

# Near-MDS codes from elliptic curves

Angela Aguglia\*    Luca Giuzzi<sup>†</sup>    Angelo Sonnino<sup>‡</sup>

## Abstract

We provide a geometric construction of  $[n, 9, n - 9]_q$  near-MDS codes arising from elliptic curves with  $n$   $\mathbb{F}_q$ -rational points. Furthermore, we show that in some cases these codes cannot be extended to longer near-MDS codes.

**Key words:** linear code; near-MDS code; elliptic curve.

**Mathematics subject classification:** 94B05, 51A05, 51E21.

## 1 Introduction

Maximum distance separable (for short MDS) codes are the best linear  $[n, k, d]_q$  codes as they meet the Singleton bound, that is,  $n = d + k - 1$ . The non-negative integer  $s(\mathbf{C}) := n - k + 1 - d$  is said to be the Singleton defect of the code  $\mathbf{C}$ . Thus, the Singleton defect of an MDS code is zero.

A linear code  $\mathbf{C}$  is defined to be a near-MDS (for short NMDS) code if  $s(\mathbf{C}) = s(\mathbf{C}^\perp) = 1$  where  $\mathbf{C}^\perp$  is the dual code of  $\mathbf{C}$ . Hence, a NMDS  $[n, k]$  code has minimum distance  $n - k$ .

NMDS codes were introduced by Dodunekov and Landjev [4] with the aim of constructing good linear codes by slightly weakening the restrictions

---

\*Angela Aguglia: [angela.aguglia@poliba.it](mailto:angela.aguglia@poliba.it)  
Dipartimento di Meccanica, Matematica e Management - Politecnico di Bari - Via Orabona, 4 - 70126 Bari (Italy).

<sup>†</sup>Luca Giuzzi: [luca.giuzzi@unibs.it](mailto:luca.giuzzi@unibs.it)  
DICATAM - University of Brescia - Via Branze 53 - I-25123 Brescia, (Italy)

<sup>‡</sup>Angelo Sonnino: [angelo.sonnino@unibas.it](mailto:angelo.sonnino@unibas.it)  
Dipartimento di Matematica, Informatica ed Economia - Università degli Studi della Basilicata - Viale dell'Ateneo Lucano, 10 - 85100 Potenza (Italy).

in the definition of an MDS code. NMDS codes have similar properties to MDS codes. Some non-binary linear codes such as the ternary Golay codes, the quaternary quadratic residue  $[11, 6, 5]_4$ -code, and the quaternary extended quadratic residue  $[12, 6, 6]_4$ -code are notable examples of NMDS codes; see [13].

The geometrical counterpart of an NMDS code is an  $n$ -track in a Galois space which is a set of  $n$  points in an  $N$ -dimensional Galois space such that every  $N$  of them are linearly independent but some  $N + 1$  of them, see [3]. If every  $N + 2$  points of the  $n$ -track generate the whole space then the  $n \times (N + 1)$  matrix whose columns are homogeneous coordinates of the  $n$ -track points is a generator matrix of an NMDS code. The  $n$ -track is complete, i.e. maximal with respect to set theoretical inclusion, if and only if the code is not extendable.

Let  $N_q$  denote the maximum number of  $\mathbb{F}_q$ -rational points on an elliptic curve defined over  $\mathbb{F}_q$ ; it is well-known that, by Hasse theorem,  $|N_q - (q + 1)| \leq 2\sqrt{q}$ .

NMDS codes of length up to  $N_q$  may be constructed from elliptic curves. An interesting question is whether there exist NMDS codes of length greater than  $N_q$ . Constructions of NMDS codes from elliptic curves are found in [1, 2, 8] where results both from combinatorics and algebraic geometry are used.

