840, 38049410558787653088, 391365365747526797184, 3130922925980215586784,18785537555881293195120,79562276707261947711480, 212166071219365193889984, 267999247856040244914072)
20	(27360, 2558160, 197582976, 11851257600, 568869667200, 22185898881120, 709948792413120,18742648084233216, 408930503692276800, 7360749066430749600,108712601596536151680, 1304551219158422657280, 12523691703920862347136, 93927687779406465975600, 530415178048412984743200, 2121660712193651938899840, 5359984957120804898281440, 6431981948544965877937296)
21	(31920, 3160080, 259327656, 16591760640, 853304500800, 35838759731040, 1242410386722960, 35781419069899776, 858754057753781280, 17175081155005082400, 285370579190907398160, 3913653657475267971840, 43832920963723018214976, 394496288673507157097520, 2784679684754168169901800, 14851624985355563572298880, 56279842049768451431955120, 135071620919444283436683216, 154367566765079181070495560)
22	(36960, 3862320, 335600496, 22813670880, 1251513267840, 56318051005920, 2102540654454240, 65599268294816256, 1717508115507562560, 37785178541011181280, 697572526911106973280, 10762547558056986922560, 137760608743129485818496, 1446486391802859576024240, 12252590612918339947567920, 81683937419455599647643840, 412718841698301977167670880, 1485787830113887117803515376, 3396086468831741983550902320, 3704821602361900345691892960)
23	(42504, 4675440, 428822856, 30865554720, 1799050322520, 86354344875744, 3454173932317680, 116060243906213376, 3291890554722828240, 79005373313023379040, 1604416811895546038544,27504288203923411024320, 396061750136497271728176, 4752741001637967178365360, 46968264016186969799010360, 375746112129495758379161664, 2373133339765236368714107560, 11391040030873134569826951216, 39054994391565032810835376680, 85210896854323707950913538080, 88915718456685608296605431544)
24	(48576, 5610528, 541670976, 41154072960, 2539835749440, 129531517313616, 5526678291708288, 198960418124937216, 6077336408719067520, 158010746626046758080,3500545771408464084096, 66010291689416186458368,1056164667030659391275136,

	14258223004913901535096080,161034048055498182168035520, 1502984448517983033516646656,11391040030873134569827716288, 68346240185238807418961707296,312439955132520262486683013440, 1022530762251884495410962456960, 2133977242960454599118530357056, 2133977242960454599118530356528)
25	(55200, 6679200, 677088720, 54150096000, 3527549652000, 190487525461200, 8635434830794200, 331600696874895360, 10852386444141192000, 303866820434705304000,292803690434300175200, 150023390203218605587200, 2640411667576648478187840, 39606175013649726486378000, 503231400173431819275111000, 5367801601849939405416595200, 47462666795304727374282151200, 341731200926194037094808536480, 1952749719578251640541768834000, 8521089685432370795091353808000, 26674715537005682488981629463200, 53349431074011364977963258913200, 51215453831050910378844728557224)
26	(62400, 7893600, 838300320, 70395124800, 4827173208000, 275148647888400, 13207135623567600, 538851132421704960, 18810803169844732800, 564324095093024136000, 14585607380868600350400, 325050678773640312105600, 6240973032453896402989440, 102976055035489288864582800, 1453779600501025255683654000, 17445355206012303067603934400, 176289905239703273104476561600, 1480835204013507494077503658080, 10154298541806908530817197936800, 55387082955310410168093799752000, 231180867987382581571174122014400, 693542603962147744713522365871600,1331601799607323669849962942487824, 1229170891945221849092273485372800)

■

Al-Zangana and Shehab [14] proved that there are eight inequivalent 5-arcs and 365 inequivalent 6-arcs in the projective plane over F_{25} through the standard frame $\Gamma_{25}(4) = \{U_0, U_1, U_2, U\}$. The corresponding PG-MDS codes to these arcs are summarized in the following theorem.

Theorem 6. Over F_{25}, there are

(i) eight non-isomorphic PG-MDS [5,3,3]-codes with $e = 1$ and weight distribution $(1, 0, 0, 240, 2640, 12744)$. The dual codes of these codes are PG-MDS [5,2,4]-code with $e = 1$ and weight distribution $(1, 0, 0, 0, 120, 504)$.

