

Research Article

Open Access

Weight Distribution of Some Codewords of 3-ary Linear Code over GF(27)

Maha Majeed Ibrahim*, Emad Bakr Al-Zangana

Department of Mathematics, College of Science, Mustansiriyah University, Baghdad, IRAQ

*Contact email: mahamajeed8200@gmail.com

Article Info

Received
23/09/2020

Accepted
26/10/2020

Published
20/12/2020

ABSTRACT

This paper is devoted to introduce the structure of the p-ary linear codes $C(n,q)$ of points and lines of $PG(n,q)$, $q = p^h$, when $p=3$. The linear code $C(2,27)$ is given with its generator matrix. Also, some of weight distributions are calculated. Finally, the generator matrix to the dual code of $C(2,27)$ has been founded.

KEYWORDS: Finite Projective Space, Incidence Matrix, Linear Code, Weight Distribution.

الخلاصة

هذا البحث مكرس لتقديم بنية ال p-ary للترميزات الخطية $C(n,q)$ من نقاط وخطوط ال $PG(n,q)$ حيث $q=p^h$ عندما $p=3$. تم إعطاء الترميز الخطى $(2,27)$ مع المصفوفة المولدة الخاصة به ، وتم أيضا حساب بعض توزيع الوزن لها. أخيرا، المصفوفة المولدة للترميز المزدوج لي $C(2,27)$ قد تم ايجاده.

INTRODUCTION

Let $GF(q)$, $q = p^h$, p prime, $h \geq 1$ be Galois field, and let F_q^n be the n -dimensional vector space over $GF(q)$.

A *linear code* of length n and dimension k over $GF(q)$ is a k -dimensional subspace C of F_q^n and denoted by $C[n, k]$. For any two elements of F_q^n , $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$, the *Hamming distance* $d(x, y)$ between them is defined by $d(x, y) = |\{i : 1 \leq i \leq n, x_i \neq y_i\}|$. For $x \in F_q^n$, the *Hamming weight* $w(x)$ is defined as number of non-zero coordinate of x ; that is, $w(x) = d(x, 0)$. If the minimum weight of nonzero elements in $C[n, k]$ is d denoted by $d(C)$, then the linear code C denoted by $C[n, k, d]$. The elements of $C[n, k, d]$ are called *codewords*. A $k \times n$ matrix G , whose rows form a linearly independent basis for $C[n, k]$ is called a *generator matrix* for C . If $C[n, k]$ has minimum distance d , then it can detect $d - 1$ errors and correct $e = \lfloor (d - 1)/2 \rfloor$ errors, where $\lfloor m \rfloor$ denotes the integer part of m . The *support* of a codeword x , denoted by $supp(x)$, is the set of all

non-zero positions of x . Here, A_i denotes the number of codewords with weight i , $0 \leq i \leq n$. The *weight distribution* of $C[n, k]$ is defined as the sequence A_0, A_1, \dots, A_n . Clearly, the weight distribution can give the minimum distance of the code. For details and properties of linear codes, see [1-4].

The *n-dimensional projective space over the finite field* $GF(q)$, denoted by $PG(n, q)$, is the set consisting of the equivalence classes $[X]$ of non-zero vectors X of the $(n + 1)$ -dimensional vector space F_q^{n+1} ; $[X] = \{Y : Y = tX \text{ for some } t \in GF(q) - 0\}$. The elements of $PG(n, q)$ are called *points* and the point denoted $P(X)$ is the equivalence class of the vector X . The number of points in $PG(n, q)$ is $\theta(n, q) = \frac{q^{n+1}-1}{q-1}$. For furthers about finite projective geometry, see [5].

Definition 1.1 [1,2]: 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 $PG(n, q)$ and whose columns are indexed by the points of $PG(n, q)$, and with entry $a_{ij} = \begin{cases} 0 & \text{if point } j \text{ belongs to } k - \text{space } i, \\ 1 & \text{otherwise.} \end{cases}$

Clearly, dimension of IM^* is $\theta(n, q) \times \theta(n, q)$.