Here we provide a geometric construction of 9 dimensional NMDS codes using an algebraic curve of order 9 in  $\text{PG}(9, q)$  which arises from a non-singular cubic curve  $\mathcal{E} : f(X, Y, Z) = 0$  of  $\text{PG}(2, q)$  via the (modified) Veronese embedding:

$$\nu_3^2 : (X:Y:Z) \mapsto (f(X, Y, Z) : X^2Y : X^2Z : XY^2 : XYZ : XZ^2 : Y^3 : Y^2Z : YZ^2 : Z^3). \quad (1)$$

We also show that certain codes from elliptic curves are not extendible to longer NMDS codes. The proof depends on some results on the number of  $\mathbb{F}_q$ -rational lines through a given point  $P$  that meet a plane elliptic curve in exactly three  $\mathbb{F}_q$ -rational points and on some computations carried out with the aid of GAP [7].

## 2 Preliminaries

The following definitions of an NMDS code of length  $n$  and dimension  $k$  over a finite field  $\mathbb{F}_q$  are equivalent to that given in the Introduction; see [5].

**Definition 1.** *A linear  $[n, k]$  code over  $\mathbb{F}_q$  is NMDS if any of its generator matrices, say  $G$ , satisfies the following conditions:*

- (i) *any  $k - 1$  columns of  $G$  are linearly independent;*
- (ii)  *$G$  contains  $k$  linearly dependent columns;*
- (iii) *any  $k + 1$  columns of  $G$  have full rank.*

**Definition 2.** *A linear  $[n, k]$  code over  $\mathbb{F}_q$  is NMDS if any of its parity check matrices, say  $H$ , satisfies the following conditions:*

- (i) *any  $n - k - 1$  columns of  $H$  are linearly independent;*
- (ii)  *$H$  contains  $n - k$  linearly dependent columns;*
- (iii) *any  $n - k + 1$  columns of  $H$  have full rank.*

From a geometric point of view, a NMDS  $[n, k]$  code  $\mathbf{C}$  over  $\mathbb{F}_q$  can be regarded as a projective system (i.e. a distinguished point set)  $\mathbf{C}$  in a projective space  $\text{PG}(k - 1, q)$ ; see [15] for more details.

**Definition 3.** *A subset  $\mathbf{C} \subseteq \text{PG}(k - 1, q)$  is an  $(n; k, k - 2)$ -set in  $\text{PG}(k - 1, \mathbb{F}_q)$  if it satisfies the following conditions:*

- (i) *every  $k - 1$  points in  $\mathbf{C}$  span a hyperplane of  $\text{PG}(k - 1, q)$ ;*
- (ii) *there exists a hyperplane of  $\text{PG}(k - 1, q)$  containing exactly  $k$  points of  $\mathbf{C}$ ;*
- (iii) *every  $k + 1$  points of  $\mathbf{C}$  generate the whole  $\text{PG}(k - 1, q)$ .*

**Definition 4.** *An  $(n; k, k - 2)$ -set in  $\text{PG}(k - 1, \mathbb{F}_q)$  is complete if it is maximal with respect to set-theoretical inclusion.*

Thus, in this setting, an NMDS  $[n, k]$  code over  $\mathbb{F}_q$  is an  $(n; k, k - 2)$ -set in  $\text{PG}(k - 1, \mathbb{F}_q)$ .

Given an integer  $\nu \geq 1$  and a prime power  $q = p^h$ , consider the set  $\mathfrak{C}^\nu$  of all the curves of degree  $\nu$  contained in the projective plane  $\text{PG}(2, q)$  over a finite field  $\mathbb{F}_q$ . Since any curve  $\mathcal{C} \in \mathfrak{C}^\nu$  is uniquely determined by  $m + 1 = \binom{\nu+2}{2}$  parameters in  $\mathbb{F}_q$ , that is, the coefficients of its equation

$$\begin{aligned} a_0 Z^\nu + (a_1 X + a_2 Y) Z^{\nu-1} + (a_3 X^2 + a_4 XY + a_5 Y^2) Z^{\nu-2} + \cdots \\ + (a_{m-\nu} X^\nu + a_{m-\nu+1} X^{\nu-1} Y + \cdots + a_{m-1} XY^{\nu-1} + a_m Y^\nu) = 0, \end{aligned}$$

and the curve is unchanged if these parameters are multiplied by a common factor, then  $\mathfrak{C}^\nu$  can be regarded as a projective space  $\text{PG}(m, q)$  with homogeneous coordinates  $(a_0 : a_1 : \cdots : a_m)$ . We may also denote a curve  $\mathcal{C}$  by using its defining polynomial.