(ii) 365 non-isomorphic PG-MDS [6,3,4]-codes with e =2 and weight distribution $(1, 0, 0, 0, 360, 3024, 12240)$. The dual codes of these codes are equivalent to the base codes.

Example 7

(i) PG-MDS [5,3,3]-code C_1 with generator matrix $G_1 = \begin{bmatrix} 1001\beta^{16} \\ 0101\,\beta^{7} \\ 0011\;\;1 \end{bmatrix}$. The generator matrix of PG-MDS [5,2,4]-code $C_1^{\perp}$ is $H_1 = \begin{bmatrix} \beta^{12}\beta^{12}\beta^{12}10 \\ \beta^{4}\;\beta^{19}\beta^{12}01 \end{bmatrix}$.

(ii) PG-MDS [6,3,4]-code C_2 with generator matrix $G_2 = \begin{bmatrix} 1001\beta^{20}\beta^{19} \\ 0101\;\beta\;\;\beta^{20} \\ 0011\;\;1\;\;\;1 \end{bmatrix}$. The generator matrix of PG-MDS [6,3,4]-code $C_2^{\perp}$ is $H_2 = \begin{bmatrix} \beta^{12}\,\beta^{12}\,\beta^{12}100 \\ \beta^{8}\;\beta^{13}\,\beta^{12}010 \\ \beta^{7}\;\beta^{8}\beta\,\alpha^{12}001 \end{bmatrix}$. The matrix H_2 can be transformed to G_2 after dividing the first, second, and third columns of H_2 by β^{12} and applying some permutations in rows and columns. Thus, $C_2^{\perp}$ is equivalent to C_2.

3. Codes from Incidence Matrix

The incidence matrix $IM^* = (a_{ij})$ of points and k-dimensional projective subspaces in the projective space $PG(n, q), q = p^h$, p prime, $h \geq 1$, is defined as the matrix whose rows are indexed by the k-spaces of $PG(n, q)$, $1 \leq k \leq n - 1$, and whose columns are indexed by the points of $PG(n, q)$, and with the entry

$$a_{ij} = \begin{cases} 0 & \text{if point } j \text{ belongs to } k-\text{space } i, \\ 1 & \text{otherwise.} \end{cases}$$

Clearly, the dimension of IM^* is $\theta(n,q) \times \theta(n,q)$. For more details, see [15, 16].

It is known that the rows of the matrix IM^* generate a p-ary $[n,k,d]$-code over a field F_p. This code is normally denoted by $C_k = C_k(n,q)$, and by $C(2,q)$ if $k = 1$ and $n = 2$.

The minimum weight of $C(2,q)$ is $q+1$, which is provedin by giving the general case for that. Therefore, $e = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{q+1-1}{2} \right\rfloor = \left\lfloor \frac{q}{2} \right\rfloor$.

Over F_{25}, The incidence matrix $IM^* = (a_{ij})$ of points and lines in the projective space $PG(2,25)$ was computed. An algorithm was executed with GAP program to compute the generator matrices of linear codes from IM^*over several finite fields. The results are summarized below.

The matrix IM^* is given by identifying each row, r_i, by a non-zero position, as shown below.

$$IM^* = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{650} \\ r_{651} \end{pmatrix}$$

$$= \begin{pmatrix} 1,2,4,44,65,74,93,162,170,176,215,252,269,310,397,422,454,472,501,506,516,528,532,539,552,587 \\ 2,3,5,45,66,75,94,163,171,177,216,253,270,311,398,423,455,473,502,507,517,529,533,540,553,588 \\ \vdots \\ \vdots \\ 2,42,63,72,91,160,168,174,213,250,267,308,395,420,452,470,499,504,514,526,530,537,550,585,650,651 \\ 1,3,43,64,73,92,161,169,175,214,251,268,309,396,421,453,471,500,505,515,527,531,538,551,586,651 \end{pmatrix}.$$

In the following theorem, the q-ary $[n,k,d]$-code over $F_q, q = p^m$, generated by IM^*, was founded for $2 \leq p \leq 397$ and p is prime. Since the results will be out of the memory of the computer, the program for $p > 397$ cannot be run .

Theorem 8. Over F_{25}, the IM^* generates the following error-correcting, e, q-ary $[n,k,d]$-code over the field F_q, $q = p^m$:

(i) q-ary $[651,226,1 \leq d \leq 26]$-code with $e = 12$ if $q = 5^m$.

