



Near-*MDS* Codes of Degree Three over the Galois Field of Order 25

Sadeq Hamdallah Naji

Emad Bakr Al-Zangana

Abdulrasool Hasan Sultan Al-Huseniawi

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

alhsynawysadq278@gmail.com

e.b.abdulkareem@uomustansiriyah.edu.iq,

rassolhussanawi55@yahoo.com,

ABSTRACT. In the projective plane $PG(2, q)$ a $(n; 3)$ -arc may be generated by a non-singular cubic curve, which generates an almost-*MDS* code. In this work, 108 novel nearly-*MDS* codes are constructed from nonsingular cubic curves over the order 25 Galois field, and their nearly-*MDS* status is shown. With the exception of 26 and 26, which are incomplete, these codes are between 16 and 36 characters long. Also supplied are the covering radius and weight distributions for these codes.

Key Words: elliptic cubic curves, *Arc*, Weight distributions, Near-*MDS*-code

رموز MDS القريبة من الدرجة الثالثة فوق حقل جالوا من الرتبة 25

صادق حمد الله ناجي

عماد بكر الزنجانا

عبدالرسول حسن سلطان الحسينياوي

قسم الرياضيات، كلية العلوم، الجامعة المستنصرية، بغداد، العراق

aalhsynawysadq278@gmail.com

ce.b.abdulkareem@uomustansiriyah.edu.iq

Brassolhussanawi55@yahoo.com,

خلاصة

في المستوى الإسقاطي $PG(2, q)$ ، يمكن إنشاء قوس $(n; 3)$ بواسطة منحنى مكعب غير مفرد، والذي يولد رمز MDS تقريباً. في هذا العمل، تم إنشاء 108 رموز جديدة تقريباً لـ MDS من منحنيات مكعبة غير مفردة على الترتيب 25 لحقل جالوا، ويتم عرض حالة شبه MDS الخاصة بهم. باستثناء 26 و 26، وهي غير مكتملة، يتراوح طول هذه الرموز بين 16 و 36 حرفاً. يتم أيضاً توفير نصف قطر التغطية وتوزيعات الوزن لهذه الرموز.

الكلمات المفتاحية: المنحنيات المكعبة الإهليلجية، القوس، توزيعات الوزن، كود MDS القريب

INTRODUCTION



Let $F_q = GF(q)$ represent the order q Galois field, where q is a prime power ($q = p^m$, p is a prime number, and m is a positive integer), and let $PG(2, q)$ be the projective plane over F_q . A set of k points with r collinear points and no $(r + 1)$ collinear points is known as a $(k; r)$ -arc. If a $(k + 1, r)$ -arc does not contain a $(k; r)$ -arc, it is said to be complete. For further details on the salient features of these geometric structures see [1] .

$V(n, q)$ is a vector space of dimension n over F_q , and C is a subspace of this space of size $\dim(C) = k$. This code is also known as a $[n, k, d]_q$ -code or a $[n, k, d]$ linear q - ary -code C and the shortest distance is given by $d(C) = d = \min w(x) | x \neq (0) \in C = \min \{d(x, y) | x \neq y\}$.

We indicate $x = (x_1, \dots, x_n) = x_1 \dots x_n$ and $y = (y_1, \dots, y_n) = y_1 \dots y_n$ where $w(x) = |\{i | x_i \neq 0\}|$, is the codeword's weight x . $d(x, y) = |\{i | x_i \neq y_i\}|$ is the Hamming distance between x and y . Generator matrix refers to a matrix G whose columns serve as the building blocks of a linear code. An $[n, k, d]_q$ -code If any two columns of the generator matrix are linearly independent, C is referred to as a projective code (PG code). The term " e -error correcting code" refers to a code of distance d , where $e = \lfloor (d - 1)/2 \rfloor$. The quantity A_i , where $i = 0$ to n , of Hamming-weighted codewords in C . The vector $(A_0, \dots, A_n)$ represents the weight distribution of C .