Definition 1.2 [1,3]: The p -ary linear code of points and k -dimensional projective subspaces of $PG(n, q)$, $q = p^h$, p prime, $h \geq 1$, $1 \leq k \leq n - 1$, is the code generated by the rows of the incidence matrix IM^* and is denoted by $C_k = C_k(n, q)$. In the particular case that $k = 1$ and $n = 2$, we denote the p -ary linear code of points and lines of a projective plane $PG(2, q)$, by $C(2, q)$.

The minimum weight of $C(2, q)$ is $q + 1$ which proved in [8] by giving the general case for that.

Therefore, $e = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{q+1-1}{2} \right\rfloor = \left\lfloor \frac{q}{2} \right\rfloor$. Clearly from Definition 1.1 that length of $C(2, q)$ is $\theta(2, q)$.

The most important property of the rows of incidence matrix is that each i -th row is just circulate to the $(i - 1)$ -th row except the last row. In 1960s, *E Prange* and *L D Rudolph* perceived that projective planes could be used to construct error-correcting codes by using the incidence matrix. In the 1970's, the code of points and t -dimensional projective spaces was studied, but apart from the determination of the codewords of minimum weight and weight distributions, not much was known. Recently, calculating weight distributions of linear codes become an important research topic in coding theory since a few weights can be applied to secret sharing, association schemes, combinatorial designs, authentication codes and strongly regular graphs, see [6,7]. Some researchers spend their effort to calculate weight distributions and studied linear codes with a few weight, for example see [8-11].

In this paper, the most details of the 3-ary linear code of points and lines of a projective plane $PG(2, 27)$, $C(2, 27)$. Because of the large number of codewords of $C(2, 27)$ which is 3^{217} , the weight distributions have been not computed completely. The number of codewords, κ , that entered to account of weight distribution are 13723544 ; that is, $3^{14} \leq \kappa \leq 3^{15}$. The calculations are done with the mathematical programming language GAP [12].

The Linear Code $C(2, 27)$

The incidence matrix $IM^* = (a_{ij})$ of points and lines in the projective plane $PG(2, 27)$, is a matrix of dimension 757×757 , where $\theta(2, 27) = 757$. The matrix IM^* is written by filling each row by identify with the corresponding support of the certain row so, each row of the matrix IM^* , r_i , are written identifying to the $support(r_i)$ as below.

$$IM^* = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{756} \\ r_{757} \end{pmatrix}, \text{ where}$$

$r_1 = 1, 2, 4, 10, 28, 82, 149, 168, 212, 244, 309, 356, 386, 399, 438, 445, 461, 502, 506, 555, 576, 624, 634, 659, 674, 725, 730, 747;$

$r_2 = 2, 3, 5, 11, 29, 83, 150, 169, 213, 245, 310, 357, 387, 400, 439, 446, 462, 503, 507, 556, 577, 625, 635, 660, 675, 726, 731, 748;$

⋮

$r_{756} = 2, 8, 26, 80, 147, 166, 210, 242, 307, 354, 384, 397, 436, 443, 459, 500, 504, 553, 574, 622, 632, 657, 672, 723, 728, 745, 756, 757;$

$r_{757} = 1, 3, 9, 27, 81, 148, 167, 211, 243, 308, 355, 385, 398, 437, 444, 460, 501, 505, 554, 575, 623, 633, 658, 673, 724, 729, 746, 757.$

The number of linearly independent rows of IM^* which generated $C(2, 27)$ is 217; that is, the generator matrix of $C(2, 27)$, let denoted it by Ψ , is of dimension 217×757 . This matrix was computed by executed an algorithm on GAP mathematical language program. The details of the matrix Ψ are written below. Here, n_{r_i} denote the order of the row r_i and $=_s$ denote the size of $support(r_i)$.