(ii) q-ary $[651,650,1 \leq d \leq 2]$-code with $e = 0$ if $q = p^m, p = 2,13$.

(iii) q-ary $[651,651,1]$-code with $e = 0$ if $q = p^m$, $3 \leq p(\neq 2,5,13) \leq 397$.

Proof. The procedure that was used to find the generating matrix of the q-ary $[n,k,d]$-code, depending on the field F_q, is firstly looking for the linearly dependent rows in the matrix $IM^*$and secondly looking for the linearly dependent codewords that are generated from the linearly dependent rows of IM^*. This was achieved using the mathematical language GAP. The generating matrix of q-ary $[n,k,d]$-code over F_q, $q = p^m$ is exactly the generating matrix of q-ary $[n,k,d]$-code over F_p. Since the entries of the matrix IM^* are just 0 and 1, then the sums between rows of IM^* will behave like elements of F_p.

(i) The details of the generating matrix Ψ of the 5-ary $[651,226,1 \leq d \leq 26]$-code, $C(2,25)$, with $e = 12$, are given in Tables 4 and 5. Let n_{r_i} denotes the order of the row r_i and $=_s$ denotes the size of non-zero positions of row r_i.

Table 4- Details of the generator matrix Ψ of C(2,25)

n_{r_i}	$=_s$	n_{r_i}	$=_s$	n_{r_i}	$=_s$	n_{r_i}	$=_s$	n_{r_i}	$=_s$
1	26	51	26	101	427	151	410		
2	26	52	26	102	427	152	397		
3	26	53	26	103	434	153	397		
4	26	54	26	104	434	154	397		
5	26	55	26	105	432	155	397		
6	26	56	26	106	424	156	394		
7	26	57	26	107	434	157	420		
8	26	58	26	108	421	158	404		
9	26	59	26	109	436	159	379		
10	26	60	26	110	436	160	408		
11	26	61	26	111	429	161	404		
12	26	62	26	112	449	162	402		
13	26	63	26	113	449	163	385	201	366
14	26	64	26	114	430	164	361	202	361
15	26	65	26	115	442	165	361	203	360
16	26	66	468	116	440	166	367	204	358
17	26	67	448	117	440	167	399	205	365
18	26	68	441	118	435	168	387	206	364
19	26	69	452	119	439	169	385	207	358
20	26	70	465	120	439	170	390	208	363
21	26	71	447	121	444	171	390	209	353
22	26	72	460	122	419	172	385	210	353
23	26	73	469	123	432	173	374	211	342
24	26	74	463	124	434	174	387	212	342
25	26	75	444	125	434	175	389	213	352
26	26	76	458	126	415	176	388	214	353
27	26	77	449	127	412	177	391	215	351
28	26	78	461	128	420	178	391	216	351
29	26	79	451	129	420	179	370	217	347
30	26	80	451	130	423	180	370	218	347
31	26	81	453	131	405	181	389	219	345
32	26	82	465	132	398	182	380	220	345
33	26	83	440	133	412	183	354	221	344
34	26	84	456	134	404	184	354	222	342
35	26	85	456	135	404	185	354	223	344
36	26	86	442	136	425	186	359	224	345
37	26	87	455	137	425	187	381	225	342
38	26	88	440	138	424	188	385	226	343
39	26	89	436	139	416	189	385		
40	26	90	437	140	421	190	362		
41	26	91	437	141	414	191	367		
42	26	92	437	142	402	192	365		
43	26	93	449	143	410	193	387		
44	26	94	459	144	410	194	376		
45	26	95	450	145	411	195	365		
46	26	96	450	146	403	196	350		
47	26	97	460	147	422	197	370		
48	26	98	451	148	422	198	370		
49	26	99	443	149	411	199	370		
50	26	100	443	150	410	200	370		

