On maximal plane curves of degree 3 over $\mathbb{F}_4$, and Sziklai's example of degree $q-1$ over $\mathbb{F}_q$

Masaaki Homma
Department of Mathematics and Physics, and
Research Institute for Integrated Science
Kanagawa University
Hiratsuka 259-1293, Japan
homma@kanagawa-u.ac.jp

Abstract

The classification of maximal plane curves of degree 3 over $\mathbb{F}_4$ will be given, which complements Hirschfeld-Storme-Thas-Voloch's theorem on a characterization of Hermitian curves in $\mathbb{P}^2$. This complementary part should be understood as the classification of Sziklai's example of maximal plane curves of degree $q-1$ over $\mathbb{F}_q$. Although two maximal plane curves of degree 3 over $\mathbb{F}_4$ up to projective equivalence over $\mathbb{F}_4$ appear, they are birationally equivalent over $\mathbb{F}_4$ each other.
Key Words: Plane curve, Finite field, Rational point, Maximal curve
MSC: 14G15, 14H50, 14G05, 11G20, 05B25

1 Introduction

This paper is concerned with upper bounds for the number of $\mathbb{F}_q$-points of plane curves defined over $\mathbb{F}_q$. Let C be a plane curve defined by a homogeneous equation $f \in \mathbb{F}_q[x_0, x_1, x_2]$. The set of $\mathbb{F}_q$-points $C(\mathbb{F}_q)$ of C is $\{(a_0, a_1, a_2) \in \mathbb{P}^2 \mid a_0, a_1, a_2 \in \mathbb{F}_q \text{ and } f(a_0, a_1, a_2) = 0\}$. The cardinality of $C(\mathbb{F}_q)$ is denoted by $N_q(C)$, and the degree of C by $\deg C$, or simply by d. We are interesting in upper bounds for $N_q(C)$ with respect to $\deg C$.

Aubry-Perret's generalization [1] of the Hasse-Weil bound implies that for absolutely irreducible plane curve of degree d over $\mathbb{F}_q$,

$$N_q(C) \leq q + 1 + (d-1)(d-2)\sqrt{q}. \tag{1}$$

On the other hand, the Sziklai bound established by a series of papers of Kim and the author [3, 4, 5] gives a one under a more mild condition, that is, for C without $\mathbb{F}_q$-linear components,

$$N_q(C) \leq (d-1)q + 1 \tag{2}$$

except for the curve over $\mathbb{F}_4$ defined by

$$(x_0 + x_1 + x_2)^4 + (x_0x_1 + x_1x_2 + x_2x_0)^2 + x_0x_1x_2(x_0 + x_1 + x_2) = 0.$$

When $d < \sqrt{q} + 1$, the Aubry-Perret generalization of Hasse-Weil bound is better than the Sziklai bound, however when $d > \sqrt{q} + 1$, the latter is better than the former, and these two bounds meet at $d = \sqrt{q} + 1$, that is, both (1) and (2) imply

$$N_q(C) \leq \sqrt{q}^3 + 1 \text{ if } \deg C = \sqrt{q} + 1, \tag{3}$$

where q is an even power of a prime number. From now on, when a statement contains $\sqrt{q}$, we tacitly understand q to be an even power of a prime number.

Three decades ago, Hirschfeld, Storme, Thas and Voloch [2] gave a characterization of Hermitian curves of degree $\sqrt{q} + 1$ over $\mathbb{F}_q$, which is a maximal curve in the sense of the bound (3).

Theorem 1.1 (Hirschfeld-Storme-Thas-Voloch) *In $\mathbb{P}^2$ over $\mathbb{F}_q$ with $q \neq 4$, a curve over $\mathbb{F}_q$ of degree $\sqrt{q}+1$, without $\mathbb{F}_q$-linear components, which contains $\sqrt{q}^3+1$ $\mathbb{F}_q$-points, is a Hermitian curve.*

For $q = 4$, they gave an example of a nonsingular plane curve over $\mathbb{F}_4$ which had $9\,(= 2^3 + 1)$ $\mathbb{F}_4$-points, but was not a Hermitian. Actually the plane curve defined by

$$x_0^3 + \omega x_1^3 + \omega^2 x_2^3 = 0 \tag{4}$$

is such an example, where $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$.

Our primary concern is to complete the determination of plane curves over $\mathbb{F}_q$ of degree $\sqrt{q} + 1$ with $\sqrt{q}^3 + 1$ $\mathbb{F}_q$-points.

Theorem 1.2 *Let C be a plane curve over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components. If $\deg C = \sqrt{q} + 1$ and $N_q(C) = \sqrt{q}^3 + 1$, then C is either*

(i) *a Hermitian curve, or*

(ii) *a nonsingular curve of degree 3 which is projectively equivalent to the curve (4) over $\mathbb{F}_4$.*

The second case (ii) in the above theorem should be understood the case of $q = 4$ among Sziklai's curves [8] of degree $q - 1$ that achieve the Sziklai bound (2). Here a Sziklai's curve means one over $\mathbb{F}_q$,of degree $q - 1$ defined by the following type of equation:

$$\alpha x_0^{q-1} + \beta x_1^{q-1} + \gamma x_2^{q-1} = 0 \text{ with } \alpha\beta\gamma \neq 0 \text{ and } \alpha + \beta + \gamma = 0. \tag{5}$$

The curve (5) will be denoted by $C_{(\alpha,\beta,\gamma)}$. Since $x^{q-1} = 1$ for any $x \in \mathbb{F}_q^*$ and $\alpha + \beta + \gamma = 1$,

$$C_{(\alpha,\beta,\gamma)}(\mathbb{F}_q) \supset \mathbb{P}^2(\mathbb{F}_q) \setminus (\cup_{i=0}^2 \{x_i = 0\}). \tag{6}$$

Here $\{x_i = 0\}$ denotes the line defined by $x_i = 0$. Furthermore, since $\deg C_{(\alpha,\beta,\gamma)} = q-1$,

$$N_q(C_{(\alpha,\beta,\gamma)}) \le (q-2)q + 1 = (q-1)^2$$

by the Szikali bound. Therefore equality must hold in (6), that is,

$$C_{(\alpha,\beta,\gamma)}(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q) \setminus (\{x_0 = 0\} \cup \{x_1 = 0\} \cup \{x_2 = 0\}). \tag{7}$$

Note that $C_{(\alpha,\beta,\gamma)}$ makes sense under the condition $q > 2$.

