ON NEAR-MDS ELLIPTIC CODES

MASSIMO GIULIETTI

Abstract. The Main Conjecture on maximum distance separable (MDS) codes states that, except for some special cases, the maximum length of a q-ary linear MDS code of is $q+1$. This conjecture does not hold true for near maximum distance separable codes because of the existence of q-ary near-MDS elliptic codes having length bigger than $q+1$. An interesting related question is whether a near-MDS elliptic code may be extended to a longer near-MDS code. Our results are some non-extendability results and an alternative and simpler construction for certain known near-MDS elliptic codes.

Keywords: Projective Spaces, Near-MDS Codes, Elliptic Curves.

1. Introduction

Let F_q be a finite field with q elements and ${F_q}^n$ the vector space of n-tuples over F_q. A q-ary linear code $\mathbf{C}$ of length n and dimension k is a k-dimensional subspace of ${F_q}^n$. The number of non-zero positions in a vector $\mathbf{x} \in \mathbf{C}$ is called the Hamming weight $w(\mathbf{x})$ of $\mathbf{x}$; the Hamming distance $d(\mathbf{x},\mathbf{y})$ between two vectors $\mathbf{x},\mathbf{y} \in \mathbf{C}$ is defined by $d(\mathbf{x},\mathbf{y}) = w(\mathbf{x}-\mathbf{y})$. The minimum distance of $\mathbf{C}$ is

$$d(\mathbf{C}) := \min\{w(\mathbf{x}) \mid \mathbf{x} \in \mathbf{C}, \mathbf{x} \neq 0\},$$

and a q-ary linear code of length n, dimension k and minimum distance d is indicated as an $[n,k,d]_q$ code. For such codes the Singleton bound holds:

$$d \le n-k+1.$$

The non-negative integer $s(\mathbf{C}) := n-k+1-d$ is referred to as the Singleton defect of $\mathbf{C}$.

A linear code $\mathbf{C}$ with $s(\mathbf{C}) = 0$ is said to be maximum distance separable, or briefly MDS. A code with $s(\mathbf{C}) = 1$ is called almost-MDS, or AMDS

Massimo Giulietti is with the Dipartimento di Matematica e Informatica, Università di Perugia, 06123 Perugia, Italy. E-mail: giuliet@dipmat.unipg.it.

This research was performed within the activity of GNSAGA of the Italian CNR, with the financial support of the Italian Ministry MIUR, project “ Strutture geometriche, combinatoria e loro applicazioni”, PRIN 2001-2002.

for short. The dual $\mathbf{C}^{\perp}$ of a code $\mathbf{C}$ consists of all the vectors of ${F_q}^n$ orthogonal to every codewords in $\mathbf{C}$:

$$\mathbf{C}^{\perp} := \{\mathbf{x} \in {F_q}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for any } \mathbf{y} \in \mathbf{C}\},$$

where $\langle , \rangle$ denotes the inner product in ${F_q}^n$. Unlike the MDS case, the dual of an AMDS code need not be AMDS. This motivates to define $\mathbf{C}$ to be near-MDS (NMDS) when $s(\mathbf{C}) = s(\mathbf{C}^{\perp}) = 1$.

For given k and q, let $m(k, q)$ be the maximum length of a q-ary linear MDS code of dimension k. The Main Conjecture on MDS codes states that $m(k, q) = q + 1$ provided that $2 \le k < q$, except for the case $m(3, q) = m(q-1, q) = q+2$ for even q (see e.g. [25, p. 13]). The situation is quite different for NMDS codes, since q-ary linear NMDS codes of length bigger than $q + 1$ arise from elliptic curves via Goppa construction. In particular the following theorem holds ([25, Sec. 3.2]).

Theorem 1.1. *Let $q = p^m$, p prime. An $[n, k, d]_q$ NMDS code can be constructed from an elliptic curve over F_q having exactly n F_q-rational points, for every $k = 2, 3, \ldots, n-1$.*

It should be noted that the proof of Theorem 1.1 which appears in Tsfasman-Vladut book [25] depends on deep algebraic geometry. Here in Section 2 only elementary facts from algebraic geometry are used to construct certain $[n, k, d]_q$ NMDS codes from an elliptic curve with n F_q-rational points (cf. Theorem 2.2). We will refer to such codes as k-elliptic codes.

For every prime power q, Theorem 1.1 provides NMDS codes of length up to $N_q(1)$, where $N_q(1)$ denotes the maximum number of F_q-rational points that an elliptic curve defined over F_q can have. From work by Waterhouse [28], we know that for every $q = p^r$, p prime,

$$N_q(1) = \begin{cases} q + \lceil 2\sqrt{q} \rceil, & \text{for } p \mid \lceil 2\sqrt{q} \rceil \text{ and odd } r \ge 3, \\ q + \lceil 2\sqrt{q} \rceil + 1, & \text{otherwise,} \end{cases}$$

where $\lceil x \rceil$ is the integer part of x.

Constructing $[n, k, d]_q$ NMDS codes of length bigger than $N_q(1)$ appears to be hard for $q \ge 17$ and $k \ge 3$ (see [2]). In Sections 3 and 4 we discuss the related problem whether such codes can be obtained by extending NMDS k-elliptic codes. In that context the following definition turns out to be useful.

Definition 1.2. An $[n, k, d]_q$ code $\mathbf{C}$ is h-extendable if there exists an $[n+h, k, d+h]_q$ code $\mathbf{C}'$ such that $\pi_{n,h}(\mathbf{C}') = \mathbf{C}$, where $\pi_{n,h} : {F_q}^{n+h} \to {F_q}^n$, $\pi_n(a_1, \ldots, a_{n+h}) = (a_1, \ldots, a_n)$. A 1-extendable code is simply referred to as extendable code.