Table 5- Numerical information of the generator matrix Ψ of $C(2,25)$

No.	$=_s$	$n_{=_s}$	*No.*	$=_s$	$n_{=_s}$
1	26	65	44	411	2
2	342	4	45	412	2
3	343	1	46	414	1
4	344	2	47	415	1
5	345	3	48	416	1
6	347	2	49	419	1
7	350	1	50	420	3
8	351	2	51	421	2
9	352	1	52	422	2
10	353	3	53	423	1
11	354	3	54	424	2
12	358	2	55	425	2
13	359	1	56	427	2
14	360	1	57	429	1
15	361	3	58	430	1
16	362	1	59	432	2
17	363	1	60	434	5
18	364	1	61	435	1
19	365	3	62	436	3
20	366	1	63	437	3
21	367	2	64	439	2
22	370	6	65	440	4
23	374	1	66	441	1
24	376	1	67	442	2
25	379	1	68	443	2
26	380	1	69	444	2
27	381	1	70	447	1
28	385	5	71	448	1
29	387	3	72	449	4
30	388	1	73	450	2
31	389	2	74	451	3
32	390	2	75	452	1
33	391	2	76	453	1
34	394	1	77	455	1
35	397	4	78	456	2
36	398	1	79	458	1
37	399	1	80	459	1
38	402	2	81	460	2
39	403	1	82	461	1
40	404	4	83	463	1
41	405	1	84	465	2
42	408	1	85	468	1
43	410	4	86	469	1

(ii) Over the field F_2, the Hamming weights of vectors in the generating matrix take the values 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192, 194, 196, 198, 200, 202, 204, 206, 208, 210, 212, 214, 216, 218, 220, 222, 224, 226, 228, 230, 232, 234, 236, 238, 240, 242, 244, 246, 248, 250, 252, 254, 256, 258, 260, 262, 264, 266, 268, 270, 272, 274, 276, 278, 280, 282, 284, 286, 288, 290, 292, 294, 296, 298, 300, 302, 304, 306, 308, 310, 312, 314, 316, 318, 320, 322, 324, 326, 328, 330, 336, 340. Therefore, the Hamming weight of this code is 2.

Over the field F_{13}, the Hamming weights of vectors in the generating matrix take the values from 2 to 556 and 558. Therefore, the Hamming weight of this code is 2.

(iii) Over the field F_3, the Hamming weights of vectors in the generating matrix take the values from 1 to 418 and 425. Therefore, the Hamming weight of this code is 1.

Over the field F_{397}, the Hamming weights of vectors in the generating matrix take the values 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 66, 68, 69, 70, 72, 73, 74, 75, 76, 78, 79, 80, 82, 84, 85, 86, 87, 89, 90, 91, 92, 93, 96, 98, 99, 100, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 131, 133, 134, 135, 137, 138, 140, 141, 143, 144, 146, 147, 148, 149, 151, 152, 153, 154, 156, 157, 159, 160, 162, 164, 165, 167, 168, 169, 171, 172, 173, 174, 176, 177, 178, 180, 181, 182, 184, 185, 187, 189, 190, 191, 192, 193, 194, 196, 197, 199, 200, 201, 202, 204, 205, 206, 207, 209, 211, 212, 213, 214, 215, 216, 218, 219, 220, 221, 223, 224, 225, 227, 229, 230, 231, 233, 234, 235, 236, 237, 238, 241, 243, 244, 245, 246, 248, 249, 250, 251, 252, 254, 255, 256, 257, 259, 260, 261, 262, 263, 264, 265, 267, 268, 270, 271, 272, 274, 275, 276, 278, 279, 280, 281, 283, 284, 285, 286, 287, 289, 290, 292, 294, 295, 296, 297, 299, 300, 301, 303, 305, 307, 308, 310, 311, 312, 314, 316, 317, 320, 321, 322, 323, 324, 325,326, 328, 330, 332, 333, 335, 337, 338, 339, 340, 341, 344, 345, 346, 347, 348, 350, 351, 352, 354, 355, 357, 358, 359, 360, 361, 362, 363, 365, 368, 369, 372, 374, 376, 377, 379, 381, 382, 384, 385, 386, 387, 388, 389, 391, 392, 393, 395, 396, 397, 398, 400, 402, 403, 404, 407, 408, 409, 411, 412, 414, 415, 418, 419, 421, 422, 424, 425, 428, 429, 430, 431, 432, 435, 436, 437, 438, 440, 442, 444, 445, 446, 447, 450, 451, 452, 454, 455, 456, 458, 461, 463, 464, 466, 467, 469, 471, 472, 473, 475, 476, 477, 479, 480, 481, 484, 485, 488, 490, 492, 494, 495, 496, 497, 499, 500, 502, 503, 504, 507, 508, 509, 510, 511, 512, 514, 515, 518, 520, 522, 523, 524, 526, 527, 529, 530, 531, 533, 536, 538, 539, 540, 541, 542, 543, 544, 545, 546, 548, 549, 550, 551, 552, 553, 556, 557, 558, 559, 561, 562, 563, 564, 565.