Theorem 1.3 *The number ν_q of projective equivalent classes over $\mathbb{F}_q$ in the family of curves*

$$\{C_{(\alpha,\beta,\gamma)} \mid \alpha, \beta, \gamma \in \mathbb{F}_q^*,\ \alpha + \beta + \gamma = 0\}$$

is as follows:

(I) *Suppose that the characteristic of $\mathbb{F}_q$ is neither 2 nor 3.*

- (I-i) *If $q \equiv 2 \bmod 3$, then $\nu_q = \frac{q+1}{6}$.*
- (I-ii) *If $q \equiv 1 \bmod 3$, then $\nu_q = \frac{q+5}{6}$.*

(II) *Suppose that q is a power of 3. Then $\nu_q = \frac{q+3}{6}$.*

(III) *Suppose that q is a power of 2.*

- (III-i) *If $q = 2^{2s+1}$, that is, $q \equiv 2 \bmod 3$, then $\nu_q = \frac{q-2}{6}$.*
- (III-ii) *If $q = 2^{2s}$, that is, $q \equiv 1 \bmod 3$, then $\nu_q = \frac{q+2}{6}$.*

In this theorem, we don't assume $q > 2$ explicitly, however the assertion (III-i) says the family of curves in question is empty if $q = 2$.

The construction of this article is as follows:

In Section 2, we will give the proof of Theorem 1.3 together with the characterization of Sziklai's curve of degree $q-1$.

In Section 3, we will give the proof of Theorem 1.2; actually we will handle the case $q = 4$.

In Section 4, we will make explicitly an $\mathbb{F}_4$-isomorphism between the function field of the Hermitian curve over $\mathbb{F}_4$ defined by $x_0^3 + x_1^3 + x_2^3 = 0$ and that of the curve (4).

2 Sziklai's example of maximal curves of degree $q-1$

The purpose of this section is to prove Theorem 1.3. Let $\mathscr{S}_q = \{C_{(\alpha,\beta,\gamma)} \mid \alpha, \beta, \gamma \in \mathbb{F}_q^*,\ \alpha + \beta + \gamma = 0\}$. The first step of the proof is to give a characterization of the member of $\mathscr{S}_q$.

Proposition 2.1 *Let C be a possibly reducible plane curve over $\mathbb{F}_q$ of degree $q-1$. Then $C \in \mathscr{S}_q$ if and only if*

$$C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q) \setminus \left(\cup_{i=0}^{2}\{x_i = 0\}\right). \tag{8}$$

The "only if" part has already observed in Introduction. Now we prove the "if" part.

Lemma 2.2 *In $\mathbb{A}^2$ with coordinates x, y over $\mathbb{F}_q$, the ideal I in $\mathbb{F}_q[x, y]$ of the set $\{(a, b) \in \mathbb{F}_q^2 \mid ab \neq 0\}$ is $(x^{q-1} - 1, y^{q-1} - 1)$.*

Furthermore, if $f(x, y) \in I$ is of degree at most $q-1$, then $f(x, y) = \alpha(x^{q-1} - 1) + \beta(y^{q-1} - 1)$ for some $\alpha, \beta \in \mathbb{F}_q$.

Proof. Let J denote the ideal $(x^{q-1} - 1, y^{q-1} - 1)$ of $\mathbb{F}_q[x, y]$. Obviously $J \subseteq I$. For $f(x, y) \in I$, there are polynomials $g_i(x) \in \mathbb{F}_q[x]$ $(0 \le i \le q-2)$ of degree $\le q-2$ so that

$$f(x, y) \equiv \sum_{i=0}^{q-2} g_i(x) y^i \bmod J.$$

For each $a \in \mathbb{F}_q^*$, the equation $\sum_{i=0}^{q-2} g_i(a) y^i = 0$ has to have $q-1$ $(= |\mathbb{F}_q^*|)$ solutions because $\sum_{i=0}^{q-2} g_i(x) y^i \in I$. Hence $g_i(a) = 0$ for any i. Since $\deg g_i \le q-2$, g_i must be the zero polynomial. Hence $f(x, y) \equiv 0 \bmod J$. This completes the proof of the first part.

For the second part, let α and β be the coefficients of x^{q-1} and y^{q-1} in $f(x, y)$ respectively. Then

$$f(x, y) - \alpha(x^{q-1} - 1) - \beta(y^{q-1} - 1) = \sum_{i=1}^{q-2} u_{q-1-i}(x) y^i + v_{q-2}(x), \tag{9}$$

where $\deg u_{q-1-i}(x) \le q-1-i$ $(\le q-2)$ and $\deg v_{q-2}(x) \le q-2$. So the same argument as above works well, and we know the right side of (9) is the zero polynomial. □

Proof of Proposition 2.1. Choose a homogeneous equation $f(x_0, x_1, x_2) = 0$ of degree $q-1$ over $\mathbb{F}_q$ for a given curve C with the property (8). From Lemma 2.2, there are elements $\alpha, \beta \in \mathbb{F}_q$ such that $f(\frac{x_0}{x_2}, \frac{x_1}{x_2}, 1) = \alpha((\frac{x_0}{x_2})^{q-1} - 1) + \beta((\frac{x_1}{x_2})^{q-1} - 1)$. Therefore $f(x_0, x_1, x_2) = x_2^{q-1} f(\frac{x_0}{x_2}, \frac{x_1}{x_2}, 1) = \alpha(x_0^{q-1} - x_2^{q-1}) + \beta(x_1^{q-1} - x_2^{q-1})$. Since $C(\mathbb{F}_q) \cap \{x_2 = 0\}$ is empty, $f(a, b, 0) \neq 0$ for any $(a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}$. In particular, $\alpha = f(1, 0, 0) \neq 0$, $\beta = f(0, 1, 0) \neq 0$ and $\alpha + \beta = f(1, 1, 0) \neq 0$. Hence $C \in \mathscr{S}_q$. □

Now we want to classify $\mathscr{S}_q$ up to projective equivalence over $\mathbb{F}_q$.