The following result—which is an implicit formulation of the famous Cayley-Bacharach theorem—will be useful later; see [6].

**Theorem 2.1.** *Let  $\mathcal{E}$  and  $\mathcal{C}$  be two distinct cubic curves meeting in a set  $\mathcal{S}$  consisting of 9 points (counted with multiplicities). If  $\mathcal{D} \subset \text{PG}(2, q)$  is any cubic curve containing all but one point of  $\mathcal{S}$ , then  $\mathcal{C} \cap \mathcal{D} = \mathcal{S}$ .*

### 3 Lifting point sets

The space  $\mathfrak{C}^3$  consisting of all the cubics in  $\text{PG}(2, q)$  has projective dimension 9, hence 10 independent cubic curves are required to generate it. Let  $\mathcal{E}$  be a non-singular cubic curve of equation  $f(X, Y, Z) = 0$  over  $\mathbb{F}_q$ . A suitable basis  $\mathcal{B}$  for  $\mathfrak{C}^3$ , containing  $\mathcal{E}$ , can be written by using the following polynomials:

$$\mathcal{B} = \{f(X, Y, Z), X^2 Y, X^2 Z, XY^2, XYZ, XZ^2, Y^3, Y^2 Z, YZ^2, Z^3\},$$

where  $f(X, Y, Z)$  is required to contain the term  $X^3$ . In fact, the defining polynomial of any cubic curve would be suitable as first element of the basis  $\mathcal{B}$ , as long as it contains the monomial  $X^3$ ; nevertheless, the choice of an elliptic curve is motivated by the fact that, unlike the case of genus 0, the number of  $\mathbb{F}_q$ -rational points of a carefully chosen elliptic curve is not necessarily limited to  $q + 1$ .

We consider the following embedding of the points of  $\text{PG}(2, q)$  onto  $\text{PG}(9, q)$  with projective coordinates  $(X_0 : X_1 : X_2 : X_3 : X_4 : X_5 : X_6 : X_7 : X_8 : X_9)$  by means of

the mapping  $\nu_3^2 : \text{PG}(2, q) \rightarrow \text{PG}(9, q)$  (1) which is a Veronese embedding of degree 3. Let  $\mathcal{V}_3$  be the image of  $\nu_3^2$ ; clearly  $\mathcal{V}_3$  is (projective equivalent to) the cubic Veronese surface.

More in detail, the points of the curve  $\mathcal{E}$  are mapped onto a curve  $\Gamma$  of  $\text{PG}(9, q)$  with the same number  $n$  of  $\mathbb{F}_q$ -rational points as  $\mathcal{E}$ . Also  $\Gamma$  is the complete intersection of  $\mathcal{V}_3$  with the hyperplane  $\Sigma \cong \text{PG}(8, q)$  of equation  $X_0 = 0$ . Since for every cubic curve  $\mathcal{C}$  of equation  $g(X, Y, Z) = 0$  in  $\text{PG}(2, q)$ , the defining polynomial is a linear combination of the elements of  $\mathcal{B}$ , that is,

$$g(X, Y, Z) = \lambda_0 f(X, Y, Z) + \lambda_1 Y^3 + \lambda_2 XZ^2 + \lambda_3 YZ^2 + \lambda_4 X^2Z + \lambda_5 Y^2Z + \lambda_6 XYZ + \lambda_7 X^2Y + \lambda_8 XY^2 + \lambda_9 Z^3,$$

it turns out that  $\nu_3^2(\mathcal{C})$  is the complete intersection of  $\mathcal{V}_3$  with the hyperplane  $\Pi \subset \text{PG}(9, q)$  of equation

$$\sum_{i=0}^9 \lambda_i X_i = 0, \tag{2}$$

which is distinct from  $\Sigma$ . Thus, every cubic curve  $\mathcal{C} : g(X, Y, Z) = 0$  of  $\text{PG}(2, q)$  corresponds to a hyperplane of equation (2). Back to  $\text{PG}(2, q)$ , the set  $(\nu_3^2)^{-1}(\Pi \cap \mathcal{V}_3)$  corresponds to a unique cubic curve  $\mathcal{C}$  distinct from  $\mathcal{E}$ , and, clearly,  $(\nu_3^2)^{-1}(\Pi \cap \Gamma)$  corresponds to  $\mathcal{C} \cap \mathcal{E}$ .

