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

Research Article

Masaaki Homma

Abstract: An elementary and self-contained argument for the complete determination 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.

2020 MSC: 14G15, 14H50, 14G05, 11G20, 05B25

Keywords: Plane curve, Finite field, Rational point, Maximal curve

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 polynomial $f \in \mathbb{F}_q[x_0, x_1, x_2]$. The set of $\mathbb{F}_q$-points $C(\mathbb{F}_q)$ of $C$ is $\{(a_0, a_1, a_2) \in \mathbb{P}^2 \mid a_0, a_1, a_2 \in \mathbb{F}_q$ 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 $C$ of degree $d$ over $\mathbb{F}_q$,

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

On the other hand, the Sziklai bound established by a series of papers of Kim and the author [5–7] gives one under a more mild condition, that is, for $C$ without $\mathbb{F}_q$-linear components,

$$N_q(C) \leq (d - 1)q + 1 \quad (2)$$

Masaaki Homma; Department of Mathematics, Faculty of Science, Kanagawa University, Yokohama 221-8686, Japan (email: homma@kanagawa-u.ac.jp).
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 the Hasse-Weil bound is better than the Sziklári 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
\[N_q(C) \leq \sqrt{q}^3 + 1 \text{ if } \deg C = \sqrt{q} + 1,\]
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.

More than three decades ago, Hirschfeld, Storme, Thas and Voloch [4] 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). Here we understand a Hermitian curve as a plane curve defined by an equation
\[(x_0^\sqrt{q}, x_1^\sqrt{q}, x_2^\sqrt{q})A \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = 0\]
for a certain matrix $A \in GL(3, \mathbb{F}_q)$ satisfying $tA = A(\sqrt{q})$, where $tA$ denotes the transposed matrix of $A$ and $A(\sqrt{q})$ the matrix taking entry-wise the $\sqrt{q}$-th power of $A$. Note that any two Hermitian curves are projectively equivalent each other over $\mathbb{F}_q$ [3, §7.3].

**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 curve. Actually the plane curve defined by
\[x_0^3 + \omega x_1^3 + \omega^2 x_2^3 = 0\]
is such an example, where $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$.

It would be preferable to give the complete picture of plane curves over $\mathbb{F}_q$ of degree $\sqrt{q} + 1$, without $\mathbb{F}_q$-linear components, having $\sqrt{q}^3 + 1$ $\mathbb{F}_q$-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 $\mathbb{F}_4$.

**Proof.** Thanks to Theorem 1.1, only the missing case for the determination of maximal curves of degree $\sqrt{q} + 1$ is the case of $q = 4$. In this case, $C$ is a cubic curve, which must be nonsingular (see, Lemma 3.2 in Section 3 below). The number of projective equivalent classes of nonsingular cubic curves over $\mathbb{F}_4$ with 9 $\mathbb{F}_4$-points is exactly two, which is given by Schoof [9, Example 5.3].

The second case (ii) in the above theorem should be understood the case of $q = 4$ among Sziklári curves [11] of degree $q - 1$ that achieve the Sziklári bound (2). Here a Sziklári curve means one over $\mathbb{F}_q$, of degree $q - 1$ defined by the following type of equation:
\[\alpha x_0^{q-1} + \beta x_1^{q-1} + \gamma x_2^{q-1} = 0 \text{ with } \alpha \beta \gamma \neq 0 \text{ and } \alpha + \beta + \gamma = 0.\]
The curve (5) will be denoted by $C_{(\alpha, \beta, \gamma)}$, which is obviously nonsingular, in particular has no linear component. Since $x^{q-1} = 1$ for any $x \in \mathbb{F}_q^*$ and $\alpha + \beta + \gamma = 0$,

$$C_{(\alpha, \beta, \gamma)}(\mathbb{F}_q) \supset \mathbb{P}^2(\mathbb{F}_q) \setminus (\cup_{i=0}^2 \{x_i = 0\}).$$  \hspace{1cm} (6)

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

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

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

$$C_{(\alpha, \beta, \gamma)}(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q) \setminus (\{x_0 = 0\} \cup \{x_1 = 0\} \cup \{x_2 = 0\}).$$ \hspace{1cm} (7)

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

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

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

$$C_{(\alpha, \beta, \gamma)}(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q) \setminus (\{x_0 = 0\} \cup \{x_1 = 0\} \cup \{x_2 = 0\}).$$ \hspace{1cm} (7)

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

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

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

is as follows:

