RESEARCH
O&G Forum 2024; 34-3s: 1663-1665

APPLICATIONS OF THE PG (2,8) IN CODING THEORY

Marwa Hussein Rajab Hussein[1], Nada Yassen Kasm Yahya[2]

[1,2]Department of Mathematics, College of Education for Pure science, University of Mosul, Iraq
Drnadaqasim3@uomosul.edu.iq, Marwa.21esp28@student.uomosul.edu.iq

Abstract
In this research, we studied the projective level, the finite even field, and the theory of encryption. We found the lines and points using an array. We have created an incidence matrix with a zero-one system. We collect the elements of (0,1,2,3,4,5,6,7) with the incidence matrix. We found that the maximum value we obtained was 72, and the lowest value was 9. We tested the code. Is it perfect or not.
Keywords: projective plane, finite field

Introduction
In symbology theory, many scientists have studied a planar Gallo field projective to a finite field for example Hirschfeld [1],[3] Many researchers have studied the theories and definitions between projective geometry and coding theory. AL-Seraji [4] Two papers presented important results on the relationship between the projective level of command 17 and the error correction code. Hill [2]. Classification of some concepts and study of the tools of the notation theorem AL-Zangana [5] They presented the relationship the projective level and command 19 - correcting the code and the error values. Also, Yahya and AL-Zangana studied linear cobles [6] [7]. In this research, we studied the eighth-order even field, the projective plane, and the coding theory

Theorem1.1[1](sphere packing or Hamming bound)
A q– ary (n,M, d) – code *k* satisfies
$M\{\binom{n}{0}+\binom{n}{1}(q-1)+\cdots+\binom{n}{e}(q\text{- }1)^{e}\}\leq q^{n}$

Corollary1.2.[1] A q- ary (n ,M , d) code k is perfect if and only if equality holds in Theorem 1.1

Definition 1.3 [1] A q - ary code k The subset of length is n of $(F_q)^n$

Example 1.4 [1] There are two messages sent a and b, the symbols yes = a, no = b are encrypted. If there is an error in sending the message, for example it has been sent, it will not be detected so he added some redundancy in the symbols when sending it: yes =aa, no .bb. Now, if aa is sent and ba arrives, it means that the error in the message has been detected, and not corrected in the message, since the messages in the original code aa and bb are accepted with the same value. Therefore, we added several recurring symbols: yes = aaa, no = bbb. Now if bab arrives, there is one error or two or more lines, then we know there is bbb. You have been sent: The original message was no. The finite Gallo field is classified as cubic curves of order eight The equation for the even field is F (y)= y3 – y2 – ʎ3 the element in F8 = (0,1,2,3,4,5,6,7) of PG (2,8) as follows:

$$r(i) = [1 , 0,0]\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ ʎ^{3} & 0 & 1 \end{pmatrix}^{i} \quad , i=0,\ldots\ldots\ldots..,72.$$

The point of PG (2,8) are: r_0=[1,0,0], r_1=[2,3,0], r_2= [5,6,1]…….. ,r_{71} = [1,6,6], r_{72} = [1,7,7]
r_i = i , i = 0,1……..,72 each straight line contains 9 points where the first straight line is r_0 =[1,0,0], r_1=[0,1,0], r_{11}=[1,2,0], r_{20}=[1,7,0], r_{38}=[1,3,0], r_{43}=[1,3,7], r_{59}=[1,4,0] r_{67}=[1,6,0], r_{71}=[1,6,6]

$$\ell i = \ell_0\, c(g\,)^{i} \;=\; \ell_0\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ ʎ^{3} & 0 & 1 \end{pmatrix}^{i} \qquad i= 0,1,\ldots\ldots\ldots..,72\ \ell 0$$

: Lines in the finite field q = 8

ℓ0	0	1	11	20	38	43	59	67	71
ℓ1	1	2	12	21	39	44	60	68	72
ℓ2	2	3	13	22	40	45	61	69	0
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
ℓ 69	69	70	7	16	34	39	55	63	67
ℓ 70	70	71	8	17	35	40	56	64	68
ℓ 71	71	72	9	18	36	41	57	65	69
ℓ 72	72	0	10	19	37	42	58	66	70