Table 1. Details of the generator matrix Ψ of $C(2, 27)$

| n_{r_i} | $=_s$ | n_{r_i} | $=_s$ | n_{r_i} | $=_s$ |
|-----------|-------|-----------|-------|-----------|-------|
| 1 | 28 | 101 | 421 | 201 | 345 |
| 2 | 28 | 102 | 421 | 202 | 345 |
| 3 | 28 | 103 | 421 | 203 | 370 |
| 4 | 28 | 104 | 439 | 204 | 370 |
| 5 | 28 | 105 | 445 | 205 | 373 |
| 6 | 28 | 106 | 424 | 206 | 372 |
| 7 | 28 | 107 | 448 | 207 | 361 |
| 8 | 28 | 108 | 430 | 208 | 373 |
| 9 | 28 | 109 | 463 | 209 | 367 |
| 10 | 28 | 110 | 433 | 210 | 343 |
| 11 | 28 | 111 | 436 | 211 | 367 |
| 12 | 187 | 112 | 412 | 212 | 379 |
| 13 | 187 | 113 | 423 | 213 | 379 |
| 14 | 225 | 114 | 436 | 214 | 403 |
| 15 | 145 | 115 | 445 | 215 | 357 |
| 16 | 235 | 116 | 447 | 216 | 364 |

| | | | | | | | | | | | |
|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|--|--|
| 17 | 274 | 117 | 447 | 217 | 376 | 76 | 463 | 176 | 400 | | |
| 18 | 232 | 118 | 421 | | | 77 | 442 | 177 | 400 | | |
| 19 | 232 | 119 | 430 | | | 78 | 451 | 178 | 388 | | |
| 20 | 232 | 120 | 427 | | | 79 | 478 | 179 | 355 | | |
| 21 | 364 | 121 | 427 | | | 80 | 448 | 180 | 355 | | |
| 22 | 303 | 122 | 436 | | | 81 | 442 | 181 | 385 | | |
| 23 | 340 | 123 | 409 | | | 82 | 442 | 182 | 384 | | |
| 24 | 340 | 124 | 409 | | | 83 | 433 | 183 | 391 | | |
| 25 | 331 | 125 | 423 | | | 84 | 433 | 184 | 391 | | |
| 26 | 331 | 126 | 423 | | | 85 | 462 | 185 | 373 | | |
| 27 | 376 | 127 | 430 | | | 86 | 462 | 186 | 397 | | |
| 28 | 322 | 128 | 409 | | | 87 | 451 | 187 | 379 | | |
| 29 | 313 | 129 | 417 | | | 88 | 445 | 188 | 379 | | |
| 30 | 313 | 130 | 424 | | | 89 | 426 | 189 | 385 | | |
| 31 | 391 | 131 | 418 | | | 90 | 430 | 190 | 379 | | |
| 32 | 322 | 132 | 403 | | | 91 | 442 | 191 | 388 | | |
| 33 | 388 | 133 | 403 | | | 92 | 442 | 192 | 397 | | |
| 34 | 403 | 134 | 430 | | | 93 | 462 | 193 | 373 | | |
| 35 | 369 | 135 | 415 | | | 94 | 462 | 194 | 352 | | |
| 36 | 382 | 136 | 415 | | | 95 | 445 | 195 | 352 | | |
| 37 | 435 | 137 | 424 | | | 96 | 427 | 196 | 361 | | |
| 38 | 355 | 138 | 396 | | | 97 | 448 | 197 | 379 | | |
| 39 | 403 | 139 | 391 | | | 98 | 448 | 198 | 379 | | |
| 40 | 403 | 140 | 406 | | | 99 | 438 | 199 | 379 | | |
| 41 | 426 | 141 | 400 | | | 100 | 438 | 200 | 364 | | |
| 42 | 415 | 142 | 409 | | | | | | | | |
| 43 | 427 | 143 | 409 | | | | | | | | |
| 44 | 420 | 144 | 409 | | | | | | | | |
| 45 | 420 | 145 | 403 | | | | | | | | |
| 46 | 420 | 146 | 403 | | | | | | | | |
| 47 | 451 | 147 | 408 | | | | | | | | |
| 48 | 471 | 148 | 409 | | | | | | | | |
| 49 | 471 | 149 | 417 | | | | | | | | |
| 50 | 463 | 150 | 426 | | | | | | | | |
| 51 | 460 | 151 | 409 | | | | | | | | |
| 52 | 438 | 152 | 409 | | | | | | | | |
| 53 | 454 | 153 | 412 | | | | | | | | |
| 54 | 430 | 154 | 406 | | | | | | | | |
| 55 | 457 | 155 | 414 | | | | | | | | |
| 56 | 445 | 156 | 400 | | | | | | | | |
| 57 | 460 | 157 | 400 | | | | | | | | |
| 58 | 489 | 158 | 412 | | | | | | | | |
| 59 | 478 | 159 | 385 | | | | | | | | |
| 60 | 459 | 160 | 420 | | | | | | | | |
| 61 | 478 | 161 | 390 | | | | | | | | |
| 62 | 478 | 162 | 390 | | | | | | | | |
| 63 | 478 | 163 | 390 | | | | | | | | |
| 64 | 465 | 164 | 376 | | | | | | | | |
| 65 | 493 | 165 | 381 | | | | | | | | |
| 66 | 469 | 166 | 381 | | | | | | | | |
| 67 | 460 | 167 | 406 | | | | | | | | |
| 68 | 454 | 168 | 406 | | | | | | | | |
| 69 | 460 | 169 | 406 | | | | | | | | |
| 70 | 463 | 170 | 378 | | | | | | | | |
| 71 | 463 | 171 | 382 | | | | | | | | |
| 72 | 463 | 172 | 376 | | | | | | | | |
| 73 | 463 | 173 | 385 | | | | | | | | |
| 74 | 489 | 174 | 397 | | | | | | | | |
| 75 | 471 | 175 | 406 | | | | | | | | |