**Theorem 3.1.** *Suppose that  $\mathcal{E}$  has  $n \geq 9$  points. Then the point set  $\Gamma$  is an  $(n; 9, 7)$ -set in  $\Sigma = \text{PG}(8, q)$ .*

*Proof.* To prove the theorem it suffices to consider the mutual position of cubic curves in  $\text{PG}(2, q)$ .

- (i) Take eight distinct points  $P_1, \dots, P_8 \in \Gamma$  and consider the corresponding distinct points  $Q_1, \dots, Q_8 \in \mathcal{E}$ , with  $Q_i = (\nu_3^2)^{-1}(P_i)$ . Suppose that there is a  $t$ -dimensional net with  $t \geq 2$ , say  $\mathcal{F}$ , consisting of cubics through  $Q_1, \dots, Q_8$ . Then, from Theorem 2.1 there is a ninth point  $Q_9 \in \mathcal{E}$  such that the points  $Q_1, \dots, Q_9$  are in the support of  $\mathcal{F}$ . This implies that every further point  $Q_{10} \in \mathcal{E} \setminus \{Q_1, \dots, Q_9\}$  yields a  $(t-1)$ -dimensional net consisting of cubics through  $Q_1, \dots, Q_9$  which are distinct from  $\mathcal{E}$  and have ten points in common with it, contradicting Bézout's theorem. Hence,  $\mathcal{F}$  must be a pencil of cubic curves in  $\text{PG}(2, q)$  including  $\mathcal{E}$  and passing through  $Q_1, \dots, Q_8$ . Back to  $\text{PG}(9, q)$ , we observe that  $\mathcal{F}$  corresponds to a pencil of hyperplanes

of  $\text{PG}(9, q)$  which meet in a unique 7-dimensional subspace  $\Delta$  such that  $\{P_1, \dots, P_8\} \subset (\Gamma \cap \Delta)$ , that is,  $P_1, \dots, P_8$ , generate the hyperplane  $\Delta$  of  $\Sigma$ .

- (ii) From Theorem 2.1, there is a further point  $Q_9 \in \text{PG}(2, q)$  which belongs to the intersection of  $\mathcal{E}$  and all the other cubics of the above pencil  $\mathcal{F}$ . This proves that the previous subspace  $\Delta$  meets  $\Gamma$  in  $P_1, \dots, P_8, P_9 = \nu_3^2(Q_9)$ .
- (iii) Let  $\Pi$  be a hyperplane of  $\text{PG}(9, q)$  different from  $\Sigma$ . Put  $\mathcal{C} = (\nu_3^2)^{-1}(\Pi)$ . From Bézout's theorem we know that  $|\mathcal{E} \cap \mathcal{C}| \leq 9$ , therefore any hyperplane of  $\text{PG}(9, q)$  has at most 9 points in common with  $\Gamma$ . Hence,  $\Gamma$  is a curve of order 9, therefore 10 points of  $\Gamma$  generate the whole  $\Sigma$ .

The claim follows. □

**Remark 1.** *The code associated to  $\Gamma$  can also be interpreted as an AG-code, see [15]. Indeed, Theorem 3.1 is a consequence of [15, Theorem 4.4.19]. However, our proof does not use the Riemann-Roch Theorem.*

## 4 Some complete NMDS codes

In this section we provide some examples of complete NMDS codes in the set of codes constructed above by lifting the elliptic curve  $\mathcal{E}$  in the case when the base field is large enough.

By Definition 4, the algebraic curve  $\Gamma = \nu_3^2(\mathcal{E})$  provides a complete NMDS code, that is a complete  $(n; 9, 7)$ -set of  $\text{PG}(8, q)$ , if and only if for any  $Q \in \Sigma$  there exists at least one hyperplane  $\Pi$  of  $\Sigma$  with  $Q \in \Pi$  meeting  $\Gamma$  in 9 points.