Theorem (2.1) Gallo field in the projective plane of 8 is a code symbole k with other parameters
n=q2+q+1,d=2e+1,e=4,m=q2+q+1-k
[n = 73 , m ≤ 8^{70} , d = 9]
Proof: π_8 has an z = (bij), where

$$bij = \begin{cases} 1 & if\ \ p_j \in \ell_i \\ 0 & if\ \ p_j \notin \ell_i \end{cases}$$

z=

1100000000010000000010000000000000000010000100000000000000010000000100010
0110000000001000000001000000000000000001000010000000000000001000000010001
1011000000000100000000100000000000000000100001000000000000000100000001000
0101100000000010000000010000000000000000010000100000000000000010000000100
0010110000000001000000001000000000000000001000010000000000000001000000010
0001011000000000100000000100000000000000000100001000000000000000100000001
1000101100000000010000000010000000000000000010000100000000000000010000000
0100010110000000001000000001000000000000000001000010000000000000001000000
0010001011000000000100000000100000000000000000100001000000000000000100000
0001000101100000000010000000010000000000000000010000100000000000000010000
0000100010110000000001000000001000000000000000001000010000000000000001000
0000010001011000000000100000000100000000000000000100001000000000000000100
0000001000101100000000010000000010000000000000000010000100000000000000010
0000000100010110000000001000000001000000000000000001000010000000000000001
1000000010001011000000000100000000100000000000000000100001000000000000000
0100000001000101100000000010000000010000000000000000010000100000000000000
0010000000100010100000000001000000001000000000000000001000010000000000000
0001000000010001011000000000100000000100000000000000000100001000000000000
0000100000001000101100000000010000000010000000000000000010000100000000000
0000010000000100010110000000001000000001000000000000000001000010000000000
0000001000000010001011000000000100000000100000000000000000100001000000000
0000000100000001000101100000000010000000010000000000000000010000100000000
0000000010000000100010110000000001000000001000000000000000001000010000000
0000000001000000010001011000000000100000000100000000000000000100001000000
0000000000100000001000101100000000010000000010000000000000000010000100000
0000000000010000000100010110000000001000000001000000000000000001000010000
0000000000001000000010001010000000000100000000100000000000000000100001000
0000000000000100000001000101100000000010000000010000000000000000010000100
0000000000000010000000100010110000000001000000001000000000000000001000010
0000000000000001000000010001011000000000100000000100000000000000000100001
1000000000000000100000001000101100000000010000000010000000000000000010000
0100000000000000010000000100010110000000001000000001000000000000000001000
0010000000000000001000000010001011000000000100000000100000000000000000100
0001000000000000000100000001000101100000000010000000010000000000000000010
0000100000000000000010000000100010110000000001000000001000000000000000001
1000010000000000000001000000010001011000000000100000000100000000000000000
0100001000000000000000100000001000101100000000010000000010000000000000000
0010000100000000000000010000000100010110000000001000000001000000000000000
0001000010000000000000001000000010001011000000000100000000100000000000000
0000100001000000000000000100000001000101100000000010000000010000000000000
0000010000100000000000000010000000100010110000000001000000001000000000000
0000001000010000000000000001000000010001011000000000100000000100000000000
0000000100001000000000000000100000001000101100000000010000000010000000000
0000000010000100000000000000010000000100010110000000001000000001000000000

```
0000000000100001000000000000000100000001000101100000000010000000010000000
0000000000010000100000000000000010000000100010110000000001000000001000000
0000000000001000010000000000000001000000010001011000000000100000000100000
0000000000000100001000000000000000100000001000101100000000010000000010000
0000000000000010000100000000000000010000000100010110000000001000000001000
0000000000000001000010000000000000001000000010001011000000000100000000100
0000000000000000100001000000000000000100000001000101100000000010000000010
0000000000000000010000100000000000000010000000100010110000000001000000001
1000000000000000001000010000000000000001000000010001011000000000100000000
0100000000000000000100001000000000000000100000001000101100000000010000000
0010000000000000000010000100000000000000010000000100010110000000001000000
0001000000000000000001000010000000000000001000000010001011000000000100000
0000100000000000000000100001000000000000000100000001000101100000000010000
0000010000000000000000010000100000000000000010000000100010110000000001000
0000001000000000000000001000010000000000000001000000010001011000000000100
0000000100000000000000000100001000000000000000100000001000101100000000010
0000000010000000000000000010000100000000000000010000000100010110000000001
1000000001000000000000000001000010000000000000001000000010001011000000000
0100000000100000000000000000100001000000000000000100000001000101100000000
0010000000010000000000000000010000100000000000000010000000100010110000000
0001000000001000000000000000001000010000000000000001000000010001011000000
0000100000000100000000000000000100001000000000000000100000001000101100000
0000010000000010000000000000000010000100000000000000010000000100010110000
0000001000000001000000000000000001000010000000000000001000000010001011000
0000000100000000100000000000000000100001000000000000000100000001000101100
0000000010000000001000000000000000001000010000000000000001000000010001011 0
0000000001000000000100000000000000000100001000000000000000100000001000101 1
1000000000100000000100000000000000000100001000000000000000100000001000101
```

These are field elements that we combine with an array to find the symbol values
a = (00000……000000), b = (11111…….1111111), c = (2222 .... 22222) d = (3333........ 33333),
e = (4444.......... 4444), i = (5555....... 5555), j = (66666............ 666666)
l = (77777....... 77777), $0 \leq i \leq 72$