From Table 1, the following numerical information are deduced and given in Table 3. Here, $n_{=s}$ denote the number of rows identifying to $=_s$.

Table 2. Numerical information of the generator matrix Ψ of $C(2,27)$

| No. | $=_s$ | $n_{=s}$ | No. | $=_s$ | $n_{=s}$ |
|-----|-------|----------|-----|-------|----------|
| 1 | 28 | 11 | 39 | 406 | 6 |
| 2 | 145 | 1 | 40 | 408 | 1 |
| 3 | 187 | 2 | 41 | 409 | 9 |
| 4 | 225 | 1 | 42 | 412 | 3 |
| 5 | 232 | 3 | 43 | 414 | 1 |
| 6 | 235 | 1 | 44 | 415 | 3 |
| 7 | 274 | 1 | 45 | 417 | 2 |
| 8 | 303 | 1 | 46 | 418 | 1 |
| 9 | 313 | 2 | 47 | 420 | 4 |
| 10 | 322 | 2 | 48 | 421 | 4 |
| 11 | 331 | 2 | 49 | 423 | 3 |
| 12 | 340 | 2 | 50 | 424 | 3 |
| 13 | 343 | 1 | 51 | 426 | 3 |
| 14 | 345 | 2 | 52 | 427 | 4 |
| 15 | 352 | 2 | 53 | 430 | 6 |
| 16 | 355 | 3 | 54 | 433 | 3 |
| 17 | 357 | 1 | 55 | 435 | 1 |
| 18 | 361 | 2 | 56 | 436 | 3 |
| 19 | 364 | 3 | 57 | 438 | 3 |
| 20 | 367 | 2 | 58 | 439 | 1 |
| 21 | 369 | 1 | 59 | 442 | 5 |
| 22 | 370 | 2 | 60 | 445 | 5 |
| 23 | 372 | 1 | 61 | 447 | 2 |



| | | | | | |
|----|-----|---|----|-----|---|
| 24 | 373 | 4 | 62 | 448 | 4 |
| 25 | 376 | 4 | 63 | 451 | 3 |
| 26 | 378 | 1 | 64 | 454 | 2 |
| 27 | 379 | 8 | 65 | 457 | 1 |
| 28 | 381 | 2 | 66 | 459 | 1 |
| 29 | 382 | 2 | 67 | 460 | 4 |
| 30 | 384 | 1 | 68 | 462 | 4 |
| 31 | 385 | 4 | 69 | 463 | 7 |
| 32 | 388 | 3 | 70 | 465 | 1 |
| 33 | 390 | 3 | 71 | 469 | 1 |
| 34 | 391 | 4 | 72 | 471 | 3 |
| 35 | 396 | 1 | 73 | 478 | 5 |
| 36 | 397 | 3 | 74 | 489 | 2 |
| 37 | 400 | 5 | 75 | 493 | 1 |
| 38 | 403 | 8 | | | |

The first row r_1 and last row r_{217} of Ψ are given below.

