

Some Applications of Coding Theory in the Projective Plane of Order Four

Najm A. M. AL-Seraji*, Hamza L. M. Ajaj

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

² Author 2 departments, Faculty name, University of Baghdad, IRAQ

*Correspondent author email: dr.najm@uomustansiriyah.edu.iq

Article Info

Received
19/02/2018

Accepted
12/06/2018

Published
15/08/2019

Abstract

The main aim of this research is to introduce the relationship between the topic of coding theory and the projective plane of order four. The maximum value of size code M over finite field of order four and an incidence matrix with the parameters, n (length of code), d (minimum distance of code) and e (error-correcting of code) have been constructed. Some examples and theorems have been given.

Keywords: Projective Plane, Coding Theory, Incidence Matrix.

الخلاصة

الهدف الرئيسي لهذا البحث هو تقديم العلاقة بين موضوع نظرية الترميز و المستوي الاسقاطي من الرتبة الرابعة . القيمة العظمى لحجم الرمز M حول الحقل المنتهي من الرتبة الرابعة ومصفوفة الاصابة مع المعلمات n (طول الرمز), d (اقل مسافة للرمز) و e (تصحيح رمز الاخطاء) تم تشكيلها . بعض الامثلة و النظريات اعطيت.

Introduction

The subject of this research depends on themes of Projective geometry over a finite field, Group theory, Field theory, Coding theory.

The brief history of this theme is shown as follows. All theorems and definitions of the research are taken from James Hirshfeld [1]. In 1986, R. Hill [2] studied A first course in coding theory. In 2010, N. A. M. Al-Seraji [3] showed the arcs in projective plane of order seventeen. In 2011, B. A. Al-Zangana Emad [4] described the arcs in projective plane of order nineteen. In 1998, Hirschfeld, J. W. P [5] classified projective geometries over finite fields. In 2013, N.A.M. Al-Seraji [6] classified the almost maximum distance separable codes. In 2013, N.A.M. Al-Seraji [7] described a generalized of optimal codes. In 2012, N.A.M. Al-Seraji [8] studied the optimal Code.

Background

The following results are interesting to area of research.

Theorem (2.1) [1].

A $q - ary (n, M, 2e + 1) - code C$ satisfies:

$$M\left\{\binom{n}{0} + \binom{n}{1}(q - 1) + \dots + \binom{n}{e}(q - 1)^e\right\} \leq q^n.$$

Theorem (2.2) [1].

W is a subspace of a vector space V over a finite $(F, +, \cdot)$ if and only if:

- (i) W is a nonempty subset of V
(i.e. $\phi \neq C \subseteq X$).
- (ii) W is closed under the binary operation $+$ defined on V (i.e. $x + c \in C$).
- (iii) W is closed under the scalar multiplication defined on $F \times V$
(i.e. $k \cdot v \in W \forall k \in F$ and $\forall v \in W$).

Definition (2.3) [5]:

Let $f(X) = X^n - a_{n-1}X^{n-1} - \dots - a_0$ be a monic polynomial of degree $n \geq 1$ over F_q . Its companion matrix $C(f)$ is given by the $n \times n$ matrix

$$C(f) = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \end{bmatrix}$$

$$\ell_i = \ell_0 C(g)^i = \ell_0 \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \theta^2 & \theta & \theta^2 \end{pmatrix}^i, \quad i = 0, 1, \dots, 20$$