With this definition, our main result is stated as follows:

Theorem 1.3. *Let $q \geq 121$ be an odd prime power. Let $\mathcal{E}$ be an elliptic curve defined over F_q whose j-invariant $j(\mathcal{E})$ is different from 0. Then,*

(1) *for $k = 3, 6$, the k-elliptic code associated to $\mathcal{E}$ is non-extendable;*
(2) *for $k = 4$, the k-elliptic code associated to $\mathcal{E}$ is not 2-extendable;*
(3) *for $k = 5$, the k-elliptic code associated to $\mathcal{E}$ is not 3-extendable.*

2. Elliptic Codes

¿From now on, K denotes the algebraic closure of the finite field with q elements F_q, and $(X_1, X_2, \dots, X_k)$ are homogeneous coordinates for $\mathbf{P}^{k-1}(K)$. We also let $X = X_2/X_1$ and $Y = X_3/X_1$ be the non-homogeneous coordinates for $\mathbf{P}^2(K)$. As usual we identify $(X, Y) \in K^2$ with the point $(1, X, Y) \in \mathbf{P}^2(K)$.

Also, $\mathcal{E}$ denotes an elliptic plane curve defined over F_q with affine equation

$$f(X,Y) := Y^2 + a_1XY + a_2Y - X^3 - a_3X^2 - a_4X - a_5 = 0\,,$$

where $a_i \in F_q$ for $i = 1, \dots, 5$.

Let $n := \#\mathcal{E}(F_q)$, the number of F_q-rational points of $\mathcal{E}$. Then $\mathcal{E}(F_q)$ consists of $n-1$ affine points, say $P_1, \dots, P_{n-1}$, together with its infinite point $P_n = P_\infty = (0, 0, 1)$.

Let $\Sigma = K(x, y)$ be the rational function field of $\mathcal{E}$, that is the field of fractions of the domain $K[X, Y]/(f(X, Y))$, where $x = X + (f(X, Y))$ and $y = Y + (f(X, Y))$. For any point $P \in \mathcal{E}$ and for any $\alpha \in \Sigma$ let $v_P(\alpha)$ denote the order of α in P. For $v_P(\alpha) = h > 0$, the point P is a zero of α of multiplicity h, and for $v_P(\alpha) = h < 0$ the point P is a pole of α of multiplicity $-h$. By a classical result (see e.g. [25, Thm. 2.1.50]), any rational function $\alpha \neq 0$ on an irreducible plane curve defined over an algebraically closed field has as many zeros as poles, counted with multiplicity, and α has no zero (and no pole) if and only if α is constant. As usual, the number of zeros of $\alpha \in \Sigma$ is indicated by $\mathrm{ord}(\alpha)$. In our case $\mathrm{ord}(x) = 2$, $\mathrm{ord}(y) = 3$, $v_{P_\infty}(x) = -2$ and $v_{P_\infty}(y) = -3$.

For any integer $i > 1$, let

$$\psi_i(X,Y) := \begin{cases} Y^s & \text{if } i = 3s,\ s \geq 1\,, \\ XY^s & \text{if } i = 3s+2,\ s \geq 0\,, \\ X^2Y^s & \text{if } i = 3s+4,\ s \geq 0\,. \end{cases}$$

Note that $v_{P_\infty}(\psi_i(x, y)) = -i$ and hence $\mathrm{ord}(\psi_i(x, y)) = i$.

Then, for any $k \in \{3, 4, \dots, n-1\}$ define the morphism

$$\varphi_k := \begin{cases} \mathcal{E} & \rightarrow & \mathbf{P}^{k-1}(K) \\ (1,X,Y) & \mapsto & (1,\psi_2(X,Y),\psi_3(X,Y),\ldots,\psi_k(X,Y)) \end{cases} .$$

Note that $\varphi_k(P_n) = (0,0,\ldots,0,1)$.

Let $G_k(\mathcal{E})$ be the $(k \times n)$ matrix whose i^{th}-column is the k-tuple $\varphi_k(P_i)$ for $i = 1,\ldots n$.

Definition 2.1. The subspace of ${F_q}^k$ spanned by the rows of $G_k(\mathcal{E})$ is called the k-elliptic code associated to $\mathcal{E}$.

Remark. In the notation of [25], the k-elliptic code associated to $\mathcal{E}$ is a special Goppa code, more precisely the code obtained from $(\mathcal{E},\mathcal{P},D)_L$ by continuation to the point P_∞ ([25, p. 271]), with $\mathcal{P} = \{P_1,\ldots,P_{n-1}\}$ and $D = kP_\infty$.

We are in a position to prove the following theorem.

Theorem 2.2. *For every k with $3 \leq k \leq n-1$, the k-elliptic code $\mathbf{C}$ associated to $\mathcal{E}$ is either an NMDS code or an MDS code of length n and dimension k.*

Proof. The proof consists of three steps.

Step 1. The dimension of $\mathbf{C}$ is equal to k and $d(\mathbf{C}) \geq n-k$.

For any hyperplane $\mathcal{H}$ of $\mathbf{P}^{k-1}(F_q)$, we need to show that

$$\#(\mathcal{H} \cap \varphi_k(\mathcal{E}(F_q)) \leq k\,.$$

Let $\mathcal{H} : a_1X_1+a_2X_2+\ldots+a_kX_k = 0$. Note that for every $P \in \mathcal{E}(F_q)$, $P \neq P_\infty$, we have that $\varphi_k(P) \in \mathcal{H}$ if and only if $P \in \mathcal{C}(F_q)$, where $\mathcal{C}$ is the plane curve of equation $h(X,Y) := a_1 + a_2\psi_2(X,Y) + \ldots + a_k\psi_k(X,Y) = 0$.