Definition 2.3 Let C be a possibly reducible curve in $\mathbb{P}^2$ over $\mathbb{F}_q$, and δ a nonnegative integer. An $\mathbb{F}_q$-line l is said to be a δ-line with respect to C if $|l \cap C(\mathbb{F}_q)| = \delta$.

δ	the number of δ-lines
0	3
$q-2$	$(q-1)^2$
$q-1$	$3(q-1)$

Table 1: δ-lines w.r.t. $C \in \mathscr{S}_q$

Lemma 2.4 *Let $C \in \mathscr{S}_q$, and δ a nonnegative integer such that a δ-line with respect to C actually exists. Then δ is either 0 or $q-2$ or $q-1$, and the number of δ-lines are as in Table 1.*

Proof. Note that $q > 2$ because $\mathscr{S}_q$ is not empty. Since $\mathbb{P}^2(\mathbb{F}_q) = C(\mathbb{F}_q) \sqcup (\cup_{i=0}^{2}\{x_i = 0\})$ (where the symbol $\sqcup$ indicates disjoint union) and $q > 2$, the possible values of δ are 0, $q-2$ and $q-1$. Obviously the number of 0-lines is 3. A $(q-1)$-line is not a 0-line, and passes through one of intersection points of two 0-lines. Other lines are $(q-2)$-lines. □

We need an elementary fact on the finite group action, so called "Burnside's lemma" [7, Corollary 7.2.9].

Lemma 2.5 *Let G be a finite group which acts on a finite set X. For $g \in G$, $\operatorname{Fix} g$ denotes the set of fixed points of g on X. Then the number ν of orbits of G on X is given by*

$$\nu = \frac{1}{|G|}\sum_{g\in G} |\operatorname{Fix} g|.$$

Proof. Let us consider the set

$$\mathscr{C} := \{(g, x) \in G \times X \mid g \cdot x = x\}$$

with projections $p_1(g, x) = g$ and $p_2(g, x) = x$. Counting $|\mathscr{C}|$ by using p_1, $|\mathscr{C}| = \sum_{g\in G} |\operatorname{Fix} g|$, and by p_2, $|\mathscr{C}| = \sum_{x\in X} |G_x|$, where G_x is the isotropy subgroup of $x \in X$. Let $x_1, \ldots, x_\nu$ be the set of complete representatives of the orbits of G on X. Then

$$\sum_{x\in X} |G_x| = \sum_{i=1}^{\nu} |Gx_i| \cdot |G_{x_i}| = \nu|G|,$$

where Gx_i is the orbit containing x_i. So $\nu|G| = \sum_{g\in G} |\operatorname{Fix} g|$. □

Proof of Theorem 1.3. The first claim is that if two members $C_{(\alpha,\beta,\gamma)}, C_{(\alpha',\beta',\gamma')} \in \mathscr{S}_q$ are projectively equivalent over $\mathbb{F}_q$, then the point $(\alpha', \beta', \gamma') \in \mathbb{P}^2(\mathbb{F}_q)$ is a permutation of the point $(\alpha, \beta, \gamma) \in \mathbb{P}^2(\mathbb{F}_q)$, that is, there is a nonzero element $\lambda \in \mathbb{F}_q^*$ such that the triple $(\lambda\alpha', \lambda\beta', \lambda\gamma')$ is a permutation of the triple (α, β, γ).

Actually, let Σ be a projective transformation so that $\Sigma C_{(\alpha,\beta,\gamma)} = C_{(\alpha',\beta',\gamma')}$. Note that Σ induces an automorphism of the homogeneous coordinate ring $\mathbb{F}_q[x_0, x_1, x_2]$, which is denoted by Σ^*. The set of 0-lines with respect to each of curves in $\mathscr{S}_q$ is $\{\{x_0 = 0\}, \{x_1 = 0\}, \{x_2 = 0\}\}$ by Lemma 2.4. Hence Σ induces a permutation of those three lines. Hence $\Sigma^*(x_i) = u_i x_{\sigma(i)}$ for some $u_i \in \mathbb{F}_q^*$, and $(\sigma(0), \sigma(1), \sigma(2))$ is a permitation of $(0,1,2)$. Hence

$$\Sigma^*(\alpha x_0^{q-1} + \beta x_1^{q-1} + \gamma x_2^{q-1}) = \alpha x_{\sigma(0)}^{q-1} + \beta x_{\sigma(1)}^{q-1} + \gamma x_{\sigma(2)}^{q-1}$$

because $u_i^{q-1} = 1$.

So we need to classfy $\mathscr{S}_q/\mathbb{F}_q^*$ by the action of S_3 as permutations on coefficients.

Observe the map

$$\rho : \mathscr{S}_q/\mathbb{F}_q^* \ni C_{(\alpha,\beta,\gamma)} \to (\alpha : \beta) \in \mathbb{P}^1,$$

which is well-defined and

$$\operatorname{Im} \rho = \mathbb{P}^1 \setminus \{(0,1), (1,0), (1,-1)\}.$$

Obviously, ρ gives a one to one correspondence, so S_3 acts on $\operatorname{Im} \rho$ also. Table 2 shows the S_3-action on $\operatorname{Im} \rho$ explicitly.