**Definition 5.** *We call a point  $Q \in \Sigma$  special for  $\Gamma$  if for all hyperplanes  $\Pi$  of  $\Sigma$  through  $Q$  we have  $|\Pi \cap \Gamma| < 9$ .*

We expect that for large  $q$  special points, if they exist at all, are very few; see Lemma 4.4. So we propose the following conjecture.

**Conjecture 1.** *Suppose  $q \geq 121$  to be such that  $2, 3 \nmid q$ . Then there are no special points for  $\Gamma$ .*

In order to verify Conjecture 1, we performed some computer searches for some values of  $q$ . For  $q \in \{7, 11, 13\}$  we executed a (non-trivial) exhaustive

search. For  $q \geq 121$  we provide an argument showing that there cannot be too many special points, if they exist at all. We leave the solution of the problem and its generalization to a future work.

## 4.1 Search for small $q$

Recall that any 8 distinct points of  $\mathcal{V}_3$  are linearly independent; see [11].

For small values of  $q$  it is possible to perform an exhaustive search, adopting the following procedure:

1. Let  $\Gamma = \nu_3^2(\mathcal{E})$  be the embedding of  $\mathcal{E}$ ;
2. for any set of 9 points of  $\Gamma$ , consider the matrix containing their components; let  $\mathfrak{G}$  be the list of such matrices having rank 8. In particular, each element of  $\mathfrak{G}$  corresponds to a hyperplane meeting  $\Gamma$  in 9 points. We call such hyperplanes *good*.
3. For each matrix  $H \in \mathfrak{G}$ , let  $H'$  be a column vector spanning the kernel of  $H$ . In particular, we have that a row vector  $v$  belongs to the span of the rows of  $H$  if and only if  $vH' = \mathbf{0}$ .
4. Consider the linear code  $C$  with parameters  $[|\mathfrak{G}|, 9]$  whose generator matrix  $G$  consists of all columns of the form  $H'$  as  $H$  varies in  $\mathfrak{G}$ . A point  $P$  represented by a vector  $v$  can be added to  $\Gamma$  if, and only if,  $P$  does not belong to any of the hyperplanes represented by the columns of  $G$ ; in other words  $P$  can be added to  $\Gamma$  if and only if the word  $PG$  corresponding to  $P$  does not contain any 0-component.

Using the above argument, we can state the following.

**Theorem 4.1.** *The  $(n;9,7)$ -set  $\Gamma$  is complete if and only if the code  $C$  with generator matrix  $G$  constructed above does not contain any word of maximum weight  $n$ .*

Clearly, it is not restrictive to replace the code  $C$  with a code  $C'$  equivalent to  $C$ . In particular, if we transform its generator matrix  $G$  to row-reduced echelon form, we see that no point with at least a 0 component can give a word of  $C'$  of weight  $n$ ; this allows to exclude from the search all points whose transforms (under the operations yielding the reduction of  $C$ ) lie on the coordinate hyperplanes.

We now limit ourselves to the odd order case with  $q$  not divisible by 3. Then any elliptic curve  $\mathcal{E}$  of  $\text{PG}(2, q)$  admits an equation in canonical Weierstrass form

$$Y^2 = X^3 + aX + b,$$

with  $a, b \in \mathbb{F}_q$  such that  $-16(4a^3 + 27b^2) \neq 0$ ; see [14].

**Remark 2.** *Good hyperplanes correspond to linear systems of cubic curves cutting  $\mathcal{E}$  in 9 points; by [12, Theorem 43], we see that the number of such hyperplanes is approximately  $\frac{1}{9!}q^7$ .*

*We leave to a future work to determine exactly what sets of 9 distinct points of a given elliptic curve  $\mathcal{E}$  might arise as intersection divisor with another curve, in other terms to determine what the good hyperplanes are.*

*Our Conjecture 1 can be restated by saying that the union of all good hyperplanes for  $\mathcal{E}$  is  $\text{PG}(8, q)$  for  $q$  sufficiently large.*

We can now apply the aforementioned strategy for all possible values of  $a, b$  yielding elliptic curves. This leads to the following.