For any $y \in C$, dual code C of a $[n, k, d]_q$ -code C is defined as $C^\perp = \{x \in F_q^n | x \cdot y = 0\}$. for Further information on linear code's characteristics see [2].

One of the most challenging coding theory problems is determining the existence of a code with a given set of parameters (length, dimension, and Hamming distance). Also, figuring out the values of k for which a complete $(k; r)$ -arc exists is one of the trickier and more challenging tasks in finite projective geometry. Since the two issues are related, the outcomes of one of them will have a beneficial impact on the other, as will be shown in the next section.

One of the main areas of study in the projective geometry $PG(n, q)$ is finding complete $(k; r)$ -arcs with the most points. A few of them looked at this problem conceptually., as in [3]–[7], while others more researched it in the projective plane for a certain field. and $r = 3$, as shown in [8], [9], and [10], $q = 27$. Additionally, several writers examined codes through arcs for certain fields, as in [10], $q = 17$, [11], [12], $q = 19$, [13], $q = 2, 3, 5, 7$, [14], $q = 11, 13$, [15] , $q = 27$.

To find original linear codes, this study makes use of the connection between cubic curves and the PG linear code, Near- MDS codes providing information on their weight distributions and covering radius..



In order to establish linear coding of Near – *MDS* code, as well as To determine the covering radius and weight distributions, it was necessary to identify the generating matrices for each of these codes. These algorithms were built on a pc with a Core i7-8565U CPU operating from Intel at 1.99 GHz using the GAP application [16]. RAM 8 GB.

BACKGROUND AND PREVIOUS RESULTS

This section contains a discussion of the calculation techniques as well as the vocabulary and algebra used in this subject.

Definition 1 [2]. The $[n, k, d]_q$ -code's covering radius C is the smallest integer, $\cup_{x \in C} S(x, \omega) = F_q^n$, where the ball $S(x, \omega)$ has radius ω and centre x .

Definition 2[17][18]. The term "almost-*MDS* code" (abbreviated "*AMDS*") refers to a linear code C with $d(C) = n - k$ and a Near-*MDS* code, or *MDS*, is $d(C) = d(C^\perp)$.

Theorem 3[18]: Suppose C is an $[n, k, d]_q$ -Near – *MDS* code, its weight distribution is $\{A_i | i = 0 \text{ to } n\}$ and the weight distribution of $C^\perp$ is $\{A'_i | i = 0 \text{ to } n\}$. Then,

$$A_{n-k+s} = \binom{n}{k-s} \sum_{j=0}^{s-1} (-1)^j \binom{n-k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{k}{s} A_{k-s},$$

where $s \in \{1, 2, \dots, k\}$, and

$$A'_{n-k+s} = \binom{n}{k+s} \sum_{j=0}^{s-1} (-1)^j \binom{k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{n-k}{s} A'_k,$$

$s \in \{1 \text{ to } n - k\}$.

In [19] and [20] theoretically, the connection between projective coding theory and the theory of a $(n; r)$ -arcs is provided. Below is a summary of this relationship.

Theorem 4 . $[n, k, d]_q$ - code in F_q^n is identical to an $(n; n - d)$ -arc in $PG(k - 1, q)$.

Therefore, there is a 1:1 correspondence between $[n, 3, n - 3]_q$ -code C and $(n; 3)$ -arcs in $PG(2, q)$ for $k = 3$ and $n - d = 3$.

The primary finding upon which this study is predicated is presented in [8] and is briefly summarized in the following Table.

Suppose F stands for collection of points on F'_i (the cubic curve), where $|F|$ shows how many points are on F'_i and the size of the whole curve created by $F(F'_i)$ is shown by $M(F)$. Assume α is fundamental component of F_q .



