The maximum number of rational points for a genus 4 curve over $\mathbb{F}_7$ is 24

Alessandra Rigato

Abstract

In this paper we show that the maximum number of rational points possible for a smooth, projective, absolutely irreducible genus 4 curve over a finite field $\mathbb{F}_7$ is 24. It is known that a genus 4 curve over $\mathbb{F}_7$ can have at most 25 points. In this paper we prove that such a curve can have at most 24. On the other hand we provide an explicit example of a genus 4 curve over $\mathbb{F}_7$ having 24 points.

1 Introduction

Given a prime power $q$ and a positive integer $g$ it has become an interesting challenge to determine the largest number $N_q(g)$ of rational points possible for a smooth, projective, absolutely irreducible genus $g$ curve over a finite field $\mathbb{F}_q$. Tables are constantly updated at [M]. The main result of this note is the following Theorem.

**Theorem 1.1.** The maximum number of points $N_7(4)$ for a genus 4 curve defined over $\mathbb{F}_7$ is 24. Indeed:

1. Every genus 4 curve defined over $\mathbb{F}_7$ has at most 24 rational points.
2. The projective, smooth, absolutely irreducible curve $C$ defined over $\mathbb{F}_7$ by the set of affine equations

$$
C: \begin{cases}
y^2 = x^3 + 3 \\
z^2 = -x^3 + 3
\end{cases}
$$

is a genus 4 curve having 24 rational points. Its Zeta function is

$$
Z(t) = \frac{(7t^2 + t + 1)(7t^2 + 5t + 1)^3}{(1-7t)(1-t)}.
$$

It is well known that an upper bound for $N_7(4)$ is 25. This follows by Oesterlé’s optimization of Serre’s explicit formula bound [Sch, Theorem 7.3]. The bound of 25 points was also obtained by Ihara [I] and Stöhr-Voloch [S-V, Proposition 3.2]. We show in Section 5 that a genus 4 curve over $\mathbb{F}_7$ with 25 rational points can not exist. This proves the first part of the Theorem. The second part is proved in Section 3.

In Section 2 we present some properties and results on the Zeta function and the real Weil polynomial of a curve, while in Section 4 we introduce some notations and number theoretical results that will be useful for the study of non-Galois function fields extensions arising in Section 5.
2 Zeta function and real Weil polynomial of a curve

Many authors have recently focused on properties of the Zeta function and the real Weil polynomial of a curve in order to improve the bounds for the number of rational points of a curve over a finite field. The Zeta function of a curve $X$ defined over $\mathbb{F}_q$ is given by

$$Z(t) = \prod_{d \geq 1} \frac{1}{(1 - t^d)^{a_d}},$$

where $a_d$ denotes the number of places of degree $d$ of the function field of $X$. In particular $a_1 = \#X(\mathbb{F}_q)$ is the number of rational places. If $X$ has genus $g$, its Zeta function $Z(t)$ is a rational function of the form

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)},$$

where $L(t) = \prod_{i=1}^{g}(1 - \alpha_i t)(1 - \overline{\alpha_i} t)$

for certain $\alpha_i \in \mathbb{C}$ of absolute value $\sqrt{q}$. Therefore the Weil polynomial $L(t) = qg t^{2g} + b_{2g-1} t^{2g-1} + \ldots + b_1 t + 1 \in \mathbb{Z}[t]$ is determined by the coefficients $b_1, \ldots, b_g$ which are in turn determined by the numbers $a_1, \ldots, a_g$ \cite[Section 5.1]{Sti}. To a genus $g$ curve $X$ having $L(t)$ as numerator of its Zeta function, we associate the real Weil polynomial of $X$ defined by