**Theorem 4.2.** *Suppose  $q \in \{7, 11, 13\}$ . Then, the lifted  $(n; 9, 7)$ -set  $\Gamma$  in  $\text{PG}(8, q)$  is complete if and only if  $n = |\mathcal{E}| \geq 15$ . In particular, for  $q = 7$  the lifted set  $\Gamma$  is never complete.*

## 4.2 Properties for large $q$

We now provide an argument to prove that there might not be too many special points. This makes it possible to verify for several values of  $q$  that the  $(n; 9, 7)$ -set  $\Gamma$  in  $\Sigma = \text{PG}(8, q)$  is complete and gives evidence supporting Conjecture 1.

As in the previous section, the projective plane  $\text{PG}(2, q)$  is assumed to be of order  $q$  odd and not divisible by 3. Furthermore we suppose  $q \geq 121$ . Let  $j(\mathcal{E})$  be the  $j$ -invariant of  $\mathcal{E}$ , that is the six cross-ratios of the four tangents from a point of  $\mathcal{E}$  to other points of  $\mathcal{E}$ . We limit ourselves to the case  $j(\mathcal{E}) \neq 0$ , see [10, Theorem 11.15].

We will use the following result which is a direct consequence of [8, Lemma 3.2].

**Lemma 4.3.** *Let  $q \geq 121$  and consider an elliptic cubic  $\mathcal{E}(\mathbb{F}_q)$  with  $j(\mathcal{E}) \neq 0$ . Then there are at least 7 trisecant  $\mathbb{F}_q$ -rational lines through any given  $\mathbb{F}_q$ -rational point.*

Up to a change of projective reference, we can assume without loss of generality that the curve  $\mathcal{E}$  in  $\text{PG}(2, q)$  is met by the reducible cubic  $XYZ = 0$  in 9 distinct  $\mathbb{F}_q$ -rational points.

**Lemma 4.4.** *Under the assumption  $q \geq 121$  any special point  $Q \in \Sigma$  has to be a point  $Q = (0, q_1, q_2, \dots, q_9) \in \Sigma \setminus \Gamma$  such that  $[q_1, q_3, q_4], [q_4, q_7, q_8] \in \mathcal{E}$  and one of the following conditions holds*

- $q_1, q_7 = 0; q_3, q_4, q_8 \neq 0;$
- $q_1, q_8 = 0; q_3, q_4, q_7 \neq 0;$
- $q_3, q_7 = 0; q_1, q_4, q_8 \neq 0;$
- $q_3, q_8 = 0; q_1, q_4, q_7 \neq 0.$

*Proof.* Let  $Q = (0, q_1, q_2, \dots, q_9) \in \Sigma$ . If  $Q \in \Gamma$ , then  $Q$  is not special; indeed, if  $Q \in \Gamma$ , then  $Q = \nu_3^2(P)$  with  $P \in \mathcal{E}$ . Consider a reducible cubic curve  $\mathcal{C}$  in  $\text{PG}(2, q)$ , union of 3 lines  $\ell, m, r$  with  $P \in \ell \setminus \{m \cup r\}$  and such that  $|(\ell \cup m \cup r) \cap \mathcal{E}| = 9$ . Such a curve if  $|\mathcal{E}| > 9$  is guaranteed to exist by Lemma 4.3 and it corresponds to a hyperplane of  $\text{PG}(9, q)$  through  $Q$  meeting  $\Gamma$  in 9 distinct points. So  $Q$  is not special.

Now consider a cubic curve  $\mathcal{C}$  in  $\text{PG}(2, q)$  with equation of the form

$$YZ(\alpha X + \beta Y + \gamma Z) = 0, \quad (3)$$

and a cubic curve  $\mathcal{C}'$  with equation of type

$$XY(aX + bY + cZ) = 0. \quad (4)$$

Via the Veronese embedding  $\nu_3^2$ ,  $\mathcal{C}$  corresponds to the hyperplane of equation  $\alpha X_4 + \beta X_7 + \gamma X_8 = 0$ , whereas  $\mathcal{C}'$  corresponds to the hyperplane  $aX_1 + bX_3 + cX_4 = 0$ .