The classification of cubic curves over a finite field of order 4

Let the polynomial $g_1(x) = x^2 + x + 1$ and $F_4 = \frac{F_2[x]}{\langle g_1(x) \rangle}$ which has 4 elements namely $0, 1, \theta, \theta^2$ where θ be x plus the ideal $\langle g_1(x) \rangle$ generated by polynomial of degree 2 with coefficients in $F_2 = \{0, 1\}$. The polynomial $g_2(x) = x^3 + \theta^2 x^2 + \theta x + \theta^2$ is primitive over F_4 , since $g_2(0) = \theta^2, g_2(1) = \theta^2, g_2(\theta) = \theta^2$ and $g_2(\theta^2) = \theta$, this means g_2 is irreducible over F_4 , also $g_2(\beta^{11}) = g_2(\beta^{44}) = g_2(\beta^{50}) = 0$, where $\beta^{11}, \beta^{44}, \beta^{50}$ in F_{4^3} , this means g_2 is reducible over F_{64} . The companion matrix of $g_2(x) = x^3 + \theta^2 x^2 + \theta x + \theta^2$ generated the points and lines of $PG(2,4)$ as follows:

$$P_i = [1, 0, 0]C(g)^i = [1, 0, 0] \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \theta^2 & \theta & \theta^2 \end{pmatrix}^i, \quad i = 0, 1, \dots, 20$$

The points of $PG(2,4)$ are:

- $P_0 = [1, 0, 0]$
- $P_1 = [0, 1, 0]$
- $P_2 = [0, 0, 1]$
- $P_3 = [1, \theta^2, 1]$
- $P_4 = [1, 1, 0]$
- $P_5 = [0, 1, 1]$
- $P_6 = [\theta, 1, 1]$
- $P_7 = [\theta, 0, 1]$
- $P_8 = [1, 0, 1]$
- $P_9 = [1, 1, 1]$
- $P_{10} = [\theta, \theta, 1]$
- $P_{11} = [\theta^2, 0, 1]$
- $P_{12} = [1, \theta, 1]$
- $P_{13} = [\theta^2, \theta^2, 1]$
- $P_{14} = [\theta^2, 1, 0]$
- $P_{15} = [0, \theta^2, 1]$
- $P_{16} = [\theta, 1, 0]$
- $P_{17} = [0, \theta, 1]$
- $P_{18} = [\theta^2, \theta, 1]$
- $P_{19} = [\theta^2, 1, 1]$
- $P_{20} = [\theta, \theta^2, 1]$

With select the points in $PG(2,4)$ such that the third coordinate equal to zero, this means belong to $\ell_0 = v(z)$ such that $v(z) = tz = z$ for all t in $F_4 \setminus \{0\}$ therefore, and with $P_i = i, i = 0, 1, \dots, 20$, we obtain

$$\ell_0 = \{0, 1, 4, 14, 16\}$$

Remove this,

The lines of $PG(2,4)$ are:

ℓ_0	0	1	4	14	16
ℓ_1	1	2	5	15	17
ℓ_2	2	3	6	16	18
ℓ_3	3	4	7	17	19
ℓ_4	4	5	8	18	20
ℓ_5	5	6	9	19	0
ℓ_6	6	7	10	20	1
ℓ_7	7	8	11	0	2
ℓ_8	8	9	12	1	3
ℓ_9	9	10	13	2	4
ℓ_{10}	10	11	14	3	5
ℓ_{11}	11	12	15	4	6
ℓ_{12}	12	13	16	5	7
ℓ_{13}	13	14	17	6	8
ℓ_{14}	14	15	18	7	9
ℓ_{15}	15	16	19	8	10
ℓ_{16}	16	17	20	9	11
ℓ_{17}	17	18	0	10	12
ℓ_{18}	18	19	1	11	13
ℓ_{19}	19	20	2	12	14
ℓ_{20}	20	0	3	13	15

In the following theorem the parameters n, M, d are constructed.

Theorem (3.1). The projective plane of order four is a code C with a parameter $[n = 21, M \leq 4^{17}, d = 5]$.