$$h(t) = \prod_{i=1}^{g}(t - \mu_i) \in \mathbb{Z}[t],$$

where $\mu_i = \alpha_i + \overline{\alpha_i}$ is a real number in the interval $[-2\sqrt{q}, 2\sqrt{q}]$, for all $i = 1, \ldots, g$. We have $L(t) = t^g h/qt + 1/t)$. Moreover we denote by $a(X) = [a_1, a_2, \ldots, a_d, \ldots]$ the vector whose $d$-th entry displays the number $a_d = a_d(X)$ of places of degree $d$ of the function field of $X$. Not every polynomial $h(t)$ with all zeros in the interval $[-2\sqrt{q}, 2\sqrt{q}]$ and with the property that

$$\frac{L(t)}{(1-t)(1-qt)} = \prod_{d \geq 1} \frac{1}{(1 - t^d)^{a_d}}$$

for certain integers $a_d \geq 0$ is necessarily the real Weil polynomial of a curve. The following result is due to Serre \cite[page 11]{Ser}, \cite[Lemma 1]{L}.

**Proposition 2.1.** Let $h(t)$ be the real Weil polynomial of a curve $X$ over $\mathbb{F}_q$. Then $h(t)$ cannot be factored as $h(t) = h_1(t)h_2(t)$, with $h_1(t)$ and $h_2(t)$ non-constant polynomials in $\mathbb{Z}[t]$ such that the resultant of $h_1(t)$ and $h_2(t)$ is $\pm 1$.

Generalizations of this result are due to E. Howe and K. Lauter, for example \cite[Theorem 1, Proposition 13]{HL}.

**Proposition 2.2.** Let $h(t) = (t - \mu)h_2(t)$ be the real Weil polynomial of a curve $X$ over $\mathbb{F}_q$, where $t - \mu$ is the real Weil polynomial of an elliptic curve $E$ and $h_2(t)$ a non-constant polynomial in $\mathbb{Z}[t]$ coprime with $t - \mu$. If $r \neq \pm 1$ is the resultant of $t - \mu$ and the radical of $h_2(t)$, then there is a map from $X$ to an elliptic curve isogenous to $E$, of degree dividing $r$. 
3 An explicit example of a genus 4 curve having 24 points over $\mathbb{F}_7$

In this section we prove that the curve $C$ defined by the set of affine equations (1) is a genus 4 curve having 24 rational points over $\mathbb{F}_7$.

**Proof of Theorem 1.1 part 2.** The function field of the smooth projective curve $C$ is $\mathbb{F}_7(x, y, z)$, where $x$, $y$ and $z$ are defined by the set of equations (1). This is a Galois extension of the rational function field $\mathbb{F}_7(x)$ of Galois group $G$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The three quadratic subfields are:

1. $\mathbb{F}_7(x, y)$ the function field of the curve of affine equation
   \[
   \tilde{E} : y^2 = x^3 + 3. \quad (2)
   \]
   This is a genus 1 curve with 13 rational points over $\mathbb{F}_7$. The Weil polynomial is $7t^2 + 5t + 1$.

2. $\mathbb{F}_7(x, z)$ the function field of the curve of affine equation $z^2 = -x^3 + 3$, which is isomorphic to $\tilde{E}$ and has hence the same Weil polynomial.

3. $\mathbb{F}_7(x, w)$, where $w = xy$ and hence $w^2 = (x^3 + 3)(-x^3 + 3) = -x^6 + 2$. This is an affine equation of a smooth projective curve of genus 2. One checks that for each $x \in \mathbb{F}_7$ there are two rational points. Thus in total 14 rational points, since the place at infinity has degree 2. A small computation gives that there are 19 places of degree 2, thus the Weil polynomial is $(7t^2 + t + 1)(7t^2 + 5t + 1)$.