For any  $Q \in \Sigma \setminus \Gamma$  write  $P_Q := [q_4, q_7, q_8]$  and  $P'_Q := [q_1, q_3, q_4] \in \text{PG}(2, q)$ .

If  $P_Q \notin \mathcal{E}$ , by Lemma 4.3 there are at least 7 lines through  $P_Q$  meeting  $\mathcal{E}$  in 3 distinct points; in particular there is at least one line of equation  $\alpha X + \beta Y + \gamma Z = 0$  through  $P_Q$  meeting  $\mathcal{E} \setminus ([Y = 0] \cup [Z = 0])$  in 3 distinct points. Consequently the cubic  $\mathcal{C} : YZ(\alpha X + \beta Y + \gamma Z) = 0$  corresponds to a hyperplane  $\Pi$  of  $\text{PG}(9, q)$  through  $Q$ , meeting  $\Gamma$  in 9 distinct points and we are done.

If  $P_Q \in \mathcal{E}$  but  $P'_Q \notin \mathcal{E}$ , repeating the same argument starting from a cubic  $\mathcal{C}'$  with equation (4), we see that  $Q$  is not special.

Thus, we suppose  $P_Q, P'_Q \in \mathcal{E}$  and distinguish several cases:

1. If  $q_4 = 0$ , then the cubic  $\mathcal{C}$  of equation  $XYZ = 0$  corresponds to the hyperplane  $X_4 = 0$  passing through  $Q$  with 9 intersections with  $\Gamma$ .
2. If  $q_4 \neq 0$  and  $q_7 = q_8 = 0$ , then  $P_Q = [1, 0, 0] \notin \mathcal{E}$ , which is excluded.
3. If  $q_4 \neq 0$  and  $q_1 = q_3 = 0$ , then  $P'_Q = [0, 0, 1] \notin \mathcal{E}$ , which is excluded.
4. Let  $q_4 \neq 0$  with  $q_7 \neq 0$  and  $q_8 \neq 0$ , then  $P_Q$  is not on  $[Y = 0] \cup [Z = 0]$  in  $\text{PG}(2, q)$ . Then, from Lemma 4.3 there are at least 7 lines in  $\text{PG}(2, q)$  through  $P_Q$  which are 3-secants to  $\mathcal{E}$ . Since  $\mathcal{E}$  has 6 points on the union of the lines  $[Y = 0]$  and  $[Z = 0]$ , there is at least one line through  $P_Q$  with equation:  $\alpha_1 X + \beta_1 Y + \gamma_1 Z = 0$  meeting  $\mathcal{E}$  in 3 points none of which is on  $[Y = 0]$  and  $[Z = 0]$ . So, the hyperplane of  $\text{PG}(9, q)$  through  $Q$ , corresponding to the cubic  $\mathcal{C} : YZ(\alpha_1 X + \beta_1 Y + \gamma_1 Z) = 0$  meets  $\Gamma$  in 9 points.
5. Let  $q_4 \neq 0$ ,  $q_7 \neq 0$  and  $q_8 = 0$  (or, equivalently,  $q_4 \neq 0$ ,  $q_7 = 0$  and  $q_8 \neq 0$ ). Using an argument similar to that of point 4. but starting from a cubic  $\mathcal{C}'$  through  $P'_Q$  with equation of the form (4), it turns out that if  $q_1 \neq 0$  and  $q_3 \neq 0$  then the points  $Q(0, q_1, q_2, \dots, q_7, 0, q_9)$  (or  $Q(0, q_1, \dots, q_6, 0, q_8, q_9)$ ) are not special.