S_3	$\mathscr{S}_q/\mathbb{F}_q^*$	$\operatorname{Im} \rho$
(1)	$(\alpha,\beta,\gamma) \mapsto (\alpha,\beta,\gamma)$	$(\alpha : \beta) \mapsto (\alpha : \beta)$
$(1,2)$	$(\alpha,\beta,\gamma) \mapsto (\beta,\alpha,\gamma)$	$(\alpha : \beta) \mapsto (\beta : \alpha)$
$(2,3)$	$(\alpha,\beta,\gamma) \mapsto (\alpha,\gamma,\beta)$	$(\alpha : \beta) \mapsto (\alpha : -(\alpha+\beta))$
$(1,3)$	$(\alpha,\beta,\gamma) \mapsto (\gamma,\beta,\alpha)$	$(\alpha : \beta) \mapsto (-(\alpha+\beta) : \beta)$
$(1,2,3)$	$(\alpha,\beta,\gamma) \mapsto (\gamma,\alpha,\beta)$	$(\alpha : \beta) \mapsto (-(\alpha+\beta) : \alpha)$
$(1,3,2)$	$(\alpha,\beta,\gamma) \mapsto (\beta,\gamma,\alpha)$	$(\alpha : \beta) \mapsto (\beta : -(\alpha+\beta))$

Table 2: S_3-action on $\operatorname{Im} \rho$

Now we compute the number of fixed points on $\operatorname{Im} \rho$ by each $\sigma \in S_3$.

- Fixed points of the identity (1) are all the $q-2$ points of $\operatorname{Im} \rho$.
- $(\alpha : \beta) \in \operatorname{Fix}(1,2) \Leftrightarrow (\alpha : \beta) = (\beta : \alpha) \Leftrightarrow \alpha^2 - \beta^2 = 0$. If the characteristic of $\mathbb{F}_q \neq 2$, then $\operatorname{Fix}(1,2) = \{(1:1)\}$ because $(1:-1) \notin \operatorname{Im} \rho$. If q is a power of 2, then $\operatorname{Fix}(1,2)$ is empty.
- $(\alpha : \beta) \in \operatorname{Fix}(2,3) \Leftrightarrow (\alpha : \beta) = (\alpha : -(\alpha+\beta)) \Leftrightarrow \alpha = -2\beta$ because $\alpha \neq 0$. If the characteristic of $\mathbb{F}_q \neq 2$, then $\operatorname{Fix}(2,3) = \{(-2:1)\}$. If q is a power of 2, then $\operatorname{Fix}(2,3)$ is empty.
- $(\alpha : \beta) \in \operatorname{Fix}(1,3) \Leftrightarrow (\alpha : \beta) = (-(\alpha+\beta) : \beta) \Leftrightarrow \beta = -2\alpha$ because $\beta \neq 0$. If the characteristic of $\mathbb{F}_q \neq 2$, then $\operatorname{Fix}(1,3) = \{(1:-2)\}$. If q is a power of 2, then $\operatorname{Fix}(1,3)$ is empty.
- $(\alpha : \beta) \in \operatorname{Fix}(1,2,3) \Leftrightarrow (\alpha : \beta) = (-(\alpha+\beta) : \alpha) \Leftrightarrow \alpha^2 + \alpha\beta + \beta^2 = 0 \Leftrightarrow (\alpha : \beta) = (\eta : 1)$ with $\eta^2 + \eta + 1 = 0$ and $\eta \in \mathbb{F}_q$.
- $(\alpha : \beta) \in \operatorname{Fix}(1,3,2) \Leftrightarrow (\alpha : \beta) = (\beta : -(\alpha+\beta)) \Leftrightarrow \alpha^2 + \alpha\beta + \beta^2 = 0 \Leftrightarrow (\alpha : \beta) = (\eta : 1)$ with $\eta^2 + \eta + 1 = 0$ and $\eta \in \mathbb{F}_q$.

For the last two cases, since a cubic root of 1 other than 1 exists in $\mathbb{F}_q$ if and only if $q \equiv 1 \bmod 3$, and only the cubic root of 1 is 1 if q is a power of 3,

$$|\operatorname{Fix}(1,2,3)| = |\operatorname{Fix}(1,3,2)| = \begin{cases} 2 & \text{if } q \equiv 1 \bmod 3 \\ 1 & \text{if } q \text{ is a power of } 3 \\ 0 & \text{else.} \end{cases}$$

The number of fixed points can be summarized as in Table 3.

Case	$\lvert\operatorname{Fix}(1)\rvert$	$\lvert\operatorname{Fix}(12)\rvert$	$\lvert\operatorname{Fix}(13)\rvert$	$\lvert\operatorname{Fix}(23)\rvert$	$\lvert\operatorname{Fix}(123)\rvert$	$\lvert\operatorname{Fix}(132)\rvert$
(I-i)	$q-2$	1	1	1	0	0
(I-ii)	$q-2$	1	1	1	2	2
(II)	$q-2$	1	1	1	1	1
(III-i)	$q-2$	0	0	0	0	0
(III-ii)	$q-2$	0	0	0	2	2

Table 3: Number of fixed points

Since $\nu_q = \frac{1}{6}\sum_{\sigma\in S_3} |\operatorname{Fix}\sigma|$ by Lemma 2.5, we are able to know ν_q explicitly. □

At the end of this section, we raise a question: are there maximal plane curves over $\mathbb{F}_q$ of degree $q-1$ other than Sziklai's example?