Suppose at first that $a_k \neq 0$, that is $\varphi_k(P_\infty) \notin \mathcal{H}$. Then $\#(\mathcal{H} \cap \varphi_k(\mathcal{E}(F_q))$ is equal to the number of affine points in $\mathcal{C}(F_q) \cap \mathcal{E}(F_q)$, and hence $\#(\mathcal{H} \cap \varphi_k(\mathcal{E}(F_q)) \leq \mathrm{ord}(h(x,y))$. Note that $h \neq 0$, otherwise $\mathcal{E}$ would be a component of $\mathcal{C}$. But this is impossible, since $h(X,Y)$ has degree in X at most 2. Then $v_{P_\infty}(h) \geq -k$, hence $\mathrm{ord}(h) \leq k$ and the assertion follows.

Now, let $a_k = 0$. Then we have $\varphi_k(P_\infty) \in \mathcal{H}$, whence $\#(\mathcal{H} \cap \varphi_k(\mathcal{E}(F_q)) \leq 1 + \mathrm{ord}(h)$. Again, the assertion follows since $v_{P_\infty}(h) \geq -(k-1)$ yields $\mathrm{ord}(h) \leq k-1$.

Step 2. The dimension of $\mathbf{C}^\perp$ is equal to $n-k$ and $d(\mathbf{C}^\perp) \geq k$.

We need to prove that any $k-1$ points in $\varphi_k(\mathcal{E}(F_q))$ are linearly independent. Suppose on the contrary that there exists a set $\mathcal{B}$ of $k-1$ points in $\varphi_k(\mathcal{E}(F_q))$ contained in two distinct hyperplanes of $\mathbf{P}^{k-1}(F_q)$, say $\mathcal{H}_1 : a_1X_1+a_2X_2+\ldots+a_kX_k = 0$ and $\mathcal{H}_2 : b_1X_1+b_2X_2+\ldots+b_kX_k = 0$, and consider the rational functions $h_1 := a_1 + a_2\psi_2(x,y) + \ldots + a_k\psi_k(x,y)$ and $h_2 := b_1 + b_2\psi_2(x,y) + \ldots + b_k\psi_k(x,y)$.

If $(0,0,\ldots,1) \notin \mathcal{B}$, then h_1 and h_2 have at least $k-1$ common zeros. Moreover, since both h_1 and h_2 have order at most k, the rational function h_1/h_2 has either no or just one zero. In the former case h_1/h_2 is constant, whence $\mathcal{H}_1 = \mathcal{H}_2$, a contradiction. In the latter case, $\mathrm{ord}(h_1/h_2) = 1$, and therefore $\mathcal{E}$ is isomorphic to $\mathbf{P}^1(K)$, which is impossible.

Suppose now that $(0,0,\ldots,1) \in \mathcal{B}$. Therefore $a_k = b_k = 0$, hence $\mathrm{ord}(h_1)$ and $\mathrm{ord}(h_2)$ are both less than or equal to $k-1$, and h_1 and h_2 have at least $k-2$ zeros in common. This yields $\mathrm{ord}(h_1/h_2) \in \{0,1\}$ and we get the same contradiction as above.

Step 3. **C** is NMDS or MDS.

Step 1 yields that **C** is AMDS or MDS. By Step 2 we have $s(\mathbf{C}^{\perp}) \leq 1$, and hence the theorem is proved. □

Remark. We point out that apart from a few possibilities the k-elliptic code in Theorem 2.2 is an NMDS code. This is indeed the case as soon as $\mathcal{E}$ has $n \geq 5$ F_q-rational points, but a counterexample is known to exist for $n = 4$, see [25, Thm 3.2.19]. Here we give an elementary proof under the weaker hypothesis $n \geq 12$. With same notation as in the proof of Theorem 2.2, we have to prove

$$\#(\mathcal{H} \cap \varphi_k(\mathcal{E}(F_q)) = k\,,$$

for some hyperplane $\mathcal{H}$ of $\mathbf{P}^{k-1}(F_q)$. Let $m := \lceil \frac{k+1}{3} \rceil$. We begin by noting that every $h(X,Y) \in F_q[X,Y]$ of degree m satisfies

$$h(X,Y) - (a_1 + a_2\psi_2(X,Y) + \ldots + a_{3m}\psi_{3m}(X,Y)) = g(X,Y)f(X,Y)$$

for certain $a_1,\ldots,a_{3m} \in F_q,\ g \in K[X,Y]$.

Now, take an F_q-rational plane curve $\mathcal{X}$ of order m such that (i) $\mathcal{A} := \mathcal{X} \cap \mathcal{E}$ consists of $3m$ F_q-rational points of $\mathcal{E}$, (ii) $P_\infty \notin \mathcal{A}$ for $k \equiv 1 \pmod 3$ and $P_\infty \in \mathcal{A}$ for $k \equiv -1 \pmod 3$. It should be noted that our assumption $n \geq 12$ is used at this point for the case $m = 2$. If $\mathcal{X}$ has equation $h(X,Y) = 0$ and the coefficients a_i are defined as before, then the curve of equation $a_1 + a_2\psi_2(X,Y) + \ldots + a_{3m}\psi_k(X,Y) = 0$ passes through all points in $\mathcal{A}$. Note that the equation $\mathcal{H} : a_1X_1 + a_2X_2 + \ldots + a_{3m}X_{3m} = 0$ defines a hyperplane $\mathcal{H}$ for every k, since for $k = 3m-1$ $P_\infty \in \mathcal{A}$ yields $a_{3m} = 0$. Then $\mathcal{H}$ meets $\varphi_k(\mathcal{E}(F_q))$ in exactly k points.