From the above details, the following theorem is deduced.

Theorem 2.1: The code $C(2,27)$ is $C[757,217,28]$ with $e = 13$ and the weight distributions A_i where $28 \leq i \leq 493$, of some codewords are given in Table 3.

Table 3. Weight distributions of $C(2,27)$

| No. | i | $\leq A_i$ | No. | i | $\leq A_i$ |
|-----|-----|------------|-----|-----|------------|
| 1 | 0 | 1 | 56 | 382 | 572040 |
| 2 | 28 | 11 | 57 | 384 | 208915 |
| 3 | 145 | 1 | 58 | 385 | 411688 |

| | | | | | |
|----|-----|--------|-----|-----|--------|
| 4 | 187 | 2 | 59 | 387 | 141123 |
| 5 | 225 | 1 | 60 | 388 | 276142 |
| 6 | 232 | 3 | 61 | 390 | 88094 |
| 7 | 235 | 1 | 62 | 391 | 171354 |
| 8 | 274 | 1 | 63 | 393 | 49373 |
| 9 | 303 | 1 | 64 | 394 | 97457 |
| 10 | 313 | 2 | 65 | 396 | 26695 |
| 11 | 315 | 1 | 66 | 397 | 51446 |
| 12 | 316 | 6 | 67 | 399 | 13392 |
| 13 | 318 | 11 | 68 | 400 | 24926 |
| 14 | 319 | 36 | 69 | 402 | 5978 |
| 15 | 321 | 34 | 70 | 403 | 11621 |
| 16 | 322 | 132 | 71 | 405 | 2513 |
| 17 | 324 | 156 | 72 | 406 | 4687 |
| 18 | 325 | 277 | 73 | 408 | 912 |
| 19 | 327 | 571 | 74 | 409 | 1696 |
| 20 | 328 | 771 | 75 | 411 | 314 |
| 21 | 330 | 1131 | 76 | 412 | 646 |
| 22 | 331 | 2326 | 77 | 414 | 88 |
| 23 | 333 | 2597 | 78 | 415 | 188 |
| 24 | 334 | 5234 | 79 | 417 | 44 |
| 25 | 336 | 6286 | 80 | 418 | 46 |
| 26 | 337 | 11643 | 81 | 420 | 9 |
| 27 | 339 | 12941 | 82 | 421 | 21 |
| 28 | 340 | 24909 | 83 | 423 | 2 |
| 29 | 342 | 25913 | 84 | 424 | 6 |
| 30 | 343 | 49282 | 85 | 426 | 3 |
| 31 | 345 | 46016 | 86 | 427 | 4 |
| 32 | 346 | 90768 | 87 | 430 | 6 |
| 33 | 348 | 80597 | 88 | 433 | 3 |
| 34 | 349 | 156121 | 89 | 435 | 1 |
| 35 | 351 | 129584 | 90 | 436 | 3 |
| 36 | 352 | 253985 | 91 | 438 | 3 |
| 37 | 354 | 190027 | 92 | 439 | 1 |
| 38 | 355 | 377754 | 93 | 442 | 5 |
| 39 | 357 | 263616 | 94 | 445 | 5 |
| 40 | 358 | 528767 | 95 | 447 | 2 |
| 41 | 360 | 342185 | 96 | 448 | 4 |
| 42 | 361 | 689293 | 97 | 451 | 3 |
| 43 | 363 | 413522 | 98 | 454 | 2 |
| 44 | 364 | 835372 | 99 | 457 | 1 |
| 45 | 366 | 467226 | 100 | 459 | 1 |
| 46 | 367 | 941145 | 101 | 460 | 4 |
| 47 | 369 | 492408 | 102 | 462 | 4 |
| 48 | 370 | 987442 | 103 | 463 | 7 |
| 49 | 372 | 476411 | 104 | 465 | 1 |
| 50 | 373 | 963073 | 105 | 469 | 1 |
| 51 | 375 | 433169 | 106 | 471 | 3 |
| 52 | 376 | 875170 | 107 | 478 | 5 |
| 53 | 378 | 366524 | 108 | 489 | 2 |
| 54 | 379 | 731494 | 109 | 493 | 1 |
| 55 | 381 | 286103 | | | |