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

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

**Remark 1.4.** Since (I-i) $\Leftrightarrow q \equiv 5 \mod 6$, (I-ii) $\Leftrightarrow q \equiv 1 \mod 6$, (II) $\Leftrightarrow q \equiv 3 \mod 6$, (III) $\Leftrightarrow q \equiv 2 \mod 6$, and (III-ii) $\Leftrightarrow q \equiv 4 \mod 6$, we can state Theorem 1.3 more simply that

if $q \neq 2 \mod 6$, then $\nu_q = \lceil \frac{q}{6} \rceil$; and if $q \equiv 2 \mod 6$, then $\nu_q = \lceil \frac{q}{6} \rceil - 1$, where $\lceil \frac{q}{6} \rceil$ denotes the least integer greater than (or equal to) $\frac{q}{6}$.

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 curves of degree $q - 1$.

In Section 3, we will give a self-contained proof of Theorem 1.2 for the case $q = 4$ without using the result of Schoff.

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

\[ \text{129} \]
2. Sziklai's example of maximal curves of degree \( q - 1 \)

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

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

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

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 \( (x^q - 1, y^q - 1) \).

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

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

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

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 \( \deg g_i \leq q - 2 \), \( g_i \) must be the zero polynomial. Hence \( f(x, y) \equiv 0 \mod J \).

**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 \) + \( \beta(\frac{x_1}{x_2})^q - 1 \).
\]

Therefore \( f(x_0, x_1, x_2) = x_2^{q-1}f(\frac{x_0}{x_2}, \frac{x_1}{x_2}, 1) = \alpha(x_0^q - x_1^q) + \beta(x_0^q - x_2^q) \). 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 \( C \in \mathcal{S}_q \).

Now we want to classify \( \mathcal{S}_q \) 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 \( \delta \) a nonnegative integer. An \( \mathbb{F}_q \)-line \( l \) is said to be a \( \delta \)-line with respect to \( C \) if \( |l \cap C(\mathbb{F}_q)| = \delta \).

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

<table>
<thead>
<tr>
<th>( \delta )</th>
<th>the number of ( \delta )-lines</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>q - 2</td>
<td>((q - 1)^2)</td>
</tr>
<tr>
<td>q - 1</td>
<td>(3(q - 1))</td>
</tr>
</tbody>
</table>

**Proof.** Note that \( q > 2 \) because \( \mathcal{S}_q \) is not empty. Since \( \mathbb{P}^2(\mathbb{F}_q) = C(\mathbb{F}_q) \cup \bigcup_{i=0}^{2} \{ x_i = 0 \} \) (where the symbol \( \cup \) indicates disjoint union) and \( q > 2 \), the possible values of \( \delta \) 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. \( \square \)
We need an elementary fact on the finite group action, so called “Burnside’s lemma” [10, Corollary 7.2.9].

**Lemma 2.5.** Let G be a finite group which acts on a finite set X. For g ∈ G, 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

\[ \nu = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|. \]

**Proof of Theorem 1.3.** The first claim is that if two members C(α,β,γ), C(α',β',γ') ∈ S_q are projectively equivalent over \( \mathbb{F}_q \), then the point (α',β',γ') ∈ \( \mathbb{P}^2(\mathbb{F}_q) \) is a permutation of the point (α,β,γ) ∈ \( \mathbb{P}^2(\mathbb{F}_q) \), that is, there is a nonzero element \( \lambda \in \mathbb{F}_q^* \) such that the triple (λα',λβ',λγ') is a permutation of the triple (α,β,γ).

Actually, let \( \Sigma \) be a projective transformation so that \( \Sigma C(α,β,γ) = C(α',β',γ') \). Note that \( \Sigma \) induces an automorphism of the homogeneous coordinate ring \( \mathbb{F}_q[x_0, x_1, x_2] \), which is denoted by \( \Sigma^* \). The set of 0-lines with respect to each of curves in \( S_q \) is \( \{(x_0 = 0), (x_1 = 0), (x_2 = 0)\} \) by Lemma 2.4. Hence \( \Sigma^* \) induces a permutation of those lines. Hence \( \Sigma^*(x_i) = u_i x_{σ(i)} \) for some \( u_i \in \mathbb{F}_q^* \), and \( σ(0), σ(1), σ(2) \) is a permutation of \( (0, 1, 2) \). Hence

\[ \Sigma^*(αx_0^{q-1} + βx_1^{q-1} + γx_2^{q-1}) = αx_0^{q-1} + βx_1^{q-1} + γx_2^{q-1} \]

because \( u_i^{q-1} = 1 \).