The unique codeword in the generator matrix over F_{p^m}, $3 \leq p(\neq 2,5,13) \leq 397$ with a weight of 1 is the codeword with 1 in the last coordinate. ■

A linear code C of length n over F_q is called cyclic if: $(a_0 a_1 \dots a_{n-1}) \in C$ then $(a_{n-1} a_0 \dots a_{n-2}) \in C$. Since each codeword is identified with a polynomial $a_0 + a_1 X + \cdots a_{n-1} X^{n-1} \in F_q[X]/\langle X^n - 1\rangle$ (ring of polynomials in $F_q[X]$ of degree less than n), therefore, a q-ary $[n,k,d]$-code C over F_q can be viewed as a subset of F_q^n and a subset of $F_q[X]/\langle X^n - 1\rangle$. It is known that every non-zero cyclic C code is generated by a unique monic irreducible polynomial $f(X)$ with smallest degree r, and the property that $f(X)$ is a factor of $X^n - 1$ and $k = n - r$. This polynomial is called the generator polynomial of C. For details and characteristics of cyclic code, see [3].

Remark 9

(i) The rows $r_1, \dots, r_{65}$ of IM^* are only rows in the generating matrix of each code generated by IM^* over F_q.

The calculations show that:

(ii) the covering radius ρ of 5-ary $[651,226,1 \leq d \leq 26]$-code is $204 \leq \rho \leq 425$, and that of $5^{m\geq 2}$-ary $[651,226,1 \leq d \leq 26]$-code is $\rho \leq 425$.

(iii) the covering ρ of q^m-ary $[651,650,1 \leq d \leq 2]$-code is 1, where $q = 2,13$.

(iv) the q-ary $[651,651,1]$-code, $q = p^{m\geq 2}$, $3 \leq p(\neq 2,5,13) \leq 397$ is a perfect code with zero covering radius.

Corollary 10. All the dual codes of the codes in Theorem 8,i,ii are cyclic codes.
Proof. The dual codes of 5^m-ary $[651,226,1 \leq d \leq 26]$-code are cyclic, 5^m-ary $[651,425,1 \leq d \leq 195]$-code, and its covering radius is less than 226. The coefficients of the generator polynomials which are of degree 26 are 1, 1, 4, 3, 4, 3, 1, 2, 4, 2, 4, 4, 1, 4, 3, 0, 2, 0, 1, 3, 4, 4, 3, 0, 0, 1, 0, 2, 0, 4, 1, 3, 2, 3, 3, 2, 3, 0, 3, 2, 1, 3, 3, 0, 2, 1, 3, 3, 0, 2, 2, 2, 3, 0, 2, 1, 4, 3, 2, 3, 4, 1, 3, 3, 2, 3, 3, 4, 0, 0, 2, 2, 1, 0, 2, 4, 2, 2, 2, 1, 3, 0, 3, 1, 0, 4, 1, 1, 0, 4, 1, 2, 2, 0, 0, 2, 4, 3, 4, 0, 1, 1, 2, 1, 3, 4, 4, 3, 0, 1, 2, 2, 1, 4, 3, 4, 4, 2, 1, 2, 4, 4, 3, 4, 2, 2, 1, 4, 1, 4, 2, 1, 3, 2, 2, 4, 3, 2, 2, 0, 4, 2, 3, 4, 3, 2, 2, 3, 3, 3, 1, 2, 4, 0, 1, 4, 2, 1, 4, 3, 3, 2, 3, 4, 4, 4, 3, 4, 2, 0, 4, 4, 4, 0, 4, 1, 4, 3, 2, 3, 2, 2, 4, 1, 4, 4, 1, 2, 2, 0, 3, 3, 1, 4, 3, 1, 1, 3, 3, 3, 0, 4, 2, 1, 0, 3, 0, 1, 0, 3, 0, 0, 3, 2, 3, 3, 1, 1, 0, 3, 4, 3, 2, 1, 2, 3, 1. The weight of each row of the generator matrix is 195. Therefore, $1 \leq d \leq 195$.