A dual code of a $C[n, k, d]$ over F_q , denoted by C^\perp , is defined by

$$C^\perp = \left\{ (x_1, \dots, x_n) \in F_q^n : \sum_{i=1}^n x_i c_i = 0 \right\}$$

For all $c = (c_1, \dots, c_n) \in \mathcal{C}$.

It is known that C^\perp has length n and dimension $n - k$, see [4]. The relation between the generator matrices of code and its dual code is as follows:

$G = [I_k A_{k \times n}]$ is generator matrix of a code $C[n, k]$ iff $H = [-A^T I_{n \times (n-k)}]$ is a generator matrix of C^\perp , see [4].

Therefore, the following code is founded.

Corollary 2.2: The dual code of $C(2,27)$ is $C[757,540,140]$ with $e = 69$.

Proof: The first row s_1 and last row s_{217} of the generator matrix of C^\perp are as below:

CONCLUSIONS

From points and lines of 2-dimensional projective space over the finite field $GF(27)$, the code $C(2,27)$ of length 757, dimension 217 and minimum weight 28 has been founded using incident matrix over $p = 3$. The generator matrix of the code has been given by gave details of its rows using support function. From this code, another code, which is the dual code, has been computed. Also, some of weight distributions of $C(2,27)$ have been computed.

ACKNOWLEDGMENT

The authors thank the University of Mustansiriyah for their supported; also, thanks the Department of Mathematics at College of Science for provide a good environment to do this research.

REFERENCES

- [1] E F Assmus and J D Key, *Designs and their codes*. Cambridge; New York, USA: Cambridge University Press, 1992. ISBN-13: 978-0521413619.
 - [2] B Bagchi and S P Inamdar , "Projective geometric codes," *Journal of Combinatorial Theory, Series A*, vol. 99, no. 1, pp. 128-142, 2002.
 - [3] B A Dubrovin , A T Fomenko, and S P Novikov, *Modern geometry methods and application: Part 1. The geometry of surfaces, transformation groups, and fields*. New York: Springer Verlag, 1985. ISBN-13: 978-0387976631.
 - [4] F J MacWilliams and NJ A Sloane, *The Theory of error-correcting codes*, 6th ed. Amsterdam: North-Holland Publishing Company, 1977. ISBN: 0 444 85009 0.
 - [5] J W P Hirschfeld, *Projective geometries over finite fields*, 2nd ed. New York: Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, 1998. ISBN: 9780198502951.
 - [6] O Olmez, "A link between combinatorial designs and three-weight linear codes," *Designs Codes and Cryptography*, vol. 86, no. 9, pp. 1-17, 2017.
 - [7] C Ding, C. Li, N. Li and Z. Zhou, "Three-weight cyclic codes and their weight distributions," *Discrete Mathematics*, vol. 339, no. 2, pp. 415-427, 2016.
 - [8] L Gaojun, X Cao, S Xu, and J Mi, "Binary linear codes with two or three weights from niho exponents," *Cryptography and Communications*, vol. 10, no. 2, pp. 301-318, 2018.
 - [9] C Li, Q Yue, and F Fu, "A construction of several classes of two-weight and threeweight linear codes," *Applicable Algebra in Engineering Communication and Computing*, vol. 28, no. 1, pp. 1-20, 2018.
 - [10] Y W Liu and Z H Liu, "On some classes of codes with a few weights," *Adv. Math. Commun.*, pp. 415-428, 2018.
 - [11] Z Yao, and C Zhao, "The weight distributions of two classes of p-ary cyclic codes with few weights," *Finite Fields and Their Applications*, vol. 44, pp. 76-91, 2017.
 - [12] The GAP Group. (2020) GAP. Reference manual. [Online]. <https://www.gap-system.org/>.