Let $m_i = c + \ell_i$

Point	0	1	2			70	71	72
m_0	0	0	1	.	.	1	0	1
m_1	1	0	0	.	.	1	1	0
	.	.	.	.	.	.	.	.
m_{71}	1	1	1	.	.	1	0	0
m_{72}	0	1	1	.	.	0	1	0

Let $v_i = c + \ell_i$

	0	1	2			70	71	72
v_0	6	6	2	.	.	2	6	2
v_1	2	6	6	.	.	2	2	6
	.	.	.	.	.	.	.	.
v_{71}	2	2	2	.	.	2	6	6
v_{72}	6	2	2	.	.	6	2	6

Let $f_i = d + \ell_i$

Point	0	1	2	.	.	70	71	72
f_0	4	4	3	.	.	3	4	3
f_1	3	4	4	.	.	3	3	4
	.	.	.	.	.	.	.	.
f_{71}	3	3	3	.	.	3	4	4
f_{72}	4	3	3	.	.	4	3	4

Let $h_i = e + \ell_i$

	0	1	2			70	71	72
h_0	3	3	4	.	.	4	3	4
h_1	4	3	3	.	.	4	4	3
	.	.	.	.	.	.	.	.
h_{71}	4	4	4	.	.	4	3	3
h_{72}	1	4	4	.	.	3	4	3

Let $k_i = I + \ell_i$

Point	0	1	2			70	71	72
k_0	7	7	5	.	.	5	7	5
k_1	5	7	7	.	.	5	5	7
	.	.	.	.	.	.	.	.
k_{71}	5	5	5	.	.	5	7	7
k_{72}	7	5	5		.	7	5	7

Let $gi = j + \ell i$

Point	0	1	2	.	.	70	71	72
g_0	2	2	6	.	.	6	2	6
g_1	6	2	2	.	.	6	6	2
	.	.	.	.	.	.	.	.
g_{71}	6	6	6	.	.	6	2	2
g_{72}	2	6	6	.	.	2	6	2

Let $n_i = l + \ell_i$

Point	0	1	2	.	.	70	71	72
n_0	5	5	7	.	.	7	5	7
n_1	7	5	5	.	.	7	7	5
	.	.	.	.	.	.	.	.
n_{71}	7	7	7	.	.	7	5	5
n_{72}	5	7	7	.	.	5	7	5

We calculated the from the table above, where: $n = q^2+q+1$, $d = 2e+1$, $e = 2.2=4$, not consistent with the theorem 1.1, we get $M = 8^{70}$ Hence k is a (73, 870,9) – code

$8^{70}\left\{ \binom{73}{0} + \binom{73}{1}(7) + \binom{73}{2}(7)2 + \binom{73}{3}(7)3 + \binom{73}{4}(7)4 \right\} \leq 8^{73}$

By Corollary 1.2, therefor k is not perfect
Theorem (2.2) C is a subspace of $((F_8)73, +, .)$ over $(F_8, +2, .2)$

Conclusion

We have built a relationship between the finite Gallo field with the symbol theory and the projective plane and found the points, lines and parameters n, k and d depending on the field elements in GF(8). found the shortest distance between us each two different points, which is 9, and the highest distance, which is 72, and this achieves the equation q2+q+1nd the value The error was verifying the equation 2e+1

Acknowledgments

The authors would like to thank university of Mosul (http:// www. Uomosul .edu. iq) Mosul, Iraq, for its support in the present work.

References

1. *Hirschfeld, J. W. P. 2014. Coding Teory. lecturs. Brightanisussex University*
2. *Hirschfeld, J. W. P. 1998. Projective geometries over finite fields. 2nd Edition, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York*
3. *Hill, R. 1986. A first course in coding theory, Clarendon Press, Oxford.*
4. *Al-Seraji. N.A.M. 2010. The Geometry of The Plane of order Seventeen and its Application to Error-correcting Codes, Ph.D. Thesis, University of Sussex, UK.*

5. Al-Zangana Emad, B.A. 2011. The Geometry of The Plane of order Nineteen and its Application to Error-correcting Codes, Ph.D. Thesis, University of Sussex, UK

6. Yahya N.Y.K., AL- Zangana, E.B., 2021. The non – existence of [1864,3,1828]53 linear code by cmbinntorid Techniqus in in ternationnal journal of Mathematics and computer science 16(4), 1575 – 1585.

7. Abdullah, F.N. & Yahya, N, Y, K, 2021 Bounds on Minimum Distance for linear codes over GF (q)ltalian journal of pur and Applied Mathematics, n,45, p. 894 – 403. Issn 2239-0227.