TABLE 1. Elliptic cubic curves parameters

F'_i	Coefficient of $X_0^3 + X_1^3 X_2^3 - bX_0 X_1 X_2$	$ \mathcal{F} - M(\mathcal{F})$	F'_i	Coefficients of $X_2^2 X_1 + X_0^3 + bX_0^2 X_1 + cX_1^3$	$ \mathcal{F} - M(\mathcal{F})$
F'_1	α^{21}	18-36	F'_{41}	α, α^8	28
F'_2	α^6	27	F'_{42}	α, α^6	28
F'_3	0	36	F'_{43}	α^7, α	29
F'_4	$X_0 X_1 X_2 + bX^3$		F'_{44}	α^7, α^{13}	29
F'_5	α^9	18-31	F'_{45}	$1, \alpha^{22}$	32
F'_6	α^{21}	18-31	F'_{46}	$1, \alpha^6$	32
F'_7	Coefficient of $X_2^2 X_1 + X_0^3 - bX_1^3$		F'_{47}	$1, \alpha^{14}$	32
F'_8	α^2	21-36	F'_{48}	α^7, α^4	34
F'_9	α^4	21-36	F'_{49}	α^7, α^{14}	34
F'_{10}	Coefficient of $X_0 X_1 X_2 + bX^3$		F'_{50}	$\alpha^{22}, 1$	34
F'_{11}	α	24	F'_{51}	$0, \alpha^9$	16-32
F'_{12}	α^7	24	F'_{52}	$\alpha^{22}, 0$	20-28
F'_{13}	α^{22}	24	F'_{53}	$0, \alpha$	31
F'_{14}	α^5	24	F'_{54}	$0, \alpha^7$	31
F'_{15}	α^{14}	24	F'_{55}	$1, 0$	32
F'_{16}	α^{11}	24	F'_{56}	$\alpha^7, 0$	34
F'_{17}	α^{15}	27	F'_i	Coefficient of $X_0^3 + aX_1^3 + bX_2^3 - cX_0 X_1 X_2$	
F'_{18}	α^3	27	F'_{57}	$\alpha, \alpha^2, \alpha^6$	18-30
F'_{19}	α^{19}	30	F'_{58}	$\alpha, \alpha^2, \alpha^{22}$	18-30
F'_{20}	α^4	30	F'_{59}	α, α^2, α	27
F'_{21}	α^{20}	30	F'_{60}	$\alpha, \alpha^2, \alpha^7$	27
F'_{22}	α^{23}	30	F'_{61}	$\alpha, \alpha^2, \alpha^{16}$	27
F'_{23}	α^{10}	33	F'_{62}	$\alpha, \alpha^2, \alpha^4$	27
F'_{24}	α^2	33	F'_{63}	$\alpha, \alpha^2, 0$	36
F'_i	Coefficients of $X_2^2 X_1 + X_0^3 + bX_0^2 X_1 + cX_1^3$		F'_{64}	$\alpha, \alpha^2, \alpha^{13}$	36
F'_{25}	$1, \alpha^{15}$	17-32	F'_i	Coefficients of $X_0^2 X_1 + X_0^2 X_2 + aX_1^2 X_2 - b(X_0^3 + aX_1^3 + a^2 X_2^3 - cX_0 X_1 X_2)$	
F'_{26}	$\alpha^7, 1$	19-31	F'_{65}	$\alpha, \alpha^{10}, \alpha^{19}$	18-32
F'_{27}	α^7, α^6	19-31	F'_{66}	$\alpha^2, \alpha^4, \alpha^{20}$	18-32