Proof:

The plane π_4 has an incidence matrix $A = (a_{ij})$, where

$$a_{ij} = \begin{cases} 1 & \text{if } P_j \in \ell_i, \\ 0 & \text{if } P_j \notin \ell_i. \end{cases}$$

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}
l_0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
l_1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0
l_2	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0
l_3	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0
l_4	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1
l_5	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0
l_6	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1
l_7	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0
l_8	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0
l_9	0	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0
l_{10}	0	0	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0
l_{11}	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0
l_{12}	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0
l_{13}	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0
l_{14}	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0
l_{15}	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	1	0
l_{16}	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	1
l_{17}	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0
l_{18}	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0
l_{19}	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1
l_{20}	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1

Let

$$a=[0 \ 0]$$

$$u=[1 \ 1]$$

$$w=[0 \ 0]$$

$$y=[\theta^2 \ \theta^2]$$

$$m_i=u+l_i.$$

That is,

m_0	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1
m_1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1
m_2	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1	1
m_3	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1
m_4	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0
m_5	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0	1
m_6	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0
m_7	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1
m_8	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1
m_9	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1
m_{10}	1	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1
m_{11}	1	1	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1
m_{12}	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1
m_{13}	1	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1
m_{14}	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1
m_{15}	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1
m_{16}	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1	1	0

m_{17}	0	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1	1
m_{18}	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1
m_{19}	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	0
m_{20}	0	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0

Let $v_i = w + \ell_i$

That is,

v_0	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o
v_1	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o
v_2	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o
v_3	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o^2	o	o^2	o
v_4	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o^2	o	o^2
v_5	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o^2	o
v_6	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o^2
v_7	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o	o
v_8	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o	o
v_9	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o	o
v_{10}	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o	o
v_{11}	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o	o
v_{12}	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o	o
v_{13}	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o	o
v_{14}	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2	o
v_{15}	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o	o^2
v_{16}	o	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o	o^2
v_{17}	o^2	o	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2	o
v_{18}	o	o^2	o	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2	o^2
v_{19}	o	o	o^2	o	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o	o^2
v_{20}	o^2	o	o	o^2	o	o	o	o	o	o	o	o	o	o^2	o	o^2	o	o	o	o^2

Let $z_i = y + \ell_i$

That is,

z_0	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o	o^2	o	o^2	o^2	o^2	o^2
z_1	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o	o^2	o	o^2	o^2	o^2
z_2	o^2	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o	o^2	o	o^2	o^2
z_3	o^2	o^2	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o	o^2	o	o^2
z_4	o^2	o^2	o^2	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o	o^2	o
z_5	o	o^2	o^2	o^2	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o
z_6	o^2	o	o^2	o^2	o^2	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o
z_7	o	o^2	o	o^2	o^2	o^2	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2	o^2
z_8	o^2	o	o^2	o	o^2	o^2	o^2	o^2	o	o	o^2	o^2	o	o^2	o^2	o^2	o^2	o^2	o^2	o^2

z_9	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2
z_{10}	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2
z_{11}	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2
z_{12}	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2
z_{13}	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2	\circ	\circ^2	\circ^2	\circ^2
z_{14}	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2	\circ	\circ^2	\circ^2
z_{15}	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2	\circ	\circ^2
z_{16}	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2	\circ^2
z_{17}	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ	\circ^2
z_{18}	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ
z_{19}	\circ^2	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ
z_{20}	\circ	\circ^2	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ^2	\circ	\circ^2	\circ	\circ^2	\circ^2	\circ^2	\circ^2	\circ

$d(a, \ell_i) = 5$	$d(a, v_i) = 21$
$d(u, \ell_i) = 16$	$d(v_i, v_j) = 8, i \neq j$
$d(w, \ell_i) = 21$	$d(u, v_i) = 21$
$d(y, \ell_i) = 21$	$d(w, v_i) = 5$
$d(\ell_i, \ell_j) = 8, i \neq j$	$d(y, v_i) = 16$
$d(\ell_i, m_i) = 21$	$d(a, z_i) = 21$
$d(a, u) = 21$	$d(z_i, z_j) = 8, i \neq j$
$d(a, w) = 21$	$d(u, z_i) = 21$
$d(a, y) = 21$	$d(w, z_i) = 16$
$d(u, w) = 21$	$d(y, z_i) = 5$
$d(u, y) = 21$	$d(v_i, m_j) = 21, i \neq j$
$d(w, y) = 21$	$d(z_i, m_j) = 21, i \neq j$
$d(u, m_i) = 5$	$d(z_i, \ell_j) = 21, i \neq j$
$d(a, m_i) = 16$	$d(v_i, \ell_j) = 21, i \neq j$
$d(\ell_i, m_j) = 13, i \neq j$	$d(v_i, z_j) = 13, i \neq j$
$d(m_i, m_j) = 8, i \neq j$	
$d(w, m_i) = 21$	
$d(y, m_i) = 21$	