The dual code of p^m-ary $[651,650,1 \leq d \leq 2]$-code is cyclic, p-ary $[651,1,651]$-code. The coefficient of the generator polynomials which are of degree 650 is just 1's. When $p = 2, m = 1$, the weight of each row of the generator matrix is 195 and its covering radius is 325. Since $e = 325$, then this code is perfect.

4. Conclusions

Over the finite field of order twenty-five, using ideas of arcs in the projective space, many non-isomorphic projective MDS were found. Also, with incidence matrix idea of points and lines in the projective space, many other linear perfect (non-perfect) codes were founded. The most important property of the rows of incidence matrix IM^* is that each i-th row is just circulate to the $(i-1)$-th row, except the last row. The best linear code that can be constructed from the incidence matrix IM^* is when it is taken over F_5, since it will have a Hamming weight $1 \leq d \leq 226$, while over the others that are of order distinct from 5, it behaves like a trivial code. Also, when the matrix IM^* is taken over F_2, a perfect code is founded.

Acknowledgements

The author thanks the University of Mustansiriyah and the Department of Mathematics at the College of Science for their supported to do this research.

References

[1] Bose, R. C. " Mathematical theory of the symmetrical factorial design", *Sankhya*, vol.8, pp: 107-166, 1947.
[2] Hirschfeld, J. W. P. *Projective geometries over finite fields, 2nd ed. New York: Ox- ford Mathematical Monographs, The Clarendon Press, Oxford University Press*, 1998.
[3] MacWilliams, F.J. and Sloane, N.J.A. *The Theory of error-correcting codes, 6th ed. Amsterdam: North-Holland Publishing Company*, 1977.
[4] Ball, S. and Hirschfeld, J.W.P. "Bounds on (n;r)-arcs and their application to linear code", *Finite Fields and Their Applications* , vol. 11, pp. 326-336, 2005.
[5] Ezerman, M.F., Grassl, M. and Sole, P. "The weights in MDS codes, Institute of Electrical and Electronics Engineers". *Transactions on Information Theory*, vol. 57, no. 1, pp. 392-396, 2011.
[6] Alderson, T.L. "On the weights of general MDS codes", arXiv: Combinatorics,2019. DOI:10.1109/tit.2020.2977319.
[7] Dougherty, S.T. and Han, S. "Higher weights and generalized MDS codes", *J. Korean Math. Soc.*, vol. 47, no. 6, pp.1167-1182, 2010.
[8] Zhao, H., Nian, L. and Xiangyong, Z. "New linear codes with few weights derived from Kloosterman sums". *Finite Fields and Their Applications*, vol. 62, article No. 101608, 2020.
[9] Heng, Z., Ding, C. and Wang, W. "Optimal binary linear codes from maximal arcs" 2020, arxiv.org/abs/2001.01049v1.
[10] Al-Zangana, E. B. The geometry of the plane of order nineteen and its application to errorcorrecting codes. Ph.D. Thesis, University of Sussex, UK, 2011.

[11] Heng, Z. and Ding, C. “The subfield codes of hyperoval and conic codes”, *Finite Fields and Their Applications*, vol. 56, pp. 308-331, 2019.
[12] The GAP Group. GAP. Reference manual, 2020. [Online]. https://www.gap-system.org/
Al-Zangana, E. B. and Shehab, E. AB. “Classification of k-sets in PG(1,25), for k=4,...,13,” *Iraqi Journal of Science*, vol. 59, no. 1B, pp. 360-368, 2018.
[13] Al-Zangana, E.B. and Shehab, E. AB. “Conic Parameterization in $\boldsymbol{P}(\mathbf{2},\ \mathbf{25})$”, *Al-Mustansiriyah Journal of Science*, vol. 29, no. 2, pp. 164-168, 2018.
[14] Assmus, E.F. and Key, J.D. *Designs and their codes. Cambridge; New York, USA: Cambridge University Press*, 1992.
[15] Bagchi, B. and Inamdar, S.P. “Projective geometric codes”, *Journal of Combinatorial Theory, Series A*, vol. 99, no. 1, pp. 128-142, 2002.
[16] Gaojun, L., Cao, X., Xu, S. and Mi, J. “Binary linear codes with two or three weights from niho exponents," *Cryptography and Communications*, vol. 10, no. 2, pp. 301-318, 2018.