3. Plane elliptic curves and intersections with lines

The proof of Theorem 1.3 depends on some results on the number of F_q-rational lines through a given point P which meet an elliptic cubic curve in exactly three F_q-rational points. The aim of this section is to state and prove such results.

We limit ourselves to the odd order case, that is the underlying projective plane $\mathbf{P}^2(F_q)$ is assumed to be of odd order q. Then a canonical form for an elliptic cubic curve $\mathcal{E}$ of $\mathbf{P}^2(F_q)$ is $Y^2 = X^3 + aX^2 + bX + c$, with $a, b, c \in F_q$ (see e.g. [22, p. 46]).

We begin with the following lemma.

Lemma 3.1. *For every point $P \in \mathbf{P}^2(F_q)$ not on $\mathcal{E}$,*

(i) *there exist at most 6 tangents of $\mathcal{E}$ passing through P;*
(ii) *if P is affine, then at least one non-vertical line through P is tangent of $\mathcal{E}$.*

Proof. The assertion (i) is a classical result in zero characteristic, and it holds true in positive characteristic $p > 3$. So, we may assume that $p = 3$. Now, if the assertion is false, then more than 6 tangents to $\mathcal{E}$ pass through P, and hence more than 6 points of $\mathcal{E}$ belong to the polar quadric $\mathcal{C}$ of P with respect to $\mathcal{E}$ (see [11, Lemma 11.4]). Since $\mathcal{E}$ is irreducible, Bézout Theorem yields that $\mathcal{C}$ is actually indeterminate, and hence a line of nuclei of $\mathcal{E}$ contains P according to [11, Thm. 11.20(iv)]. A straightforward computation shows that then $a = b = 0$. But this contradicts the non-singularity of $\mathcal{E}$.

(ii) It is straightforward to check that the intersection between $\mathcal{E}$ and the polar quadric of $P = (x_0, y_0)$ with respect to $\mathcal{E}$ does not entirely consist of points on the line $X = x_0$. □

Let $j(\mathcal{E})$ denote the j-invariant of the elliptic curve $\mathcal{E}$. We start with the case $j(\mathcal{E}) \neq 0$. The following lemma is an extension of a result by Hirschfeld and Voloch ([14, Thm. 5.1]).

Lemma 3.2. *Let $q \geq 121$, and $j(\mathcal{E}) \neq 0$. Then seven or more lines through a given F_q-rational point P outside $\mathcal{E}$ intersect $\mathcal{E}$ in 3 distinct F_q-rational points.*

Proof. Assume at first that P is an affine point, and put $P = (P_x, P_y)$. Define the rational function $F(X, Y, Z)$ by

$$-Z^2 - Z\big(a + X - (\frac{Y - P_y}{X - P_x})^2\big) - \big(X^2 + aX + b - 2P_y(\frac{Y - P_y}{X - P_x}) - \frac{(Y - P_y)^2}{X - P_x}\big)$$

Let $Q = (Q_x, Q_y)$ be an F_q-rational affine point of $\mathcal{E}$ such that $Q_x \neq P_x$. The line through P and Q intersects $\mathcal{E}$ in two more (not necessarily distinct) points, say A and B. Then the X-coordinates of A and B are roots of the polynomial $F(Q_x, Q_y, Z)$. In fact, this follows from

$$F(Q_x, Q_y, Z) = \frac{1}{Z - Q_x}\big(\big(\frac{Q_y - P_y}{Q_x - P_x}(Z-P_x)+P_y\big)^2 - Z^3 - aZ^2 - bZ - c\big)\,.$$

Next we prove that quadratic polynomial $\tilde{F}(Z) = F(x, y, Z)$ is irreducible in $\Sigma[Z]$. To do this we may suppose that $F(x, y, Z) = g(x, y)(Z - h_1(x, y))(Z - h_2(x, y))$, with $g, h_1, h_1 \in \Sigma$. For $i = 1, 2$, define the rational maps

$$\Phi_i := \begin{cases} \quad \mathcal{E} & \rightarrow \qquad\qquad\qquad \mathcal{E} \\ (1, X, Y) & \mapsto \quad \big(1, h_i(X, Y), \frac{Y-P_y}{X-P_x}(h_i(X, Y) - P_x) + P_y\big) \end{cases}.$$

By definition of F, if $Q = (Q_x, Q_y) \in \mathcal{E}$ with $Q_x \neq P_x$, then $\Phi_i(Q)$ belongs to both $\mathcal{E}$ and the line through Q and P. Moreover, if Φ_i fixes a point on a non-vertical line through P then such a line is a tangent of $\mathcal{E}$. By Lemma 3.1(i), we have then that Φ_i has order greater than 4 or equal to 3. Finally, let l be a non-vertical tangent of $\mathcal{E}$ through P (such a line exists by Lemma 3.1(ii)). Then, either Φ_1 or Φ_2 fixes a point in $l \cap \mathcal{E}$, and therefore the irreducibility of $F(x, y, Z)$ over $\Sigma(Z)$ follows from Corollary 4.7 in [9]. Now, we may define the algebraic curve $\mathcal{E}'$ as the curve in $\mathbf{P}^3(K)$ whose rational function field is $\Sigma(z)$, z being a root of $\tilde{F}$. Note that the projection $\pi : \mathcal{E}' \to \mathcal{E}\,,\ \pi(X, Y, Z) = (X, Y)$ is a rational map of degree two.