Since $G$ is abelian we can compute the Zeta function $Z_C(t)$ of $C$ by means of the following [Ro, Proposition 14.9]

\[
Z_C(t) = \prod_{\chi \in \hat{G}} L(t, \chi),
\]

where $\hat{G}$ denotes the group of characters $\chi : G \to \{\pm 1\}$. For the non-trivial characters $\chi$, the $L$-function $L(t, \chi) = \prod_P (1 - \chi(P)t^{deg P})^{-1}$ is precisely the Weil polynomial $L(t)$ of the curve corresponding to the quadratic function field fixed by $\ker(\chi)$. The $L$-function of the trivial character is the Zeta function of $\mathbb{P}^1$. Thus the Weil polynomial of $C$ equals the product

\[
(7t^2 + t + 1)(7t^2 + 5t + 1)^3 = 7^4t^8 + \ldots + 118t^2 + 16t + 1, \quad a(C) = [24, 3, 120, 558, \ldots]
\]

of the Weil polynomials of the quadratic function fields described above. From this it follows that the genus of $C$ is 4 and that the number of rational points equals 24.

**Remark 3.1.** The elliptic curve $\tilde{E}$ defined by (2) is the unique genus 1 optimal curve over $\mathbb{F}_7$. Indeed, an optimal elliptic curve over $\mathbb{F}_7$ has Frobenius polynomial $t^2 + 5t + 7$. Hence, the discriminant is $-3$ and the curve admits an automorphism of order 3. Therefore its Weierstrass equation is $y^2 = x^3 + b$ for some $b \in \mathbb{F}_7^\times$ [Sil, Theorem 10.1]. Only for $b = 3$ one has a projective curve attaining the Hasse-Weil bound $q + 1 + g\sqrt{2q}$ of 13 rational points.
4 Non-Galois extensions of degree 3

In this section we introduce some notation and adapt some results of [Ri] to the examples in this paper. Let $E$ be an elliptic curve defined over $\mathbb{F}_q$ and let $X$ be a genus $g$ curve over $\mathbb{F}_q$. Let $X \rightarrow E$ be a morphism of degree 3 such that the induced function field extension $\mathbb{F}_q(X)/\mathbb{F}_q(E)$ is non-Galois.

**Definition 4.1.** We denote by $X$ the curve whose function field is the normal closure of $\mathbb{F}_q(X)$ with respect to $\mathbb{F}_q(E)$: it is a Galois extension of $\mathbb{F}_q(E)$ having Galois group isomorphic to the symmetric group $S_3$. We denote by $X'$ the curve having as function field the quadratic extension of $\mathbb{F}_q(E)$ corresponding to the group $A_3 \cong \mathbb{Z}_3$, the unique (normal) subgroup of $S_3$ of index 2. The situation is described in the following picture:

\begin{center}
\begin{tikzpicture}
  \node (X) at (0,0) {$X$};
  \node (Y) at (-1,-1) {$Y$};
  \node (Z) at (1,-1) {$Z$};
  \node (Xp) at (2,0) {$X'$};
  \node (E) at (0,-2) {$E$};
  \node (Z2) at (1,-3) {$Z_2$};
  \node (Z3) at (3,-2) {$Z_3$};
  \node (G) at (3,-4) {$G$};
  \draw[->] (X) to (Y);
  \draw[->] (X) to (Z);
  \draw[->] (X) to (E);
  \draw[->] (X) to (Xp);
  \draw[->] (Y) to (E);
  \draw[->] (Z) to (E);
  \draw[->] (E) to (Z2);
  \draw[->] (E) to (Z3);
  \draw[->] (Xp) to (Z2);
  \draw[->] (Xp) to (Z3);
  \draw[->] (Xp) to (G);
  \draw[->] (G) to (Z2);
  \draw[->] (G) to (Z3);
  \node at (0,-1.5) {$2$};
  \node at (-1,-2.5) {$2$};
  \node at (1,-2.5) {$2$};
  \node at (2,-1.5) {$3$};
  \node at (-2,-1.5) {$3$};
  \node at (-1,-3.5) {$3$};
  \node at (1,-3.5) {$3$};
  \node at (2,-3.5) {$3$};
  \node at (3,-2.5) {$2$};
  \node at (0,-4.5) {$\{1\}$};
\end{tikzpicture}
\end{center}