So we need to classify \( S_q/\mathbb{F}_q^* \) by the action of \( S_3 \) as permutations on coefficients.

Observe the map

\[ ρ : S_q/\mathbb{F}_q^* ⊆ C(α,β,γ) → (α : β) ∈ \mathbb{P}^1(\mathbb{F}_q), \]

which is well-defined and

\[ \text{Im} \, ρ = \mathbb{P}^1(\mathbb{F}_q) \setminus \{(0,1), (1,0), (1,-1)\}. \]

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

**Table 2.** \( S_3 \)-action on \( \text{Im} \, ρ \)

<table>
<thead>
<tr>
<th>( S_3 )</th>
<th>( S_q/\mathbb{F}_q^* )</th>
<th>( \text{Im} , ρ )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>(α,β,γ)</td>
<td>(α : β)</td>
</tr>
<tr>
<td>(1,2)</td>
<td>(α,β,γ)</td>
<td>(β,α,γ)</td>
</tr>
<tr>
<td>(2,3)</td>
<td>(α,β,γ)</td>
<td>(γ,α,β)</td>
</tr>
<tr>
<td>(1,3)</td>
<td>(α,β,γ)</td>
<td>(γ,β,α)</td>
</tr>
<tr>
<td>(1,2,3)</td>
<td>(α,β,γ)</td>
<td>(β,α,γ)</td>
</tr>
<tr>
<td>(1,3,2)</td>
<td>(α,β,γ)</td>
<td>(β,γ,α)</td>
</tr>
</tbody>
</table>

Now we compute the number of fixed points on \( \text{Im} \, ρ \) by each \( σ \in S_3 \).

- **Fixed points of the identity (1) are all the q − 2 points of \( \text{Im} \, ρ \).**
- \( (α : β) \in \text{Fix}(1,2) \Leftrightarrow (α : β) = (β : α) \Leftrightarrow α^2 - β^2 = 0 \). If the characteristic of \( \mathbb{F}_q \) ≠ 2, then \( \text{Fix}(1,2) = \{(1 : 1)\} \) because \( 1 : -1 \not\in \text{Im} \, ρ \). If q is a power of 2, then \( \text{Fix}(1,2) \) is empty.
- \( (α : β) \in \text{Fix}(2,3) \Leftrightarrow (α : β) = (α : -(α + β)) \Leftrightarrow α = -2β \) because \( α ≠ 0 \). If the characteristic of \( \mathbb{F}_q \) ≠ 2, then \( \text{Fix}(2,3) = \{-2 : 1\} \). If q is a power of 2, then \( \text{Fix}(2,3) \) is empty.
- \( (α : β) \in \text{Fix}(1,3) \Leftrightarrow (α : β) = -(α + β) : β \Leftrightarrow β = -2α \) because \( β ≠ 0 \). If the characteristic of \( \mathbb{F}_q \) ≠ 2, then \( \text{Fix}(1,3) = \{1 : -2\} \). If q is a power of 2, then \( \text{Fix}(1,3) \) is empty.
• \((\alpha : \beta) \in \text{Fix}(1, 2, 3) \iff (\alpha : \beta) = (-\alpha + \beta : \alpha) \iff \alpha^2 + \alpha\beta + \beta^2 = 0 \iff (\alpha : \beta) = (\eta : 1)\) with \(\eta^2 + \eta + 1 = 0\) and \(\eta \in \mathbb{F}_q\).

• \((\alpha : \beta) \in \text{Fix}(1, 3, 2) \iff (\alpha : \beta) = (\beta : -\alpha + \beta) \iff \alpha^2 + \alpha\beta + \beta^2 = 0 \iff (\alpha : \beta) = (\eta : 1)\) 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 \(q \equiv 1 \mod 3\), and only the cubic root of 1 is 1 if \(q\) is a power of 3,

\[
|\text{Fix}(1, 2, 3)| = |\text{Fix}(1, 3, 2)| = \begin{cases} 
2 & \text{if } q \equiv 1 \mod 3 \\
1 & \text{if } q \text{ is a power of 3} \\
0 & \text{else}
\end{cases}
\]

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

\begin{tabular}{c|c|c|c|c|c|c}
\(q \mod 6\) & Fix(1) & Fix(12) & Fix(13) & Fix(23) & Fix(123) & \(6\nu_q\) \\
\hline
5 & \(q - 2\) & 1 & 1 & 1 & 0 & 0 & \(q + 1\) \\
1 & \(q - 2\) & 1 & 1 & 1 & 2 & 2 & \(q + 5\) \\
3 & \(q - 2\) & 1 & 1 & 1 & 1 & 1 & \(q + 3\) \\
2 & \(q - 2\) & 0 & 0 & 0 & 0 & 0 & \(q - 2\) \\
4 & \(q - 2\) & 0 & 0 & 0 & 2 & 2 & \(q + 2\)
\end{tabular}

Since \(\nu_q = \frac{1}{6} \sum_{\sigma \in S_3} |\text{Fix}\,\sigma|\) by Lemma 2.5, we are able to know \(\nu_q\) explicitly as in the last column of Table 3.