Suppose that $R = (1, x_1, y_1, z_1)$, $x_1 \neq P_x$, is an F_q-rational point of $\mathcal{E}'$ which is not a ramification point of π. Let $\pi^{-1}(\pi(R)) = \{R, R'\}$, with $R' = (1, x_1, y_1, z_2)$. Then $(x_1, y_1) \in \mathcal{E}$ and $F(x_1, y_1, z_1) = F(x_1, y_1, z_2) = 0$; this means that the line through P and (x_1, y_1) intersects $\mathcal{E}$ in three distinct F_q-rational points. Then Lemma 3.2 for an affine point P follows from the following assertion: The curve $\mathcal{E}'$ has at least 14 affine F_q-rational non-ramification points $(1, x_1, y_1, z_1)$ such that $x_1 \neq P_x$. To prove it, we note at first that a ramification point for π is a point $(1, x_1, y_1, z_1)$ such that the line through P and (x_1, y_1) is a tangent to $\mathcal{E}$. By Lemma 3.1(i), we may have at most 6 ramification points.

By Hurwitz Theorem ([25, Thm. 2.2.36]) we have that the genus g of $\mathcal{E}'$ satisfies $2g - 2 \leq 6$, and hence $g \leq 4$. Let N denote the number of F_q-rational points of $\mathcal{E}'$. By Hasse-Weil Theorem ([25, p. 177]) we have $N \geq q + 1 - 8\sqrt{q}$, hence $N \geq 34$ from our hypothesis $q \geq 121$. Then the assertion follows, since $\deg(\mathcal{E}') = 6$ yields that at most 12 points of $\mathcal{E}'$ are in the union of the plane at infinity and the plane of equation $X = P_x$.

Now assume that P is an infinite point, and put $P = (0, 1, m)$. The proof is similar to the proof given for P affine. Here we define

$$F_1(x, y, Z) := \frac{1}{Z - x}\Big(\big(m(Z - x) + y\big)^2 - Z^3 - aZ^2 - bZ - c\Big)$$

instead of F. We remark that Lemma 3.1(ii) may not hold for P, since it may happen that the only tangent line through P is the line at infinity. However, when this occurs, the irreducibility of $\tilde{F}_1$ still follows from Corollary 4.7 in [9], since both Φ_1 and Φ_2 fix the point $(0, 0, 1)$. □

For $j(\mathcal{E}) = 0$ a result follows from [8, Thm 5.2].

Lemma 3.3. *Let $q = p^r$, $p > 3$, $q > 9887$. Suppose that $j(\mathcal{E}) = 0$ and that $\mathcal{E}$ has an even number of F_q-rational points. If r is even or $p \equiv 1 \pmod 3$, then seven or more lines through a given F_q-rational point outside $\mathcal{E}$ intersect $\mathcal{E}$ in 3 distinct F_q-rational points.*

4. Proof of the Theorem 1.3

We keep our notation and terminology used in Section 3. Our approach is based on a strong relationship between k-elliptic codes and certain point-sets in $\mathbf{P}^{k-1}(F_q)$ characterized by purely combinatorial properties. According to [12], an $(n; k, k-2)$-set in $\mathbf{P}^{k-1}(F_q)$ is defined as a set consisting of n points no $k + 1$ of which lie on the same hyperplane of $\mathbf{P}^{k-1}(F_q)$. An $(n; k, k-2)$-set in $\mathbf{P}^{k-1}(F_q)$ is complete if it is maximal with respect to set-theoretical inclusion. From the proof of Theorem 2.2, the points of $\varphi_k(\mathcal{E}(F_q))$ form an $(n; k, k-2)$-set in $\mathbf{P}^{k-1}(F_q)$.

Lemma 4.1. *A k-elliptic code $\mathbf{C}$ is not-extendable if and only if the corresponding $\varphi_k(\mathcal{E}(F_q))$ is a complete $(n; k, k-2)$-set in $\mathbf{P}^{k-1}(F_q)$.*

Proof. We have to prove that $\mathbf{C}$ is extendable if and only if there exists a point P in $\mathbf{P}^{k-1}(F_q) \setminus \varphi_k(\mathcal{E}(F_q))$ such that no hyperplane through P intersects $\varphi_k(\mathcal{E}(F_q))$ in k points.

Fix a generator matrix for $\mathbf{C}$, say $G_k(\mathcal{E})$, and suppose that no hyperplane through $P \in \mathbf{P}^{k-1}(F_q) \setminus \varphi_k(\mathcal{E}(F_q))$ intersects $\varphi_k(\mathcal{E}(F_q))$ in k points. Let $G_k(\mathcal{E})'$ be the matrix obtained from $G_k(\mathcal{E})$ by adding an extra-column whose entries are the homogeneous coordinates of P. Then the subspace $\mathbf{C}'$ of ${F_q}^k$ spanned by the rows of $G_k(\mathcal{E})'$ is a $[n + 1, k, n - k + 1]_q$ code with $\pi_{n,1}(\mathbf{C}') = \mathbf{C}$.

On the other hand, let $\mathbf{C}'$ be an $[n + 1, k, n - k + 1]_q$ code with $\pi_{n,1}(\mathbf{C}') = \mathbf{C}$. Let $R_1 = (r_{11}, \dots, r_{1(n+1)}), \dots, R_k = (r_{k1}, \dots, r_{k(n+1)})$ be an F_q-base of $\mathbf{C}'$ such that $\pi_{n,1}(R_i)$ is the i-th row of $G_k(\mathcal{E})$. Then no hyperplane through the point $P = (r_{1(n+1)}, \dots, r_{k(n+1)})$ intersects $\varphi_k(\mathcal{E}(F_q))$ in k points. $\square$

Arguing as in Lemma 4.1, a more general result can actually be proved.