F'_{25}	α^{22}, α^7	20-28	F'_{67}	$\alpha, 0$	21
F'_{26}	α^{22}, α^{19}	20-30	F'_{68}	$\alpha^2, 0$	21
F'_{27}	α^{22}, α^{15}	20-28	F'_{69}	$\alpha, \alpha^7, \alpha^{19}$	24
F'_{28}	$1, \alpha$	22-27	F'_{70}	$\alpha, \alpha^{13}, \alpha^{19}$	24
F'_{29}	$1, \alpha^{13}$	22-25	F'_{71}	$\alpha, 1, \alpha^{19}$	24
F'_{30}	$1, \alpha^8$	22-27	F'_{72}	$\alpha^2, \alpha^{13}, \alpha^{20}$	24
F'_{31}	$1, \alpha^5$	22-25	F'_{73}	$\alpha^2, \alpha^{19}, \alpha^{20}$	24
F'_{32}	α, α^4	23-26	F'_{74}	$\alpha^2, \alpha^{10}, \alpha^{20}$	24
F'_{33}	α, α^{14}	23-26	F'_{75}	$\alpha, \alpha^{19}, \alpha^{19}$	27
F'_{34}	α^{22}, α^8	25	F'_{76}	$\alpha^2, \alpha, \alpha^{20}$	27
F'_{35}	α^{22}, α^9	25-28	F'_{77}	$\alpha, \alpha, \alpha^{19}$	30
F'_{36}	α^{22}, α^4	25	F'_{78}	$\alpha, \alpha^{22}, \alpha^{19}$	30
F'_{37}	α, α	28	F'_{79}	$\alpha^2, 1, \alpha^{20}$	30
F'_{38}	α, α^{13}	28	F'_{80}	$\alpha^2, \alpha^7, \alpha^{20}$	30
F'_{39}	$\alpha, 1$	28	F'_{81}	$\alpha, \alpha^4, \alpha^{19}$	30
F'_{40}	α, α^{22}	28	F'_{82}	$\alpha^2, \alpha^{22}, \alpha^{20}$	30

Algorithm B :

Cic= points on the projective cubic curves F_i as a group

1- for g in Cic do

PIO=[] A collection of points within the code C, denoted as g, is observed.

M= A matrix is constructed such that each column represents a point within the set denoted as "g".

KL=[]; The collection of Hamming distances between codewords.

2- for s in $[1..q^n]$ Let n be the number of rows in M.

y= build from M at point

m= amount of y coordinates that are not zero;

Add(KL,m);

2- od;

d(C)= The code's shortest Hamming distance derived from the KL divergence is calculated.

W= Theorem 3's weight distribution for the code.

PO A subroutine is executed to evaluate positive integers in order to calculate covering radius. Due to the excessive time required for this process, it is separated into multiple partitions.)

30

31

32

33

34



F_{48} : [34,3,31] -code $C_{F_{48}}$	(1, 0, 4224, 792, 6960, 3648)	15	$27 \leq \omega \leq 31$
F_{49} : [34,3,31] -code $C_{F_{49}}$	(1, 0, 4224, 792, 6960, 3648)	15	$27 \leq \omega \leq 31$
F_{50} : [35,3,32] -code $C_{F_{50}}$	(1, 0, 4488, 816, 6744, 3576)	15	$28 \leq \omega \leq 32.$
F_{51} : [16,3,13] -code $C_{F_{51}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 840, 360, 6744, 7680)	6	$11 \leq \omega \leq 13$
F_{51}^+ : [32,3,29] -code $C_{F_{51}^+}$	(1, 0, 2856, 3336, 4728, 4704)	14	$25 \leq \omega \leq 29$
F_{52} : [20,3,17] -code $C_{F_{52}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1368, 456, 7464, 6336)	8	$14 \leq \omega \leq 17$
F_{52}^+ : [28,3,25] -code $C_{F_{52}^+}$	(1, 0, 2136, 2664, 5736, 5088)	12	$21 \leq \omega \leq 25$
F_{53} : [31,3,28] -code $C_{F_{53}}$	(1, 0, 3480, 720, 7464, 3960)	13	$24 \leq \omega \leq 28$
F_{54} : [31,3,28] -code $C_{F_{54}}$	(1, 0, 3480, 720, 7464, 3960)	13	$24 \leq \omega \leq 28$
F_{55} : [32,3,29] -code $C_{F_{55}}$	(1, 0, 3720, 744, 7320, 3840)	14	$25 \leq \omega \leq 29$
F_{56} : [34,3,31] -code $C_{F_{56}}$	(1, 0, 4224, 792, 6960, 3648)	15	$27 \leq \omega \leq 31$