3 Maximal curves of degree 3 over $\mathbb{F}_4$

Let C be a plane curve of degree 3 over $\mathbb{F}_4$ without $\mathbb{F}_4$-linear components, and $N_4(C) = 9$. Since the degree of C is 3, C is absolutely irreducible. If C had a singular point, then C would be an image of $\mathbb{P}^1$, and hence $N_4(C)$ would be at most $6\,(= N_4(\mathbb{P}^1) + 1)$. Therefore C is nonsingular.

Thanks to the Hirschfeld-Storme-Thas-Voloch theorem, only the missing case for the classification of maximal curves of degree $\sqrt{q}+1$ is the case of $q = 4$.

Theorem 3.1 *Let C be a nonsingular plane curve of degree 3 over $\mathbb{F}_4$. If $N_4(C) = 9$, then C is either*

(i) *Hermitian, or*

(ii) *projectively equivalent to the curve*

$$x_0^3 + \omega x_1^3 + \omega^2 x_2^3 = 0,$$

where $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$.

Notation 3.2 Let l be an $\mathbb{F}_4$-line in $\mathbb{P}^2$. The symbol $l.C$ denotes the divisor $\sum_{P\cap C} i(l.C; P)P$ on C, where $i(l.C; P)$ is the local intersection multiplicity of l and C at P. Note that though $l.C$ is defined over $\mathbb{F}_4$, a point P in the support of $l.C$ may not be $\mathbb{F}_4$-point.

From now on, we consider a nonsingular plane curve C of degree 3 with $N_4(C) = 9$, and lines over $\mathbb{F}_4$.

Lemma 3.3 *Let l be a 2-line with respect to C, say $l \cap C(\mathbb{F}_4) = \{P_1, P_2\}$. Then $l.C = 2P_1 + P_2$ or $P_1 + 2P_2$.*

Proof. Since $\deg C = 3$, there is a closed point Q of C such that $l.C = P_1 + P_2 + Q$. Applying the Frobenius map F_4 over $\mathbb{F}_4$ to both side of the above equality, we know $P_1 + P_2 + Q = P_1 + P_2 + F_4(Q)$, which implies that the point Q is also $\mathbb{F}_4$-point. Therefore Q must concide with either P_1 or P_2 because l is a 2-line. □

Lemma 3.4 *Let l_0 be a 1-line with respect to C, say $l_0 \cap C(\mathbb{F}_4) = \{P\}$. Then $l_0.C = 3P_0$.*

Proof. Consider all the $\mathbb{F}_4$-lines passing through the point P, say $l_0, l_1, \ldots, l_4$. Counting $N_4(C)$ by using the disjoint union

$$C(\mathbb{F}_q) = \{P\} \sqcup \left(\sqcup_{i=1}^{4}(l_i \cap C(\mathbb{F}_4) \setminus \{P\})\right),$$

we know that $|l_i \cap C(\mathbb{F}_4) \setminus \{P\}|$ is 2, that is the remaining four lines $l_1, \ldots l_4$ to be 3-lines with respect to C. So each of them meets with C transversally because $\deg C = 3$. Therefore l_0 is the tangent line to C at P. Hence there is a closed point $Q \in C$ such that $l_0.C = 2P + Q$. Apply F_4 to this divisor, Q should be $\mathbb{F}_4$-points. Since l_0 is a 1-line, $Q = P$. □

Definition 3.5 Since C is nonsingular, for any closed point $P \in C$, the tangent line to C at P exists, which is a unique line l such that $i(l.C; P) \geq 2$. This line is denoted by $T_P(C)$. A point P with $i(T_P(C).C; P) = 3$ is called a flex or an inflection point. It is obvious that if P is an $\mathbb{F}_4$-points, then $T_P(C)$ is an $\mathbb{F}_4$-line.

Corollary 3.6 *Let $P \in C(\mathbb{F}_4)$.*

(i) *If $i(T_P(C).C; P) = 3$, then $T_P(C)$ is a 1-line, and conversely, if an $\mathbb{F}_4$-line l passing through P is a 1-line, then $l = T_P(C)$ and $i(T_P(C).C; P) = 3$.*

(ii) *If $i(T_P(C).C; P) = 2$, then $T_P(C)$ is a 2-line, and conversely, if an $\mathbb{F}_4$-line l passing through $P_1, P_2 \in C(\mathbb{F}_4)$ is a 2-line, then l coincides with either $T_{P_1}(C)$ or $T_{P_2}(C)$.*

Proof. (i) The first part is obvious because $\deg C = 3$, and the second part is a consequence of Lemma 3.4.

(ii) This is also a consequence of Lemma 3.4: since $T_P(C)$ is not a 1-line, it should be a 2-line, and the second part is just in Lemma 3.3 □

Notation 3.7 For each nonnegative integer $\delta \leq 3$, $\mathscr{L}_\delta$ denotes the set of δ-lines with respect to C, and μ_δ denotes the cardinality of the set $\mathscr{L}_\delta$.

The next lemma is essential for the proof of Theorem 3.1.

Lemma 3.8 *The possibilities of quadruple* $(\mu_0, \mu_1, \mu_2, \mu_3)$ *are either*

(i) $\mu_0 = 0,\ \mu_1 = 9,\ \mu_2 = 0,\ \mu_3 = 12$*; or*

(ii) $\mu_0 = 3,\ \mu_1 = 0,\ \mu_2 = 9,\ \mu_3 = 9$.

Proof. Step 1. Let us consider the correspondence

$$\mathscr{I} := \{(l, P) \in \check{\mathbb{P}}^2(\mathbb{F}_4) \times C(\mathbb{F}_4) \mid l \ni P\}$$

with projections $p_1 : \mathscr{I} \to \check{\mathbb{P}}^2(\mathbb{F}_4)$ and $p_2 : \mathscr{I} \to C(\mathbb{F}_4)$, where $\check{\mathbb{P}}^2(\mathbb{F}_4)$ is the projective space of the $\mathbb{F}_4$-lines. Since $|p_2^{-1}(P)| = 5$ for all $P \in C(\mathbb{F}_4)$ and $|C(\mathbb{F}_4)| = 9$, we know $|\mathscr{I}| = 45$.