Corollary 4.2. *The k-elliptic code C of length n is not h-extendable if the corresponding $(n; k, k-2)$-set $\varphi_k(\mathcal{E}(F_q))$ is either complete or can be completed by at most $h-1$ points.*

We begin the proof of Theorem 1.3 by noting that the hypothesis $q \geq 121$ together with the Hasse-Weil theorem ensures the existence of at least seven F_q-rational points on $\mathcal{E}$. This shows that k-elliptic codes with $k \leq 6$ certainly arise from $\mathcal{E}$.

According to Corollary 4.2, Theorem 1.3 will be proved once we have shown that the $(n; k, k-2)$-set $\varphi_k(\mathcal{E}(F_q))$ is either complete or it can be completed by adding at most $h-1$ points where

$$h := \begin{cases} 1 & \text{for } k = 3, 6\,; \\ 2 & \text{for } k = 4\,; \\ 3 & \text{for } k = 5\,. \end{cases}$$

Lemma 3.2 allows us to choose a frame in $\mathbf{P}^2(F_q)$ satisfying the following conditions:

- the line of equation $X = 0$ meets $\mathcal{E}$ in two affine F_q-rational points, both distinct from $(0,0)$;
- both lines $Y = 0$ and $X = Y$ meet $\mathcal{E}$ in three affine F_q-rational points.

We distinguish several cases according to the value of k.

Case $k = 3$.
By Lemma 3.2, $\varphi_3(\mathcal{E}(F_q))$ is complete.

Case $k = 4$.
Let $\varphi_4(\mathcal{E}(F_q))$ be incomplete, and choose a point $Q = (Q_1, Q_2, Q_3, Q_4)$ in $\mathbf{P}^3(F_q)$ that can be added to $\varphi_4(\mathcal{E}(F_q))$. We show that such a point Q lies on the line through the fundamental points $(0,0,1,0)$ and $(0,0,0,1)$. In fact, for $(Q_1, Q_2, Q_3) \neq (0,0,1)$, Lemma 3.2 implies the existence of a line $l : a + bX + cY = 0$ through $P = (Q_1, Q_2, Q_3)$ that meets $\mathcal{E}$ in three distinct F_q-rational affine points. Then the plane of equation $aX_1 + bX_2 + cX_3 + 0X_4$ passes through Q and meets $\varphi_4(\mathcal{E})$ in 4 distinct F_q-rational points, more precisely the points in $\{\varphi_4(l \cap \mathcal{E}(F_q)), (0,0,0,1)\}$. But this is impossible since Q is assumed to be a point that can be added to $\varphi_4(\mathcal{E}(F_q))$. This contradiction proves the assertion. Now, to prove Theorem 1.3 for $k = 4$, we have to check that $\varphi_4(\mathcal{E}(F_q)) \cup \{Q\}$ is complete, that is no further point

$Q' = (0,0,1,\beta)$, $\beta \in F_q$, can be added to $\varphi_4(\mathcal{E}(F_q)) \cup \{Q\}$. But this follows immediately from the fact that the plane $X_2 = 0$ passes through Q', Q and three distinct points in $\varphi_4(\mathcal{E}(F_q))$, which are those in $\{\varphi_4(\{X=0\} \cap \mathcal{E}(F_q)), (0,0,0,1)\}$.

Case $k = 5$. Let $Q = (Q_1, Q_2, Q_3, Q_4, Q_5) \in \mathbf{P}^4(F_q) \setminus \varphi_5(\mathcal{E}(F_q))$. We need the following technical lemma.

Lemma 4.3. *If Q can be added to $\varphi_5(\mathcal{E}(F_q))$, then $Q_5Q_2 \neq 0$, $Q_4 = 0$ and $(1, 0, Q_5/Q_2) \in \mathcal{E}$.*

Proof. If $Q_5 = 0$, then the hyperplane $X_5 = 0$ meets $\varphi_5(\mathcal{E})$ in 5 distinct F_q-rational points, which are those in $\{\varphi_5(\{XY = 0\} \cap \mathcal{E}(F_q))\}$.

For $Q_5 \neq 0$, $Q_2 = 0$, $Q_4 = 0$, Lemma 3.2 ensures the existence a line l through $P = (0,0,1)$ which is different from $X = 0$ and meets $\mathcal{E}$ in two more distinct F_q-rational affine points. If l has equation $X + \alpha = 0$, then the hyperplane in $\mathbf{P}^4(F_q)$ of equation $\alpha X_2 + X_4 = 0$ passes through Q and meets $\varphi_5(\mathcal{E})$ in 5 distinct F_q-rational points, which are those in $\{\varphi_5(\{X(X+\alpha) = 0\} \cap \mathcal{E}(F_q)), (0,0,0,0,1)\}$.

Similarly, for $Q_5 \neq 0$, $Q_2 = 0$, $Q_4 \neq 0$: A line l through $P = (0, Q_4/Q_5, 1)$ meets $\mathcal{E}$ in three distinct F_q-rational affine points not lying on $X = 0$. If $l : \alpha(X - Q_4/Q_5Y) + \beta = 0$, then the hyperplane of equation $\beta X_2 + \alpha X_4 - \alpha Q_4/Q_5X_5 = 0$ passes through Q and meets $\varphi_5(\mathcal{E})$ in 5 distinct F_q-rational points. Also, for $Q_5 \neq 0$, $Q_2 \neq 0$, $Q_4 \neq 0$: A line of equation $\alpha(X - Q_4/Q_2) + \beta(Y - Q_5/Q_2) = 0$ meets $\mathcal{E}(F_q)$ in three distinct F_q-rational affine points not lying on $X = 0$, and the hyperplane $\alpha(X_4 - Q_4/Q_2X_2) + \beta(X_5 - Q_5/Q_2X_2) = 0$ passes through Q and meets $\varphi_5(\mathcal{E})$ in 5 F_q-rational points. Finally for $Q_5 \neq 0$, $Q_2 \neq 0$, $Q_4 = 0$, $(1, 0, Q_5/Q_2) \notin \mathcal{E}$: A line of equation $\alpha X + \beta(Y - Q_5/Q_2) = 0$ meets $\mathcal{E}(F_q)$ in three F_q-rational affine points not lying on $X = 0$, and the hyperplane $\alpha X_4 + \beta(X_5 - Q_5/Q_2X_2) = 0$ passes through Q and meets $\varphi_5(\mathcal{E})$ in 5 distinct F_q-rational points. This completes the proof of Lemma 4.3. $\square$

To settle the case $k = 5$ suppose that Q can be added to $\varphi_5(\mathcal{E}(F_q))$. Let $\{X = 0\} \cap \mathcal{E} = \{(0,0,1), (1,0,\lambda), (1,0,\mu)\}$, and assume $\lambda = Q_5/Q_2$.