F_{57} : [18,3,15] -code $C_{F_{57}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1080, 432, 7128, 6984)	7	$13 \leq \omega \leq 15$
F_{57}^+ : [30,3,27] -code $C_{F_{57}^+}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2520, 2880, 5400, 4824)	13	$23 \leq \omega \leq 27$
F_{58} : [18,3,15] -code $C_{F_{58}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1080, 432, 7128, 6984)	7	$13 \leq \omega \leq 15$
F_{58}^+ : [30,3,27] -code $C_{F_{58}^+}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2520, 2880, 5400, 4824)	13	$23 \leq \omega \leq 27$
F_{59} : [18,3,15] -code $C_{F_{59}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1080, 432, 7128, 6984)	7	$13 \leq \omega \leq 15$
F_{59}^+ : [32,3,29] -code $C_{F_{59}^+}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2904, 3192, 4872, 4656)	14	$25 \leq \omega \leq 29$
F_{60} : [18,3,15] -code $C_{F_{60}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1080, 432, 7128, 6984)	7	$13 \leq \omega \leq 15$
F_{60}^+ : [32,3,29] -code $C_{F_{60}^+}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 96, 456, 1680, 3168, 6288, 3936)	14	$25 \leq \omega \leq 29$
F_{61} : [21,3,18] -code $C_{F_{61}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1512, 504, 7560, 6048)	8	$15 \leq \omega \leq 18$
F_{62} : [21,3,18] -code $C_{F_{62}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1512, 504, 7560, 6048)	8	$15 \leq \omega \leq 18$
F_{63} : [24,3,21] -code $C_{F_{63}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2016, 576, 7776, 5256)	10	$18 \leq \omega \leq 21$
F_{64} : [24,3,21] -code $C_{F_{64}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2016, 576, 7776, 5256)	10	$18 \leq \omega \leq 21$
F_{65} : [24,3,21] -code $C_{F_{65}}$	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2016, 576, 7776, 5256)	10	$18 \leq \omega \leq 21$

37



	0, 0, 0, 0, 3240, 720, 7560, 4104)		
F_{79} : [33,3,30]-code $C_{F_{79}}$	(1, 0, 3960, 792, 7128, 3744)	14	$26 \leq \omega$ ≤ 30
F_{80} : [33,3,30]-code $C_{F_{80}}$	(1, 0, 3960, 792, 7128, 3744)	14	$26 \leq \omega \leq$ 30.
F_{81} : [36,3,33]-code $C_{F_{81}}$	(1, 0, 4752, 864, 6480, 3528)	16	$28 \leq \omega$ ≤ 30
F_{82} : [36,3,33]-code $C_{F_{82}}$	(1, 0, 4752, 864, 6480, 3528)	16	$28 \leq \omega$ ≤ 30

CONCLUSION

There exist 108 non-metric distance scaling (*NMDS*) codes that exhibit projective distinctiveness over the finite field F_{25} , with a dimension of three. The length of these codes spans all values between 16 and 36, excluding the value 26. Among the set of Near – *MDS* codes, there exist 26 codes that are not capable of being extended. These codes possess a length that corresponds to one of the following values: 21, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36.

COMPARISON BETWEEN THE PARAMETERS OF THE LINEAR CODES IN $PG(2, 25)$ AND THE PARAMETERS OF THE LINEAR CODES IN $PG(2, 27)$

From [15] and above results , we conclude the following:

<u><i>PG(2, 25)</i></u>	<u><i>PG(2, 27)</i></u>
(i) The cell $\tau : \rho$ refers to the number of points the projective linear code F_{C_i} (F_{C_i+} for extended codes) τ and corresponding number of such distinct projective code ρ :	
F_{C_i} ; 16:1 17:1 18: 7 19:2 20:4 21:4 22:4 23:2 24:12 25:3 27:9 28:6 30:8 31:2 32:4	F_{C_i} ; 18: 2 19:1 20:4 21:6 23:3 24:12 26:6 27:9 28:2 29:3 30:12 32:6 33:6 35:3 36:8 37:1 38:1