In the rest of the note we will make often use of the following notation:

**Definition 4.2.** Consider a rational place $P$ of $\mathbb{F}_q(E)$. We say that $P$ is
a) an $A$-point of $E$, if $P$ splits completely in $\mathbb{F}_q(X)$;
b) a $B$-point of $E$, if $P$ splits into two rational places of $\mathbb{F}_q(X)$, one unramified and the other one with ramification index 2;
c) a $B'$-point of $E$, if $P$ splits into two places of $\mathbb{F}_q(X)$, one rational and the other one of degree 2;
d) a $C$-point of $E$, if $P$ is totally ramified in $\mathbb{F}_q(X)$ with ramification index 3;
e) a $C'$-point of $E$, if $P$ is inert in $\mathbb{F}_q(X)$ of degree 3;

Moreover we denote by $a$, $b$, $b'$, $c$, $c'$ the number of $A$-points, $B$-points, $B'$-points, $C$-points and $C'$-points of $E$ respectively.

Here’s an auxiliary lemma.

**Lemma 4.3.** Let $q \equiv 1 \mod 3$ be a power of a prime $p \neq 2$. Then the local field $\mathbb{F}_q((t))$ does not admit an extension $K$ of Galois group $G = \text{Gal}(K/\mathbb{F}_q((t)))$ isomorphic to the symmetric group $S_3$.

**Proof.** We refer the reader to [S2] Chapter 4 §1 for notations and results on local fields and their ramification groups. Suppose such an extension $K$ exists. Let $G_0$ be the inertia subgroup of $G$. Since $G_0$ is normal in $G$, one identifies the quotient
$G/G_0$ with $\text{Gal}(K'/\mathbb{F}_q((t)))$, where $K'$ is the largest unramified subextension of $K$ over $\mathbb{F}_q((t))$. We have thus the following exact sequence

$$1 \to \text{Gal}(K/K') \to \text{Gal}(K/\mathbb{F}_q((t))) \to \text{Gal}(K'/\mathbb{F}_q((t))) \to 1.$$ 

The quotient group $G/G_0$ is isomorphic to the Galois group of the residue field extensions. So it is cyclic. Therefore the field $K$ is ramified over $\mathbb{F}_q((t))$. Moreover $K$ cannot be totally ramified, because being tamely ramified, such an extension would be cyclic. Hence the inertia group is isomorphic to $\mathbb{Z}_3$ the unique normal subgroup of $S_3$. Thus $G$ is a semidirect product of $\mathbb{Z}_3$ and $\mathbb{Z}_2$:

$$G = \langle \sigma, \tau : \sigma^2 = 1, \tau^3 = 1, \sigma\tau\sigma^{-1} = \tau^q \rangle,$$

where $\tau$ is a generator of $\text{Gal}(K/K')$ and $\sigma$ a lift of Frobenius of order 2 generating $\text{Gal}(K'/\mathbb{F}_q((t)))$. Now the order of $\tau$ is 3 and $q \equiv 1 \mod 3$, hence $G$ is abelian. But this is a contradiction.

Assume that the field of definition of the curve $\overline{X}$ is $\mathbb{F}_q$, then the following holds:

Lemma 4.4.

a) The $A$-points of $E$ split completely in $\mathbb{F}_q(\overline{X})$ and in $\mathbb{F}_q(X')$.

b) The $B$-points of $E$ split in $\mathbb{F}_q(\overline{X})$ into three rational places having ramification index 2, while they are ramified in $\mathbb{F}_q(X')$.

c) The $B'$-points of $E$ split in $\mathbb{F}_q(\overline{X})$ into three rational places having relative degree 2, while they are inert of degree 2 in $\mathbb{F}_q(X')$.

d) The $C$-points of $E$ are not totally ramified in $\mathbb{F}_q(\overline{X})$. Moreover, if $q \equiv 1 \mod 3$, they split in $\mathbb{F}_q(\overline{X})$ into two rational places having ramification index 3, while they split in $\mathbb{F}_q(X')$ into two unramified rational places.

e) The $C'$-points of $E$ split in $\mathbb{F}_q(\overline{X})$ into two places having relative degree 3, while they split into two rational places in $\mathbb{F}_q(X')$.