Note that no point $Q' = (Q'_1, Q'_2, Q'_3, 0, Q'_5)$, with $Q'_2Q'_5 \neq 0$ and such that $Q'_5/Q'_2 = \lambda$ can be added to $\varphi_5(\mathcal{E}(F_q)) \cup \{Q\}$. Lemma 3.2 ensures the existence of a line l through $P = (1, 0, \lambda)$ that meets $\mathcal{E}$ in three distinct F_q-rational affine points, two of which not lying on $X = 0$. If $l : \alpha X + \beta(Y - \lambda) = 0$, then the hyperplane of equation $\alpha X_4 + \beta(X_5 - \lambda X_2) = 0$ passes through Q' and meets $\varphi_5(\mathcal{E}(F_q)) \cup \{Q\}$ in 5 distinct points.

This shows that if a point Q' can be added to $\varphi_5(\mathcal{E}(F_q)) \cup \{Q\}$ then $Q' = (Q'_1, 1, Q'_3, 0, \mu)$. Finally, a straightforward argument shows that $\varphi_5(\mathcal{E}(F_q)) \cup \{Q, Q'\}$ is complete.

Case $k = 6$.

Given any point $Q = (Q_1, Q_2, Q_3, Q_4, Q_5, Q_6) \in \mathbf{P}^5(F_q) \setminus \varphi_6(\mathcal{E})$, we have to find a hyperplane $\mathcal{H}$ of $\mathbf{P}^5(F_q)$ through Q that meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points. To do this, we distinguish a number of cases, even if we use the same kind of argument depending on Lemma 3.2.

1) $Q_5 = 0$. The hyperplane $X_5 = 0$ passes through Q and meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points, which are those in $\{\varphi_6(\{XY = 0\} \cap \mathcal{E}(F_q)), (0, 0, 0, 0, 0, 1)\}$.

2) $Q_5 = 1$, $Q_4 = Q_6 = 0$, $Q_2 \neq Q_3$. Let l be a line through $P = (1, \frac{1}{Q_3 - Q_2}, -\frac{1}{Q_3 - Q_2})$ meeting $\mathcal{E}$ in three distinct F_q-rational points outside the line $X = Y$. If l has equation $\alpha(1+(Q_3-Q_2)Y)+\beta(X+Y) = 0$, then the hyperplane $\alpha(X_2-X_3)+\beta X_4+\alpha(Q_3-Q_2)X_5+(-\beta-\alpha(Q_3-Q_2))X_6 = 0$ passes through Q and meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points, more precisely the points in $\{\varphi_6((\{X - Y = 0\} \cup l) \cap \mathcal{E}(F_q))\}$.

3) $Q_5 = 1$, $Q_4 = Q_6 = 0$, $Q_2 = Q_3$. A line of equation $\alpha+\beta(X+Y) = 0$ meets $\mathcal{E}$ in three distinct F_q-rational points outside the line $X = Y$. Then the hyperplane of equation $\alpha(X_2 - X_3) + \beta X_4 - \beta X_6 = 0$ passes through Q and meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points.

4) $Q_5 = 1$, $Q_6 \neq 0, Q_3 = 0$. A line of equation $\alpha + \beta(X - Y/Q_6) = 0$ meets $\mathcal{E}$ in three distinct F_q-rational points outside the line $Y = 0$. Then the hyperplane of equation $\alpha X_3 + \beta X_5 - \beta/Q_6 X_6 = 0$ passes through Q and meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points.

5) $Q_5 = 1$, $Q_6 \neq 0, Q_3 \neq 0$. A line of equation $\alpha(X - 1/Q_3) + \beta(Y - Q_6/Q_3) = 0$ meets $\mathcal{E}$ in three distinct F_q-rational points outside the line $Y = 0$, and the hyperplane $\alpha(X_5 - X_3/Q_3) + \beta(X_6 - Q_6/Q_3 X_3) = 0$ passes through Q and meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points.

6) $Q_5 = 1$, $Q_4 \neq 0, Q_2 = 0$. A line of equation $\alpha(X - Q_4 Y) + \beta = 0$ meets $\mathcal{E}$ in three distinct F_q-rational points not lying on the line $X = 0$. Then the hyperplane $\alpha(X_4 - Q_4 X_5) + \beta X_2 = 0$ passes through Q and meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points, which are those in $\{\varphi_6((\{X = 0\} \cup l) \cap \mathcal{E}(F_q)), (0, 0, 0, 0, 0, 1)\}$.

7) $Q_5 = 1$, $Q_4 \neq 0, Q_2 \neq 0$. A line of equation $\alpha(X-Q_4/Q_2)+\beta(Y-1/Q_2) = 0$ meets $\mathcal{E}$ in three distinct F_q-rational points outside the line $X = 0$, and the hyperplane $\alpha(X_4 - Q_4/Q_2 X_2) + \beta(X_5 - X_2/Q_2) = 0$ passes through Q and meets $\varphi_6(\mathcal{E})$ in 6 distinct F_q-rational points.