At the end of this section, we raise a question: are there non-Sziklai curves over \(\mathbb{F}_q\) of degree \(q - 1\) that attain the Sziklai bound (2)?

**Added in the revision:** Recently, Walteir de Paula Ferreira and Pietro Speziali showed the answer of the above question is negative if \(q \geq 5\) [2].

### 3. Maximal curves of degree 3 over \(\mathbb{F}_4\)

The purpose of this section is to give an elementary and self-contained proof of the following theorem.

**Theorem 3.1.** Let \(C\) be a plane curve of degree 3 over \(\mathbb{F}_4\) without \(\mathbb{F}_4\)-linear components. 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 \(\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}\).

**Lemma 3.2.** Let \(C\) be a plane curve of degree 3 over \(\mathbb{F}_4\) without \(\mathbb{F}_4\)-linear components, and \(N_4(C) \geq 7\). Then \(C\) is nonsingular.

**Proof.** Since the degree of \(C\) is 3, \(C\) is absolutely irreducible. If \(C\) had a singular point, then \(C\) would be an image of \(\mathbb{P}^1\) with exactly one singular point, and hence \(N_4(C)\) would be at most 6 (= \(N_4(\mathbb{P}^1) + 1\)). Therefore \(C\) is nonsingular.

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

**Notation 3.3.** Let $l$ be a line in $\mathbb{P}^2$. The symbol $l.C$ denotes the divisor $\sum_{P \in l \cap C} i(l; C; P)P$ 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.

**Lemma 3.4.** 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 sides 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 coincide with either $P_1$ or $P_2$ because $l$ is a 2-line.

**Lemma 3.5.** Let $l_0$ be a 1-line with respect to $C$, say $l_0 \cap C(\mathbb{F}_4) = \{P\}$. Then $l_0.C = 3P$.

**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

\[ C(\mathbb{F}_4) = \{P\} \sqcup \left( \bigcup_{i=1}^4 (l_i \cap C(\mathbb{F}_4) \setminus \{P\}) \right), \]

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 3.6.** 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 3.7.** 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 3.5.

(ii) This is also a consequence of Lemma 3.5: since $T_P(C)$ is not a 1-line, it should be a 2-line, and the second part is just in Lemma 3.4.

**Notation 3.8.** For each nonnegative integer $\delta \leq 3$, $\mathcal{L}_\delta$ denotes the set of $\delta$-lines with respect to $C$, and $\mu_\delta$ denotes the cardinality of the set $\mathcal{L}_\delta$.

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

**Lemma 3.9.** 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) $\mu_0 = 3$, $\mu_1 = 0$, $\mu_2 = 9$, $\mu_3 = 3$. 


Proof. Step 1. Let us consider the correspondence
\[ \mathcal{F} := \{(l, P) \in \mathbb{P}^2(\mathbb{F}_q) \times C(\mathbb{F}_q) \mid l \ni P\} \]
with projections \( p_1 : \mathcal{F} \to \mathbb{P}^2(\mathbb{F}_q) \) and \( p_2 : \mathcal{F} \to C(\mathbb{F}_q) \), where \( \mathbb{P}^2(\mathbb{F}_q) \) is the projective space of the \( \mathbb{F}_q \)-lines. Since \( |p_2^{-1}(P)| = 5 \) for all \( P \in C(\mathbb{F}_q) \) and \( |C(\mathbb{F}_q)| = 9 \), we know \( |\mathcal{F}| = 45 \).