From Corollary 3.6, the tangent line at an $\mathbb{F}_q$-point is a 1-line or 2-line, and vice versa. Since $\deg C = 3$, there are no bi-tangents. Hence

$$\mu_1 + \mu_2 = 9. \tag{10}$$

Since $|p^{-1}(l)| = \delta$ if l is a δ-line,

$$\mu_1 + 2\mu_2 + 3\mu_3 = |\mathscr{I}| = 45. \tag{11}$$

Additionally, since the total number of $\mathbb{F}_q$-lines is 21,

$$\mu_0 + \mu_1 + \mu_2 + \mu_3 = 21. \tag{12}$$

Step 2. Suppose that $\mu_1 = 0$. From (10), (11), (12), we have $\mu_0 = 3, \mu_2 = \mu_3 = 9$, which is the case (ii).

Step 3. Suppose that $\mu_1 \neq 0$. Since (10) and (11), $\mu_1 \equiv 0 \bmod 3$. Hence there are at least three 1-lines, and hence there are at least three inflection $\mathbb{F}_4$-points. Choose two inflection $\mathbb{F}_4$-points Q_1 and Q_2, and consider the line l_0 passing through these two points, which is an $\mathbb{F}_4$-line. Hence l_0 meets C at another point Q_0, which is also an $\mathbb{F}_4$-point.

Claim 1. Q_0 is also a flex.

We need more notation. The linear equivalence relation of divisors on C will be denoted by $\sim$, and a general line section on C by L. Here a general line section means a representative of the divisor cut out by a line on C, which makes sense up to the relation $\sim$.

Proof of claim 1. Since $Q_0 + Q_1 + Q_2 \sim L$ and $3Q_i \sim L$ for $i = 1$ and 2, we have $3Q_0 \sim 3L - 3Q_1 - 3Q_2 \sim L$, which means that Q_0 is a flex. □

Hence the following property holds.

(†) There are exactly three $\mathbb{F}_4$-lines passing through Q_0 besides l_0 and $T_{Q_0}(C)$, say l_1, l_2, l_3. Each l_i is a 3-line.

Actually, since

$$C(\mathbb{F}_4) = \{Q_0, Q_1, Q_2\} \sqcup \left(\sqcup_{i=1}^{3}(l_i \cap C(\mathbb{F}_4) \setminus \{Q_0\})\right)$$

and $|l_i \cap C(\mathbb{F}_4) \setminus \{Q_0\}| \leq 2$, each l_i is a 3-line.

The six points of $C(\mathbb{F}_4) \setminus \{Q_0, Q_1, Q_2\}$ are named $\{P_i^{(j)} \mid i = 1, 2, 3; j = 1, 2\}$ so that $l_i \cap C(\mathbb{F}_4) = \{Q_0, P_i^{(1)}, P_i^{(2)}\}$.

Claim 2. $\sum_{i=1}^3 (P_i^{(1)} + P_i^{(2)}) \sim 2L$.

Proof of claim 2. Since $Q_0 + P_i^{(1)} + P_i^{(2)} \sim L$ and $3Q_0 \sim L$, we get $L + \sum_{i=1}^3 (P_i^{(1)} + P_i^{(2)}) \sim 3L$. $\square$

Since a nonsingular plane curve is projectively normal, the divisor $\sum_{i=1}^3 (P_i^{(1)} + P_i^{(2)})$ on C is cut out by a quadratic curve. Let D be the quadratic curve passing through those six points. Suppose that D is absolutely irreducible. Then D has exactly five $\mathbb{F}_4$-points if it is defined over $\mathbb{F}_4$, or at most four $\mathbb{F}_4$-points if it is not defined over $\mathbb{F}_4$ because an $\mathbb{F}_4$-point of D is a point of $D \cap F_4(D)$; both are absurd. Therefore D is a union of two lines m, m'. If a line is not defined over $\mathbb{F}_4$, then $F_4(m) = m'$ and D has only one $\mathbb{F}_4$-point: also absured. Hence this split occurs over $\mathbb{F}_4$. Since $\deg C = 3$, those six points split into two groups; three of them lie on m and the remaining three lie on m', and $P_i^{(1)}$ and $P_i^{(2)}$ do not belong the same group. Hence we may assume that $P_1^{(1)}, P_2^{(1)}, P_3^{(1)} \in m$ and $P_1^{(2)}, P_2^{(2)}, P_3^{(2)} \in m'$. Note that m and m' do not contain Q_0 nor Q_1 nor Q_2.

Apply the same arguments to Q_1 instead of Q_0 after (†). Since Q_1 does not lie on m nor m', there is a permutation $(\sigma(1), \sigma(2), \sigma(3))$ of $(1, 2, 3)$ such that $Q_1, P_i^{(1)}, P_{\sigma(i)}^{(2)}$ are collinear for $i = 1, 2, 3$. Similarly, there is another permutation τ such that $Q_2, P_i^{(1)}, P_{\tau(i)}^{(2)}$ are collinear for $i = 1, 2, 3$. Therefore

$$\left.\begin{array}{rcl} Q_0 + P_1^{(1)} + P_1^{(2)} & \sim & L \\ Q_1 + P_1^{(1)} + P_{\sigma(1)}^{(2)} & \sim & L \\ Q_2 + P_1^{(1)} + P_{\tau(1)}^{(2)} & \sim & L \end{array}\right\} \tag{13}$$

Claim 3. $\{\sigma(1), \tau(1)\} = \{2, 3\}$.