$F_{c_i}^+ :$ 33:4 34:3 35:1 36:3 25:2 26:3 27:2 28:2 30:3 32:3 36:3	$F_{c_i}^+ :$ 25:3 26:1 27:8 28:3 29:4 30:6 32:4 33:2 34:1
(ii) The cell $m : n$ refers to the value of e (error correcting code) for the projective linear code F_{c_i} m and corresponding number of such distinct projective code n : 6:2 7:10 8:8 9:6 10:19 11:12 12:13 13:17 14:12 15:4 16:5	7:3 8:10 9:3 10:15 11:21 12:12 13:18 14:18 15:4 16:9 17:1
(iii) Minimum value of the covering radius cr for projective linear code F_{c_i} is 11 and Maximum value is 33	Minimum value of the covering radius cr for projective linear code F_{c_i} is 13 and Maximum value is 35

REFERENCES

1. NA Al-Seraji. (2010) 'The Geometry of the plane of order seventeen and its application to error-correcting codes', Ph.D. Thesis, University of Sussex, United Kingdom.
2. EB Al-Zangana. (2011) 'The geometry of the plane of order nineteen and its application to error-correcting codes', Ph.D. Thesis, University of Sussex, United Kingdom.
3. EB Al-Zangana. (2016) 'Classification of elliptic cubic curves over the finite field of order nineteen' *Baghdad Science Journal*,13(4), pp. 846-852.
4. EB Al-Zangana. (2013) 'On non-singular plane cubic curves over $F_q, q = 2,3,5,7$ ', *J. of Education, Al-Mustansiriyah University*, 1, pp.149-160.
5. EB Al-Zangana. (2013) 'Complete and incomplete elliptic curves over the finite field of order 11 and 13' *j. of Science , AL-Mustansiriyah University*, 24(1), pp. 135-142.
6. S Ball and JWP Hirschfeld. (2005) 'Bounds on (n,r) -arcs and their application to linear codes', *Finite Fields Appl.*, 11 (3), pp. 326-336.
7. AA Bruen, JWP Hirschfeld and DL Wehlan. (2011) 'Cubic curves, finite geometry and cryptography' *World scientific Acta Apple .Math.*,115(3), pp. 265-278.
8. MA De boer. (1996) 'Almost MDS codes designs', *Codes and Cryptography*, 9, pp. 143-155.



9. S Dodunecov and I Landjev. (1995) 'On near MDS codes', *J. Geom.*, 54, pp.30-43.
10. GAP Group. (2021) 'GAP Reference Manal URL [http:// www gap – system.org](http://www.gap-system.org).
11. JWP Hirschfeld. (1998) 'Projective geometries over finite fields. 2nd edn. New York: Ox-ford Mathematical Monographs, The Clarendon Press, Oxford University Press.
12. JWP Hirschfeld. (2006) 'The numbers of points on a curve, and application', *Rend. Mat., Ser.VII*, 26, pp.13-28.
13. JWP Hirschfeld. (2010) 'Curves of genus 3', *Rend . Mat. Appl* , 30, pp. 77-88 , 2010.
14. JWP Hirschfeld and L Storme. (2001) 'The packing problem in statistics, coding theory and finite geometry :update 2001 in Finite Geometries, Developments of mathematics, pp. 201-246,Eds. A.Blokhuis , J.W.P. Hirschfeld, D.Jungnicked and J.A.Thas,Kluwer.
15. SH Naji and EB Al-Zangana. (2023) ' Special NMDS codes of dimension three
Over finite field of order twenty five .
16. JWP Hirschfeld and JF Voloch. (1988) 'The characterization of elliptic curves over finite fields', *J.Austral Math. Soc.*, 45,pp. 275-286.
17. FJ Mac Williams and NJA Sloane. (1977) 'The theory of error-correcting codes', Part 1, Amsterdam, North Holland.
18. SH Naji and EB Al-Zangana. (2020) 'Cubic curves over the finite field of order twenty seven', *J. Phys.: Conf. Ser.* 1664 012025.
19. SH Naji and EB Al-Zangana. (2021) 'Cubic curves over the finite field of order twenty five', *J. Phys.: Conf. Ser.* (To appear).
20. R Schoof. (1987) 'Non-singular plane cubic curves over finite fields', *J. Compin. Theory, Ser. A*, 46,pp. 183-211.