From Corollary 3.7, 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
\[ \mu_1 + \mu_2 = 9. \] (9)

Since \( |p^{-1}(l)| = \delta \) if \( l \) is a \( \delta \)-line,
\[ \mu_1 + 2\mu_2 + 3\mu_3 = |\mathcal{F}| = 45. \] (10)

Additionally, since the total number of \( \mathbb{F}_q \)-lines is 21,
\[ \mu_0 + \mu_1 + \mu_2 + \mu_3 = 21. \] (11)

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

Step 3. Suppose that \( \mu_1 \neq 0 \). Since (9) and (10), \( \mu_1 \equiv 0 \mod 3 \). Hence there are at least three 1-lines, and hence there are at least three inflection \( \mathbb{F}_q \)-points. Choose two inflection \( \mathbb{F}_q \)-points \( Q_1 \) and \( Q_2 \), and consider the line \( l_0 \) passing through these two points, which is an \( \mathbb{F}_q \)-line. Hence \( l_0 \) meets \( C \) at another point \( Q_0 \), which is also an \( \mathbb{F}_q \)-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 \( 3Q_1 \sim L \) 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. \( \square \)

Hence the following property holds.

(\( \dagger \)) There are exactly three \( \mathbb{F}_q \)-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
\[ C(\mathbb{F}_q) = \{Q_0, Q_1, Q_2\} \cup \{l_i \cap C(\mathbb{F}_q) \setminus \{Q_0\}\} \]
and \( |l_i \cap C(\mathbb{F}_q) \setminus \{Q_0\}| \leq 2 \), each \( l_i \) is a 3-line.

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

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 \( \mathbb{F}_q \)-points if it is defined over \( \mathbb{F}_q \), or at most four \( \mathbb{F}_q \)-points if it is not defined over \( \mathbb{F}_q \) because an \( \mathbb{F}_q \)-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 \( \mathbb{F}_q \), then \( F_4(m) = m' \) and \( D \) has
only one $\mathbb{F}_4$-point; also asserted. 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 $Q_3$ instead of $Q_0$ after (i). 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 $\tau$ such that $Q_2, P_i^{(1)}, P_{\tau(i)}^{(2)}$ are collinear for $i = 1, 2, 3$. Therefore

$$
\begin{align*}
Q_0 + P_1^{(1)} + P_2^{(2)} & \sim L \\
Q_1 + P_1^{(1)} + P_{\sigma(1)}^{(2)} & \sim L \\
Q_2 + P_1^{(1)} + P_{\tau(1)}^{(2)} & \sim L
\end{align*}
$$

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 $Q_0, P_1^{(1)}, P_2^{(2)} = P_{\sigma(1)}^{(2)}, Q_1$ 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.

By this claim,

$$
P_1^{(2)} + P_{\sigma(1)}^{(2)} + P_{\tau(1)}^{(2)} \sim L. \tag{13}
$$

Hence adding all equivalence relations in (12), together with (13) 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 $P_i^{(1)}$ is a flex. Hence $\mu_1 = 9$. Hence, from (9), (10) and (11) in Step 1, $\mu_0 = 0$, $\mu_2 = 0$ and $\mu_3 = 12$.

Remark 3.10. In Step 3 of the proof of Lemma 3.9, 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 [8].

Proof of Theorem 3.1. When the case (ii) in Lemma 3.9 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 $\mathbb{P}^2(\mathbb{F}_4) \setminus \bigcup_{i=0}^2 \{x_i = 0\} = 9 = |C(\mathbb{F}_4)|$, $C \in \mathcal{X}_4$ by Proposition 2.1. Furthermore since $\nu_4 = 1$ by Theorem 1.3 (III-ii), and $C(1, \omega, \omega^2) \in \mathcal{X}_4$, $C$ is projectively equivalent to the curve

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

Next we consider the case (i) in Lemma 3.9. 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 $\delta$-lines. Since $\delta$ is either 1 or 3, $\mu_1(Q) + 3\mu_3(Q) = 9$ and $\mu_1(Q) + \mu_3(Q) = 5$. Hence $\mu_1(Q) = 3$. 

135
Although the proof of [4, Lemma 7] works well under those three assumptions (1), (2), (3) for $C$, we give a proof here for readers’ convenience, which works only in our case $q = 4$.