Proof.

a) The rational places of $\mathbb{F}_q(E)$ splitting completely in $\mathbb{F}_q(X)$ split completely in the isomorphic function field $\mathbb{F}_q(Y)$ as well. Hence they split completely in the compositum $\mathbb{F}_q(\overline{X})$ and thus in the function field of $X'$ too.

b) Let $P$ be a $B$-point of $E$. Then the number of places of $\mathbb{F}_q(\overline{X})$ lying over the place $P$ of $\mathbb{F}_q(E)$ must be greater than or equal to 2 and divide 6. Moreover each of them must have (the same) ramification index $e \geq 2$ and dividing 6 since the extension is Galois.

c) The reasoning is analogous to the one above for the $B$-points.

5
d) The rational places of $\mathbb{F}_q(E)$ that are totally ramified in $\mathbb{F}_q(X)$ are also totally ramified in the isomorphic function field $\mathbb{F}_q(Y)$. Since $\text{char} \mathbb{F}_q \neq 3$ the ramification is tame, thus they are ramified in the compositum $\mathbb{F}_q(X)$ with the same ramification index. Hence a place $Q$ of $\mathbb{F}_q(X)$, lying over $P$ has ramification index 3. Moreover, suppose $q \equiv 1 \mod 3$. The degree of $Q$ can be either 2 or 1. Lemma 4.3 shows that the first case is impossible. In the latter case, there exists another rational place $Q'$ lying over $P$ and having ramification index 3.

This concludes the proof.

e) Let $P$ be a rational place of $\mathbb{F}_q(E)$ inert of relative degree 3 in $\mathbb{F}_q(X)$. Since $P$ is not ramified neither in $\mathbb{F}_q(X)$ nor in the isomorphic function field $\mathbb{F}_q(Y)$, the place $P$ is not ramified in the compositum $\mathbb{F}_q(X)$. Since $P$ unramified, its decomposition group must be cyclic. Hence it must have order 3. So there are two places of relative degree 3 of $\mathbb{F}_q(X)$ over $P$ and hence two rational places of $\mathbb{F}_q(X')$ over $P$.

Remark 4.5. In the case of the $B'$-points and the $C$-points the arguments used do not depend on the fact that these ramifying places are rational. Hence the same results hold for higher degree places.

5 Non-existence of a genus 4 curve with 25 points over $\mathbb{F}_7$

Let $X$ be a genus 4 curve having 25 rational points over $\mathbb{F}_7$. In this section we prove that such a curve $X$ can not exist.

Proposition 5.1. The function field $\mathbb{F}_7(X)$ of $X$ is a degree 3 extension of the function field $\mathbb{F}_7(E)$ of an elliptic curve $E$ having 10 rational points over $\mathbb{F}_7$.

Proof. We can compute a list of monic degree 4 polynomials $h(t) \in \mathbb{Z}[t]$ for which $a_1 = 25$, $a_d \geq 0$ for $d \geq 2$ in the relation described in Section 2. Moreover we require that $h(t)$ has all zeros in the interval $[-2\sqrt{7}, 2\sqrt{7}]$ and that the conditions of Proposition 2.1 are satisfied. A short computer calculation gives that if a genus 4 curve $X$ having 25 rational points over $\mathbb{F}_7$ exists there is a unique possibility for its real Weil polynomial, namely

$$h(t) = (t + 2)(t + 5)^3 \quad \text{with} \quad a(X) = [25, 1, 115, 576, \ldots].$$

Since the resultant of $t + 2$ and $t + 5$ is 3, Proposition 2.2 applies. Notice that $t + 2$ is the real Weil polynomial of a genus 1 curve with 10 rational points over $\mathbb{F}_7$.