Proof of claim 3. If not, two of $\{P_1^{(2)}, P_{\sigma(1)}^{(2)}, P_{\tau(1)}^{(2)}\}$ coincide. For example, if $P_1^{(2)} = P_{\sigma(1)}^{(2)}$, then $Q_0, P_1^{(1)}, P_1^{(2)} = P_{\sigma(1)}^{(2)}, Q_1$ are collinear, which is impossible because the line joining Q_0 and Q_1 is l_0. Other cases can be handled by similar way. $\square$

By this claim,

$$P_1^{(2)} + P_{\sigma(1)}^{(2)} + P_{\tau(1)}^{(2)} \sim L. \tag{14}$$

Hence adding all equivalence relations in (13), together with (14) we have $3P_1^{(1)} + 2L \sim 3L$, which implies $3P_1^{(1)} \sim L$. Hence $P_1^{(1)}$ is a flex. Similarly we have that any $P_i^{(j)}$ is a flex. Hence $\mu_1 = 9$. Hence, from (10), (11) and (12) in Step 1, $\mu_0 = 0$, $\mu_2 = 0$ and $\mu_3 = 12$. $\square$

Remark 3.9 In Step 3 of the proof of Lemma 3.8, what we have shown is essentially that if a point of $C(\mathbb{F}_4)$ is flex, then so are all points of $C(\mathbb{F}_4)$. If $C(\mathbb{F}_4)$ contains a flex, then C is defined over $\mathbb{F}_4$ as an elliptic curve. A sophisticated proof for the above fact may be possible by using the Jacobian variety, which coincides with the elliptic curve C. For details, see the first part of [6].

Proof of Theorem 3.1. When the case (ii) in Lemma 3.8 occurs, three 0-lines are not concurrent; Actually if three 0-lines are concurrent, there is an $\mathbb{F}_4$-point Q outside C, which these $\mathbb{F}_4$-lines pass through. The remaining two $\mathbb{F}_4$-lines pass through Q can't cover all the points of $C(\mathbb{F}_4)$.

Hence we may choose coordinates x_0, x_1, x_2 so that those 0-lines are $\{x_0 = 0\}$, $\{x_1 = 0\}$ and $\{x_2 = 0\}$. Since $|\mathbb{P}^2(\mathbb{F}_4) \setminus \cup_{i=0}^{2}\{x_i = 0\}| = 9 = |C(\mathbb{F}_4)|$, $C \in \mathscr{S}_4$ by Proposition 2.1. Furthermore since $|\mathscr{S}_4| = 1$ by Theorem 1.3 (III-ii), and $C_{(1,\omega,\omega^2)} \in \mathscr{S}_4$, C is projectively equivalent to to the curve

$$x_0^3 + \omega x_1^3 + \omega^2 x_2^3 = 0.$$

Next we consider the case (i) in Lemma 3.8. In this case C has the following properties:

(1) C is nonsingular of degree 3 defined over $\mathbb{F}_4$ with nine $\mathbb{F}_4$-points;

(2) for any $P \in C(\mathbb{F}_4)$, $i(T_P(C).C; P) = 3$;

(3) each point of $\mathbb{P}^2(\mathbb{F}_4) \setminus C(\mathbb{F}_4)$ lies on three tangent lines.

Here we will confirm the property (3). Among the five $\mathbb{F}_4$-lines passing through $Q \in \mathbb{P}^2(\mathbb{F}_4) \setminus C(\mathbb{F}_4)$, $\mu_\delta(Q)$ denotes the number of δ-lines. Since δ is either 1 or 3, $\mu_1(Q) + 3\mu_3(Q) = 9$ and $\mu_1(Q) + \mu_3(Q) = 5$. Hence $\mu_1(Q) = 3$.

The proof of [2, Lemma 7] works well under those three assumptions (1), (2), (3) for C. To adapt their proof to our case, beware of a difference of notation; their q is our $\sqrt{q}$. □

4 Comparison of two maximal curves of degree 3 over $\mathbb{F}_4$

Lastly we compare two maximal curves of degree 3

$$C: \; x_0^3 + x_1^3 + x_2^3 = 0$$

and

$$D: \; x_0^3 + \omega x_1^3 + \omega^2 x_2^3 = 0$$

over $\mathbb{F}_4 = \mathbb{F}_2[\omega]$.

Apparently, C and D are projectively equivalent over $\mathbb{F}_{2^6}$, but not over $\mathbb{F}_{2^2}$ as we have seen. We will show the function fields $\mathbb{F}_4(C)$ and $\mathbb{F}_4(D)$ are isomorphic over $\mathbb{F}_4$. This is already guaranteed theoretically by Rück and Stichtenoth [6]. Here we will give an explicit isomorphism between those two fields.

Let $x = \frac{x_0}{x_2}|C$ and $y = \frac{x_1}{x_2}|C$. Obviously $\mathbb{F}_4(C) = \mathbb{F}_4(x, y)$ with $x^3 + y^3 + 1 = 0$.