Let $Q_0 \in \mathbb{P}^2(F_4) \setminus C(F_4)$. From the property (3), there are exactly two 3-lines, say $l_1$ and $l_2$. Since $l_i$ has exactly five $F_4$-points, we can find the fifth $F_4$-point $Q_i$ on $l_i$ other than the three points on $C$ or $Q_0$. Then the $F_4$-line $Q_1Q_2$ is a 3-line. Actually, if the line $Q_1Q_2$ is a 1-line, then it tangents to $C$ at a point, say $R$. However $Q_0R$ also tangents at $R$ by (3), which is impossible. Let’s choose coordinates $x_0, x_1, x_2$ so that $Q_1Q_2$ is defined by $x_0 = 0$, and $l_i$ by $x_i = 0$ for $i = 1, 2$. Then the nine points of $C(F_4)$ is given by

\begin{align*}
(0, 1, 1) & \quad (0, 1, \omega) & \quad (0, 1, \omega^2) \\
(1, 0, 1) & \quad (\omega, 0, 1) & \quad (\omega^2, 0, 1) \\
(1, 1, 0) & \quad (1, \omega, 0) & \quad (1, \omega^2, 0)
\end{align*}

So $C$ is defined by

$$x_0^3 + x_1^3 + x_2^3 + \alpha x_0 x_1 x_2 = 0 \quad (\alpha \in F_4).$$

If $\alpha \neq 0$, the equation gives a union of three lines, which is absurd. \hfill \Box

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 $\mathbb{F}_4$, but not over $\mathbb{F}_2$, 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 [8]. 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{align*}
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{align*}

(14)

satisfy

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

**Proof.** By straightforward computation, we have

\begin{align*}((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)(y + 1) + \omega x(x + y + 1)(y + 1)^2 + (y + 1)^3
\end{align*}
\[(y + 1)(x + y + 1)\omega^3\]
\[= (\omega^2 x + y + 1) + (y + 1)\omega^3\]
\[= x^3(1 + y + 1)^3 + \omega x^2(x + y + 1)(y + 1)^2 + (y + 1)^3 \omega x(x + y + 1)(y + 1)^2 + (y + 1)^3,\]

and
\[
((y + 1)(x + y + 1)\omega^3)^3
= ((y + 1)(x + y + 1) + x(x + y + 1) + (y + 1))^3 = g + h,
\]

where
\[
g = (y + 1)\omega^3(x + y + 1)^3 + (y + 1)^2(x + y + 1)^2(x(x + y + 1) + (y + 1))
+ (y + 1)(x + y + 1)(x(x + y + 1) + (y + 1))^2,
\]
\[
h = (x(x + y + 1) + (y + 1)^3
= x^3(x + y + 1)^3 + x^2(x + y + 1)(y + 1)^2 + x(x + y + 1)(y + 1)^2 + (y + 1)^3.
\]

Hence
\[
\omega^2((y + 1)(x + y + 1)\omega^3)^3 + \omega((y + 1)(x + y + 1)\omega^3)^3 + h
= (\omega^2 + \omega + 1)x^3(x + y + 1)^3
+ (\omega^4 + \omega^2 + 1)x^2(x + y + 1)^2(y + 1)
+ (\omega^3 + \omega^3 + 1)x(x + y + 1)(y + 1)^2
+ (\omega^2 + \omega + 1)(y + 1)^3
= x(x + y + 1)(y + 1)^2.
\]

Therefore
\[
\omega^2((y + 1)(x + y + 1)\omega^3)^3 + \omega((y + 1)(x + y + 1)\omega^3)^3 + ((y + 1)(x + y + 1)\omega^3)^3
= g + x(x + y + 1)(y + 1)^2
= (y + 1)(x + y + 1)^2(x + y + 1)^2 + x(y + 1)(x + y + 1)^2 + (y + 1)^2 + x(y + 1)^2 + x(y + 1)^2 + x(y + 1)^2 + x(y + 1)^2.
\]

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 (15) is equal to
\[
(y + 1)(x + y + 1)^3(\omega^2 w^3 + \omega u^3 + u^3) = (y + 1)(x + y + 1)^2 f,
\]

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:
\[
f = x(y + 1)^2 + (y + 1)^3 + x^2(x + y + 1) + y + 1)^2 + x^3 + x^2(y + 1) + (y + 1)
= (y + 1)^3 + (y + 1)^2 + (y + 1) + x^3
= y^3 + x^3 + 1 = 0.
\]

As a conclusion, we have \(u^3 + \omega u^3 + \omega^2 u^3 = 0\). □
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 $u, v, w$ (14)
\[ \omega^2 \frac{v}{u} + \omega \frac{w}{u} = 1 - \frac{1}{u}. \]
Hence $\mathbb{F}_4(D) \cong \mathbb{F}_4(\frac{u}{v}, \frac{w}{u}) = \mathbb{F}_4(u, v, w)$. 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 $\mathbb{F}_4(D) \cong \mathbb{F}_4(C)$. \hfill \qed

Acknowledgment: The author would like to thank the referee for proposing a simple statement of Theorem 1.3 as in Remark 1.4, and giving information about a recent paper [2].

References