Let $\mathbb{F}_7(X)/\mathbb{F}_7(E)$ be as in Proposition 5.1.

Lemma 5.2. The degree 3 function field extension $\mathbb{F}_7(X)/\mathbb{F}_7(E)$ is not Galois.

Proof. Suppose that $\mathbb{F}_7(X)/\mathbb{F}_7(E)$ is Galois. Since $E$ has 10 rational points and $X$ has 25, the only possibility for the splitting behavior of the rational places of $\mathbb{F}_7(E)$ is that eight places split completely in $\mathbb{F}_7(X)$, one place $P$ is (tamely) totally ramified.
and one place $T$ is inert, i.e. it gives rise to a place of degree 3 in $\mathbb{F}_7(X)$. Moreover, by the Hurwitz genus formula the degree of the different $D$ of $\mathbb{F}_7(X)/\mathbb{F}_7(E)$ is $2 \cdot 4 - 2 = 6$. Hence we can only have that $D = 2P + 2Q$, where $Q$ is a place of $\mathbb{F}_7(E)$ of degree 2. The function field of $X$ is hence a subfield of the ray class field of $\mathbb{F}_7(E)$ of conductor $P + Q$, where all rational places in $E(\mathbb{F}_7) \setminus \{P, T\}$ split completely. By translation we can always assume that $P$ equals the point at infinity of $E$ and using the elliptic involution we can let $T$ vary among only half of $E(\mathbb{F}_7) \setminus \{P\}$. Up to isomorphism there are two elliptic curves over $\mathbb{F}_7$ with 10 rational points. They have affine equations $y^2 = x^3 + x + 4$ and $y^2 = x^3 + 3x + 4$. A short MAGMA computation allows to conclude that this ray class field is trivial for both curves $E$. See the appendix for the MAGMA code.

Since the extension $\mathbb{F}_7(X)/\mathbb{F}_7(E)$ is non-Galois, we may apply Lemma 4.4. In the following Lemma we present the possibilities for the numbers $a$, $b$, . . . of $A$-points, $B$-points, . . . of $E$. Moreover we consider the curve $X$ whose function field is the Galois closure of $\mathbb{F}_7(X)$ with respect to $\mathbb{F}_7(E)$. We compute its number $N$ of rational points and its genus $g$ in each case.

**Lemma 5.3.** There are five possibilities for the splitting behavior of the rational places of $\mathbb{F}_7(E)$ in $\mathbb{F}_7(X)$. The curve $X$ is defined over $\mathbb{F}_7$ in any of these cases. Its genus $\gamma$ and its number $N$ of rational points are displayed in Table 1.

| case | $a$ | $b$ | $b'$ | $c$ | $c'$ | $N$ | $g$ |
|------|-----|-----|------|-----|------|-----|-----|
| I    | 8   | 0   | 1    | 0   | 1    | 48  | 10  |
| II   | 8   | 0   | 0    | 1   | 1    | 50  | 7 or 9 |
| III  | 7   | 2   | 0    | 0   | 1    | 48  | 8 or 10 |
| IV   | 7   | 1   | 1    | 1   | 0    | 47  | 9   |
| V    | 6   | 3   | 1    | 0   | 0    | 45  | 10  |

Table 1: Splitting behavior of the rational places of $\mathbb{F}_7(E)$ in $\mathbb{F}_7(X)$

**Proof.** The curve $X$ has 25 rational points over $\mathbb{F}_7$, while the curve $E$ has 10. Hence by Lemma 4.4 we have that the numbers $a$, $b$, . . . of $A$-points, $B$-points, . . . of $E$ must satisfy:

\[
\begin{align*}
3a + 2b + b' + c &= 25 \\
a + b + b' + c + c' &= 10
\end{align*}
\]

(4)