Theorem 4.1 *Three functions*

$$
\begin{aligned}
u &= 1 + \frac{x}{y+1} + \frac{1}{x+y+1} \\
v &= \omega^2 \frac{x}{y+1} + \frac{1}{x+y+1} \\
w &= \omega \frac{x}{y+1} + \frac{1}{x+y+1}
\end{aligned}
\tag{15}
$$

satisfy

$$u^3 + \omega v^3 + \omega^2 w^3 = 0.$$

Proof. By straightforward computation, we have

$$
\begin{aligned}
&((y+1)(x+y+1)w)^3 \\
=&(\omega x(x+y+1) + (y+1))^3 \\
=&x^3(x+y+1)^3 + \omega^2 x^2 (x+y+1)^2 (y+1) + \omega x(x+y+1)(y+1)^2 + (y+1)^3,
\end{aligned}
$$

$$
\begin{aligned}
&((y+1)(x+y+1)v)^3 \\
=&(\omega^2 x(x+y+1) + (y+1))^3 \\
=&x^3(x+y+1)^3 + \omega x^2 (x+y+1)^2 (y+1) + \omega^2 x(x+y+1)(y+1)^2 + (y+1)^3,
\end{aligned}
$$

and

$$
\begin{aligned}
&((y+1)(x+y+1)u)^3 \\
=&((y+1)(x+y+1) + x(x+y+1) + (y+1))^3 = g + h,
\end{aligned}
$$

where

$$
\begin{aligned}
g =&(y+1)^3(x+y+1)^3 + (y+1)^2(x+y+1)^2(x(x+y+1) + (y+1)) \\
&+ (y+1)(x+y+1)(x(x+y+1) + (y+1))^2,
\end{aligned}
$$

$$
\begin{aligned}
h =&(x(x+y+1) + (y+1))^3 \\
=&x^3(x+y+1)^3 + x^2(x+y+1)^2(y+1) + x(x+y+1)(y+1)^2 + (y+1)^3.
\end{aligned}
$$

Hence

$$
\begin{aligned}
\omega^2((y+1)(x+y+1)w)^3 &+ \omega((y+1)(x+y+1)v)^3 + h \\
=&(\omega^2 + \omega + 1)x^3(x+y+1)^3 \\
&+ (\omega^4 + \omega^2 + 1)x^2(x+y+1)^2(y+1) \\
&+ (\omega^3 + \omega^3 + 1)x(x+y+1)(y+1)^2 \\
&+ (\omega^2 + \omega + 1)(y+1)^3 \\
=&x(x+y+1)(y+1)^2.
\end{aligned}
$$

Therefore

$$\begin{aligned}&\omega^2((y+1)(x+y+1)w)^3+\omega((y+1)(x+y+1)v)^3+((y+1)(x+y+1)u)^3 \quad (16)\\ =&g+x(x+y+1)(y+1)^2\\ =&(y+1)(x+y+1)\Big\{(y+1)^2(x+y+1)^2+x(y+1)(x+y+1)^2\\ &+(y+1)^2(x+y+1)+x^2(x+y+1)^2+(y+1)^2+x(y+1)\Big\}.\end{aligned}$$

Since the sum of last two terms in the braces is $(x+y+1)(y+1)$, $(x+y+1)$ divides the polynomial in the braces. Hence (16) is equal to

$$(y+1)^3(x+y+1)^3(\omega^2w^3+\omega v^3+u^3)=(y+1)(x+y+1)^2f,$$

where

$$f=(y+1)^2(x+y+1)+x(y+1)(x+y+1)+(y+1)^2+x^2(x+y+1)+(y+1)$$

Continue the computation a little more:

$$\begin{aligned}f&=x(y+1)^2+(y+1)^3+x^2(y+1)+x(y+1)^2+(y+1)^2+x^3+x^2(y+1)+(y+1)\\ &=(y+1)^3+(y+1)^2+(y+1)+x^3\\ &=y^3+x^3+1=0.\end{aligned}$$

As a conclusion, we have $u^3+\omega v^3+\omega^2w^3=0$. □

Corollary 4.2 $\mathbb{F}_4(C)\cong\mathbb{F}_4(D)$.

Proof. Trivially $\mathbb{F}_4(C)=\mathbb{F}_4(x,y)=\mathbb{F}_4(\frac{x}{y+1},\frac{1}{x+y+1})$. On the other hand, by definition of u,v,w (15)

$$\omega^2\frac{v}{u}+\omega\frac{w}{u}=1-\frac{1}{u}.$$

Hence $\mathbb{F}_4(D)\cong\mathbb{F}_4(\frac{v}{u},\frac{w}{u})=\mathbb{F}_4(u,v,w)$. Since

$$\begin{pmatrix}u\\v\\w\end{pmatrix}=\begin{pmatrix}1&1&1\\0&\omega^2&1\\0&\omega&1\end{pmatrix}\begin{pmatrix}1\\\frac{x}{y+1}\\\frac{1}{x+y+1}\end{pmatrix},$$

we know $\mathbb{F}_4(u,v,w)=\mathbb{F}_4(\frac{x}{y+1},\frac{1}{x+y+1})$. Summing up, we get $\mathbb{F}_4(D)\cong\mathbb{F}_4(C)$. □

References

[1] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, in: R. Pellikaan, M. Perret and S. Vlăduţ (Eds.), Arithmetic geometry and coding theory (Luminy, 1993), de Gruyter, Berlin, 1996, 1–7.

[2] J. W. P. Hirschfeld, L. Storme, J. A. Thas and J. F. A. Voloch, *A characterization of Hermitian curves*, J. Geom. 41 (1991) 72–78.

[3] M. Homma and S. J. Kim, *Around Sziklai's conjecture on the number of points of a plane curve over a finite field*, Finite Fields Appl. 15 (2009), 468-474.

[4] M. Homma and S. J. Kim, *Sziklai's conjecture on the number of points of a plane curve over a finite field* II, in: G. McGuire, G.L. Mullen, D. Panario, I.E. Shparlinski (Eds.), Finite Fields: Theory and Applications, 225–234, Contemp. Math., vol. 518, AMS, Providence, 2010. (An update is available at arXiv 0907.1325v2.)

[5] M. Homma and S. J. Kim, *Sziklai's conjecture on the number of points of a plane curve over a finite field* III, Finite Fields Appl. 16 (2010) 315–319.

[6] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. 457 (1994) 185–188.

[7] B. Steinberg, Representation theory of finite groups. An introductory approach, Universitext, Springer, New York, 2012.

[8] P. Sziklai, *A bound on the number of points of a plane curve*, Finite Fields Appl. 14 (2008) 41–43.