Thus, our lemma follows. □

**Remark 3.** Let  $Q = (0, q_1, \dots, q_9) \in \Sigma$  such that  $Q$  is not ruled out as special point in Lemma 4.4. For instance, suppose  $q_8 = 0$  and either  $q_1 = 0$  or  $q_3 = 0$  with  $[q_1, q_3, q_4] \in \mathcal{E}$ . So, take  $P(a, 0, 1) \in \text{PG}(2, q) \setminus \mathcal{E}$  and consider a cubic  $\mathcal{C}$  with equation:  $Y(Y - m_1 X + am_1 Z)(Y - m_2 X + am_2 Z) = 0$  passing through  $P$  meeting  $\mathcal{E}$  in 9 distinct points. Then,  $\mathcal{C}$  corresponds to the hyperplane  $\pi : m_1 m_2 X_1 - (m_1 + m_2) X_3 - 2am_1 m_2 X_4 + X_6 + a(m_1 + m_2) X_7 + a^2 m_1 m_2 X_8 = 0$  which passes through  $Q$  if and only if

$$m_1 m_2 q_1 - (m_1 + m_2) q_3 - 2am_1 m_2 q_4 + q_6 + a(m_1 + m_2) q_7 = 0. \quad (5)$$

In particular, if we can determine  $m_1, m_2$  and  $a$  such that (5) is satisfied, then the point  $Q$  is not special.

A similar argument applies when  $q_7 = 0$ .

Let now  $q \equiv 1 \pmod{3}$  and  $\omega$  be a root of  $T^2 + T + 1 = 0$  Consider a non-singular plane cubic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  with canonical equation:

$$X^3 + Y^3 + Z^3 - 3cXYZ = 0,$$

where  $c \neq \infty, 1, \omega, \omega^2$ .

If  $c = 1 + \sqrt{3}$ , then the elliptic curve  $\mathcal{E}$  is harmonic that is,  $j(\mathcal{E}) \neq 0$ , see [10, Lemma 11.47]. Using Remark 3 and the symmetry  $Y \leftrightarrow Z$  of the curve  $\mathcal{E}$  it is possible to test for the completeness of  $\nu_3^2(\mathcal{E})$ . With the aid of GAP [7], we see that for  $q = 121$  we obtain a curve with  $n = 144$  rational points, for  $q = 157, 169$  we obtain curves with  $n = 180$  rational points whereas for  $q = 179$  we get a curve with  $n = 180$  points and in each case the  $n$  rational points define a complete NMDS code.

## Acknowledgements

This research was carried out within the activities of the GNSAGA - Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni of the Italian INdAM.

## References

- [1] Abatangelo, V., Larato, B. *Near-MDS codes arising from algebraic curves*, Discrete Math. **301** (2005), no. 1, 5—19.
- [2] Abatangelo V., Larato B. *Elliptic near-MDS codes over  $F_5$* , Des. Codes Cryptogr. **46** (2008), no. 2, 167—174.
- [3] Buekenhout, F. *Generalized elliptic cubic curves. I*. Finite geometries, 35–48, Dev. Math.,**3**, Kluwer Acad. Publ., Dordrecht, 2001.
- [4] Dodunekov, S. M. and Landjev, I. N., *On near MDS codes*, J. Geom., **54** (1995), no.1–2, 30–43.
- [5] Dodunekov, S. M. and Landjev, I. N. *Near-MDS codes over some small fields* Discrete Math., **213**, (2000), no. 1–3, 55–65.
- [6] Eisenbud, D. , Green, M. and Harris, J. *Cayley-Bacharach theorems and conjectures* Bull. Amer. Math. Soc. (N.S.), **33**, (1996), no. 3, 295–324.
- [7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.0; 2020. (<https://www.gap-system.org>)

- [8] Giulietti M., *On the extendibility of near-MDS elliptic codes* Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 1—11
- [9] Landjev, I. N. *Linear codes over finite fields and finite projective geometries* Selected topics in discrete mathematics (Warsaw, 1996). Discrete Math. **213** (2000), no. 1–3, 211—244.
- [10] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998.
- [11] W.M. Kantor, E.E. Shult, *Veroneseans, power subspaces and independence*, Adv. Geom. 13 (2013), 511–531.
- [12] N. Kaplan, V. Matei, *Counting plane cubic curves over finite fields with a prescribed number of rational intersection points*, preprint arXiv:2003.13944.
- [13] F.J. MacWilliams, N.J.A. Sloane, *The theory of Error-Correcting codes*, North-Holland (1977).
- [14] J.H. Silvermann, *The arithmetic of Elliptic Curves*, Springer-Verlag (1986).
- [15] M.A. Tsfasman, S.G. Vlăduț, D.Yu. Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society (2007).