The different $D$ of the function field extension $\mathbb{F}_7(X)/\mathbb{F}_7(E)$ has degree 6 by the Hurwitz formula. Moreover the contribution of all ramifying rational points can not be exactly 5. Hence we also have that

\[
\begin{align*}
b + 2c &\leq 6 \\
b + 2c &\neq 5
\end{align*}
\]

(5)

The values of $a$, $b$, . . . that satisfy both (4) and (5) are those displayed in Table 1 plus the values $(a, b, b', c, c') = (7, 1, 2, 0, 0)$. But this case can never occur: $b' = 2$.
implies that $F_7(X)$ has at least two places of degree 2. Which contradicts the fact that $a_2(X) = 1$ as in [4]. We remark that $X$ is indeed defined over $F_7$ since in any case the number $a$ of $A$-points of $E$ in non-zero (the full constant field of the function field of $X$ is always contained in the residue fields of its places). The number $N$ of $F_7$-rational points of $X$ is 6 $a + 3b + 2c$ by Lemma 4.4. The genus $\overline{g}$ of $X$ is computed by means of the Hurwitz formula $2\overline{g} - 2 = \deg \overline{D}$, where $\overline{D}$ is the different of the function field extension $F_7(X)/F_7(E)$. We determine the degree of the divisor $\overline{D}$ as follows.

The ramifying rational places of $F_7(E)$ give a contribution of $b + 2c$ to the degree of the different $\overline{D}$. Since $a_2(X) = 1$, there can be at most one degree 2 place of $F_7(E)$ that (totally) ramifies in $F_7(X)$. If there is such a ramified place, than $b' = 0$: by Lemma 4.4 and Remark 4.5, the degree of $\overline{D}$ is 12 in case $II$ and 14 in case $III$. Thus we have $\overline{g} = 7$ and $\overline{g} = 8$ respectively. In case there is no such a ramifying place, there always exists a unique place of $F_7(E)$ of degree $6 - (b + 2c)$ splitting in $F_7(X)$ into two places of the same degree, one having ramification index 2 and one unramified. In case $I$ there is moreover the possibility that two places of $F_7(E)$ of degree $(6 - (b + 2c))/2 = 3$ appear in the support of $\overline{D}$, each of them splitting in $F_7(X)$ into two places of the same degree, one having ramification index 2 and one unramified. By Lemma 4.4 and Remark 4.5, the degree of $\overline{D}$ is 18 for both possibilities in case $I$ and thus $\overline{g} = 10$. The degree of $\overline{D}$ is 16 in cases $II$ and $IV$ and it is 18 in cases $III$ and $V$, giving $\overline{g} = 9$ and $\overline{g} = 10$ respectively.

Lemma 5.4. The does not exist a curve $\overline{X}$ with genus $\overline{g}$ and number $\overline{N}$ of $F_7$-rational points as displayed in Table 1.

Proof. By the Oesterlé bound [Sch, Theorem 7.3] a curve having 48 (resp. 45) rational points over $F_7$ must have genus at least 11 (resp. 10). Hence in the first four cases the curve $\overline{X}$ can not exist because it has too many points for its genus. In case $V$ the curve $\overline{X}$ has exactly 45 rational points. Moreover, since $b' = 1$, the curve $\overline{X}$ has at least three places of degree 2 by Lemma 4.4. We search for the real Weil polynomial $h(t)$ of such a curve. See Section 4.4 for the relation between $h(t)$ and the coefficients $a_d$ of the Zeta function of $\overline{X}$. We compute a list of monic degree 4 polynomials $h(t)$ with integer coefficients for which $a_1 = 25$, $a_2 \geq 3$ and $a_d \geq 0$ for $d \geq 3$. Moreover we require that $h(t)$ has all zeros in the interval $[−2\sqrt{7}, 2\sqrt{7}]$. A short computer calculation gives that there is only one such a polynomial, namely

$$h(t) = (t + 3)^3(t + 4)^7 \quad \text{with} \quad a(\overline{X}) = [45, 3, 17, 807, \ldots].$$

But since the resultant of $t + 3$ and $t + 4$ is 1, we have a contradiction by Proposition 2.1 and hence also in this case the curve $\overline{X}$ does not exist.