As a consequence of Lemma 3.3, an analogous to Theorem 1.3 can be proved for some cubics $\mathcal{E}$ with $j(\mathcal{E}) = 0$.

Theorem 4.4. *Let $q = p^r$, $p > 3$, $q > 9887$. Let $\mathcal{E}$ be an elliptic curve defined over F_q, with $j(\mathcal{E}) = 0$ and having an even number of F_q-rational points. If r is even or $p \equiv 1 \pmod 3$, then*

1. *for $k = 3, 6$, the k-elliptic code associated to $\mathcal{E}$ is non-extendable;*
2. *for $k = 4$, the k-elliptic code associated to $\mathcal{E}$ is not 2-extendable;*
3. *for $k = 5$, the k-elliptic code associated to $\mathcal{E}$ is not 3-extendable.*

Remark. Our method still works for $k > 6$ even if some modification is needed. However, the result is not so sharp as for $k \leq 6$ since it only ensures non-h-extendability for h sufficiently bigger than k.

Acknowledgments

The author would like to thank Prof. G. Korchmáros and Prof. F. Torres for their useful comments.

References

[1] Chen, H., Yau, S.S.-T.: Contribution to Munuera's Problem on the Main Conjecture of Geometric Hyperelliptic MDS Codes. IEEE Trans. Inform. Theory **43** 1349–1354, (1997).
[2] De Boer, M.A.: Almost MDS codes. Des. Codes Cryptogr. **9**, 143–155 (1996).
[3] Di Comite, C.: Su k-archi deducibili da cubiche piane. Atti Accad. Naz. Lincei Rend. **33**, 429–435 (1962).
[4] Di Comite, C.: Intorno a certi $(q+9)/2$-archi completi di $S_{2,q}$. Atti Accad. Naz. Lincei Rend. **36**, 819–824 (1964).
[5] S.M. Dodunekov, S.M., Landjev, I.N.: On near-MDS codes. J. Geom. **54**, 30–43 (1995).
[6] Driencourt, Y., Michon, J.F.: Remarques sur les codes geometriques. C.R. Acad. Sci., Paris, Ser. I **301**, 15–17 (1986).
[7] Fulton, W.: Algebraic Curves. An introduction to Algebraic Geometry. New York: W.A. Benjamin 1969.
[8] Giulietti, M.: On plane arcs contained in cubic curves. Finite Fields Appl. **8**, 69–90 (2002).
[9] Hartshorne, R.: Algebraic Geometry. Grad. Texts in Math. Vol. 52. Berlin New York: Springer Verlag 1977.
[10] Hirschfeld, J.W.P.: Finite Projective Spaces of Three dimension. Oxford: Oxford University Press 1985.
[11] Hirschfeld, J.W.P.: Projective Geometries Over Finite Fields, 2nd edition. Oxford: Oxford University Press 1998.
[12] Hirschfeld, J.W.P., Storme, L.: The packing problem in statistics, coding theory and finite projective planes. J. Statist. Plann. Inference **72**, 355–380 (1998).
[13] Hirschfeld J.W.P., Thas, J.A.: General Galois Geometries. Oxford: Clarendon Press 1991.
[14] Hirschfeld J.W.P., Voloch, J.F.: The characterization of elliptic curves over finite fields. J. Austral. Math. Soc. Ser. A **45**, 275–286 (1988).
[15] Landjev, I.N.: Linear codes over finite fields and finite projective geometries. Discrete Math. **213**, 211–244 (2000).

[16] MacWilliams, F.J., Sloane, N.J.: The theory of error-correcting codes. Amsterdam: North-Holland 1977.

[17] Marcugini, S., Milani, A., Pambianco, F.: Existence and classification of NMDS codes over $GF(5)$ and $GF(7)$. Proceedings of ACCT2000, the Seventh International Workshop on Algebraic and Combinatorial Coding Theory, Bulgaria, June 2000, 232–239.

[18] Marcugini, S., Milani, A., Pambianco, F.: MNDS codes of maximal length over $GF(q)$, $8 \leq q \leq 11$. IEEE Trans. Inform. Theory, submitted.

[19] Munuera, C.: On the main conjecture on geometric MDS codes. IEEE Trans. Inform. Theory **38**, 1573–1577 (1992).

[20] Munuera, C.: On MDS elliptic codes. Discrete Math. **117** 279–286 (1993).

[21] Shokrollahi, M.A.: Minimum Distance of Elliptic Codes Adv. in Math. **93** 251–281 (1992).

[22] Silverman, J.H.: The Arithmetic of Elliptic Curves. Berlin Heidelbeg New York Tokio: Springer Verlag 1986.

[23] Stichtenoth, H.: Algebraic Function Fields and Codes. Berlin Heidelbeg New York Tokio: Springer Verlag 1993.

[24] Szőnyi, T.: Arcs in cubic curves and 3-independent subsets of abelian groups. Combinatorics, Eger, Colloq. Math. Soc. János Bolyai **52** , 499–508 (1987).

[25] Tsfasman, M.A., Vladut, S.G.: Algebraic-Geometric Codes. Amsterdam: Kluwer 1991.

[26] Voloch, J.F.: On the completeness of certain plane arcs. European J. Combin. **8**, 453–456 (1987).

[27] Voloch, J.F.: On the completeness of certain plane arcs II. European J. Combin. **11**, 491–496 (1990).

[28] Waterhouse, W.G.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. **2**, 521–560 (1969).

[29] Zirilli, F.: Su una classe di k-archi di un piano di Galois. Atti Accad. Naz. Lincei Rend. **54** , 393–397 (1973).