Such that $\circ = \theta$. The remain vectors of code C are constructed by combination of $a, u, w, y, \ell_i, m_i, v_i, z_i$, where $i = 0, 1, \dots, 20$.

Note that $d(\ell_i, \ell_j) =$ number of points on exactly one of ℓ_i or ℓ_j . Then:

If we substitute the values of $n = 21, d = 5, e = 2$, in inequality of theorem (2.1), we get $M \leq 4^{17}$. Hence C is a $(21, M, 5)$ -code.

The goal of the following theorem is to show that the code C is closed under the operation of addition modulo 4:

Theorem (3.2). The code $C = [n = 21, M \leq 4^{17}, d = 5]$ which is derived from the projective plane of order four is linear; that is, the sum modulo 2 of any two elements of C is in C .

Proof: Here is the geometry with $P_i = i$, where $i = 0, \dots, 20$.

Then $\ell_i + \ell_j = a_i$, where $i, j = 0, \dots, 20$. Such that

$$a_r = 1 \Leftrightarrow P_r \text{ lies on precisely one of } \ell_i, \ell_j,$$

$$a_r = 0 \Leftrightarrow P_r \text{ lies on the third line through } \ell_i \cap \ell_j.$$

Here $\ell_i + \ell_j, \ell_i + u, \ell_i + w, \ell_i + y, \ell_i + m_i, \ell_i + v_i, \ell_i + z_i$ in C .

$m_i + m_j, m_i + u, m_i + w, m_i + y, m_i + v_i, m_i + z_i$ in C .

$v_i + v_j, v_i + u, v_i + w, v_i + y, v_i + z_i$ in C .

$z_i + z_j, z_i + u, z_i + w, z_i + y$ in C .

Theorem (3.3). The code $C = [n = 21, M \leq 4^{17}, d = 5]$ is a subspace of the vector space $((F_4)^{21}, +, \cdot)$ over a finite field $(F_4, +_2, \cdot_2)$.

Proof: The vector $a = \underbrace{0, 0, \dots, 0}_{21\text{-time}} \in C$. Thus

$C \neq \phi$.

$\forall X = (x_1, x_2, \dots, x_{21}), Y = (y_1, y_2, \dots, y_{21}) \in C$. From Theorem (3.2), we get $X + Y \in C$.

$\forall k \in F_4$ and $X \in C$, we have
 $k \cdot X = k(x_1, x_2, \dots, x_{21}) =$
 $(k \cdot_2 x_1, k \cdot_2 x_2, \dots, k \cdot_2 x_{21}) \in C$. Thus, by
Theorem (2.2), C is a subspace of $((F_4)^{21}, +, \cdot)$
over $(F_4, +_2, \cdot_2)$.

References:

- [1] J.W.P. Hirschfeld, "Coding Theory" Lectures, Sussex University, UK, 2014.
- [2] R. Hill, "A first course in coding theory", Clarendon Press, Oxford, 1986.
- [3] N.A.M. Al-Seraji, "The Geometry of The Plane of order Seventeen and its Application to Error-correcting Codes", Ph.D. Thesis, University of Sussex, UK, 2010.
- [4] E. M. Al-Zangana, "The Geometry of The Plane of order Nineteen and its Application to Error-correcting Codes" Ph.D. Thesis, University of Sussex, UK, 2011.