Summing up these results we prove the first part of the Theorem.

Proof of Theorem 1.1 part 1. Let $X$ denote a genus 4 curve over $F_7$. We pointed out in the Introduction that an upper bound for the number of rational points of $X$ is 25. If a curve $X$ with 25 rational points exists, then Proposition 5.4 implies that it is a degree 3 covering of an elliptic curve $E$ with 10 rational points. On the other hand,
Lemmas 5.2, 5.3, and 5.4 show that the curve $\overline{X}$ and hence the curve $X$ cannot exist. This proves that every genus 4 curve over $\mathbb{F}_7$ has at most 24 rational points.

6 Appendix

We list here the MAGMA code used for the ray class field computation in Lemma 5.2.

```magma
kx<x> := FunctionField(GF(7));
kxy<y> := PolynomialRing(kx);
E:=FunctionField(y^2-x^3-x-4);
// alternatively E:=FunctionField(y^2-x^3-3*x-4);
Genus(E);
P:=Places(E,1);
print "Rational places of E: ",P;
Q:=Places(E,2); #Q;
for i in {2, 4, 5, 8, 9} do
  // this sets the rational place T to be (x,y+2), (x+5,y),
  // (x+3,y+x), (x+2,y+1)
  for j:=1 to #Q do
    D:=1*P[1]+1*Q[j];
    // P[1] is the place at infinity
    S:=[2,3,4,5,6,7,8,9,10] diff {i};
    // set of splitting places
    R, mR := RayClassGroup(D);
    U := sub<R | [P[1]@@mR : x in S]>;
    if not (#quo<R|U> eq 1) then
      print "********************************************************
      quo<R|U>;
      C := FunctionField(AbelianExtension(D, U)); C;
      print "Genus", Genus(C);
      print "Number of places a(C)=[",#Places(C, 1),",",#Places(C, 2),
      ",",#Places(C, 3),",",#Places(C, 4),"]";
      print "Degree 2 place of E ramifying is Q=", Q[j];
      print "Inert place of E is T=", P[i];
    end if; end for; end for;
```

References

[H-L] E. Howe and K. Lauter, Improved upper bounds for the number of points on curves over finite fields, Ann. Inst. Fourier 53 (2003), 1677–1737.

[I] Y. Ihara Some remarks on the number of rational points of algebraic curves, J. Fac. Sci. Univ. Tokyo, IA 28 (1982), 721–724.
[L] K. Lauter, *Ray class field constructions of curves over finite fields with many rational points*, Algorithmic Number Theory, H. Cohen (ed.), Lecture Notes in Comput. Sci. **1122**, Springer, (1996), 187–195.

[M] manyPoints – *Table of Curves with Many Points*, continuously updated at http://www.manypoints.org/.

[Ri] A. Rigato, *Uniqueness of low genus optimal curves over \( \mathbb{F}_2 \)*, to appear in Proceedings of AGTC and Geocrypt 2009, Contemporary Mathematics book series of the American Mathematical Society.

[Ro] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, 2002.

[Sch] R. Schoof, *Algebraic curves and coding theory*, UTM 336, Univ. of Trento, 1990.

[S1] J.-P. Serre, *Rational points on curves over finite fields*, unpublished notes by Fernando Q. Gouvêa of lectures at Harvard University, 1985.

[S2] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979.

[Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 2008.

[S-V] K.-O. Stöhr and J.F. Voloch *Weierstrass points and curves over finite fields*, Proc. London. Math. Soc. **52** (1986), 1–19.

**Alessandra Rigato**
K.U. Leuven, Department of Mathematics, Celestijnenlaan 200 B, B-3001 Leuven (Heverlee), Belgium
Alessandra.Rigato@wis.kuleuven.be