FURTHER RESULTS ON FIBRE PRODUCTS OF KUMMER COVERS AND CURVES WITH MANY POINTS OVER FINITE FIELDS

FERRUH ÖZBUDAK
Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University
Dumlupınar Bulvarı, 06800, Ankara, Turkey

BURCU GÜLMEZ TEMÜR*
Department of Mathematics
Atılım University
İncek, Gölbaz, 06836, Ankara, Turkey

OĞUZ YAYLA
Department of Mathematics
Hacettepe University
Beytepe, 06800, Ankara, Turkey

(Communicated by Gerhard Frey)

Abstract. We study fibre products of an arbitrary number of Kummer covers of the projective line over \( \mathbb{F}_q \) under suitable weak assumptions. If \( q-1 = r^a \) for some prime \( r \), then we completely determine the number of rational points over a rational point of the projective line. Using this result we obtain explicit examples of fibre products of three Kummer covers supplying new entries for the current table of curves with many points (http://www.manypoints.org, October 31 2015).

1. Introduction

Let \( \mathbb{F}_q \) be a finite field with \( q = p^n \) elements, where \( p \) is a prime number. Let \( \chi \) be an absolutely irreducible, nonsingular and projective curve defined over \( \mathbb{F}_q \), \( N \) be the number of \( \mathbb{F}_q \)-rational points of \( \chi \) and \( g(\chi) \) be its genus. It is well known that the number \( N \) is bounded by the Hasse-Weil bound

\[
N \leq q + 1 + 2g(\chi)\sqrt{q}.
\]

If the bound in (1) is attained then \( \chi \) is called a maximal curve. For some improvements in the literature especially when \( g(\chi) \) is large we refer to [3, 4, 7, 11, 12].

Let \( N_q(g) \) denote the maximum number of \( \mathbb{F}_q \)-rational points among the absolutely irreducible, nonsingular and projective curves of genus \( g \) defined over \( \mathbb{F}_q \). Determining the number \( N_q(g) \) and constructing explicit curves with many rational points (see [2], and [13] for the current tables) is important since there are

2010 Mathematics Subject Classification: Primary: 11G20, 14G15; Secondary: 14H25.

Key words and phrases: Curves with many points over finite fields, Kummer covers, fibre products, rational points, algebraic function fields.

*Corresponding author.
many applications of such curves in current research areas such as coding theory, cryptography and quasi-random points etc. (see [4, 7, 8, 11, 12]).

In the literature using certain types of fibre products of Kummer covers of the projective line, explicit curves with many points were found (see [1, 6, 9, 10]). It is also well known that the theory of algebraic curves is essentially equivalent to the theory of algebraic function fields, we will use the terminology of function fields [11] and call a degree one place of an algebraic function field as a rational place of the function field throughout this paper.

In particular in [10] we studied the general fibre products of a finite number of Kummer covers of the projective line. More precisely we considered the following fibre product

\begin{align*}
y_1^{n_1} &= h_1(x), \\
y_2^{n_2} &= h_2(x), \\
&\vdots \\
y_k^{n_k} &= h_k(x).
\end{align*}

where \( k \geq 2 \) and \( n_1, n_2, \ldots, n_k \geq 2 \) are integers, \( h_1(x), h_2(x), \ldots, h_k(x) \in \mathbb{F}_q(x) \), \( E = \mathbb{F}_q(x, y_1, y_2, \ldots, y_k) \) is the algebraic function field with the system of equations in (2). We assumed that \( [E : \mathbb{F}_q(x)] = n_1 n_2 \ldots n_k \) and that the full constant field of \( E \) is \( \mathbb{F}_q \). We determined the number of rational places of \( E \) over \( P \) (where \( P \) is a rational place of the rational function field \( \mathbb{F}_q(x) \)) exactly for an arbitrary \( k \geq 2 \) under some strong conditions [10, Theorems 2 and 3]. Moreover, in [10] we determined the number of rational places of \( E \) over \( P \) when \( k = 2 \) exactly under a weak condition [10, Theorem 4].

In this paper we determine the number of rational places of \( E \) over \( P \) for an arbitrary positive integer \( k \geq 3 \) under the joint condition \( m_2 | q - 1, m_3 | q - 1, \ldots, m_k | q - 1 \). Note that this joint condition is independent from the order (see [10, Remark 2]). The problem seems to be much more challenging for an arbitrary \( q \). Therefore, in this paper we study the case \( q - 1 = r^a \) for some prime \( r \) (see Remark 1 below).

As in the proof of [10, Theorem 4] we determine the number of rational places of \( E \) over \( P \) using suitable intermediate field extensions of \( \mathbb{F}_q(x) \subseteq E \) depending on \( P \). The main difficulty is to determine the ratios of the number of rational extensions to the number of non-rational extensions in some intermediate field extensions for certain rational places having ramification index 1.

By a detailed study of such intermediate field extensions we observe an important connection to a system of linear equations over the ring \( \mathbb{Z}_{q-1} \) (see Equation 6 in the proof of Lemma). The form of this system of linear equations is determined by the equations of \( E \) in (2) and the place \( P \) as explained in Sections 2 and 3.

We determine the number of rational places of \( E \) over \( P \) completely for arbitrary \( k \geq 3 \) under the condition that \( q - 1 = r^a \) for some prime \( r \) using local \( r \)-adic techniques. These techniques are new in application to this problem in the sense that they were not used for example in [10]. Therefore we obtain the condition C2 in the statement of Theorem 3.1 depending on some inequalities, which correspond to some \( r \)-adic valuations. A generalization of the methods of [10] do not extend from \( k = 2 \) to arbitrary \( k \geq 3 \). In particular even for \( k = 2 \) the conditions in [10, Theorem 4] are very complicated.
Remark 1. We explain what the condition

\[(3) \quad q - 1 = r^a, \quad \text{for some prime } r\]

means in this remark. We refer to, for example, [5, Chapter IX, Lemma 2.7] for details. The condition in (3) holds such that \(\mathbb{F}_q\) is a finite field of characteristic \(p\) with \(q = p^n\) if and only if one of the following cases hold:

i) \(p = 2, n\) is a prime, \(a = 1\) and \(r\) is a Mersenne prime.

ii) \(n = 1, a = 2^m, r = 2\) and \(q = p = 2^{2^m} + 1\) is a Fermat prime.

iii) \(q = 9, p = 3, n = 2, r = 2, a = 3\).

Hence the list of \(q\) satisfying the condition in (3) such that \(q \leq 100\) and \(\mathbb{F}_q\) is a finite field is \(\{3, 4, 5, 8, 9, 17, 32\}\).

The paper is organized as follows. In Section 2 we give the notation. Then we present our main result in Section 3, and give some examples in Section 4.

2. Preliminaries

For an algebraic function field \(F\) with a separating element \(x \in F\) and full constant field \(F_q\), if \(z \in F\) and \(P\) is a rational place of \(F\), then we denote the evaluation of \(z\) at \(P\) by \(\text{Ev}_P(z)\). For an arbitrary \(u \in F_q\), we denote the rational place of the rational function field \(F_q(x)\) corresponding to the zero of \((x - u)\) as \(P_u\). Similarly the rational place corresponding to the pole of \(x\) is denoted as \(P_{\infty}\).

For \(1 \leq i \leq k\), the evaluation of \(f_i(x) \in F_q(x)\) at \(P_u\) is denoted also by \(f_i(u)\). We denote the multiplicative group \(\mathbb{F}_q \setminus \{0\}\) by \(\mathbb{F}_q^*\).

We consider the fibre product

\[(4) \quad y_1^{n_1} = h_1(x), \quad y_2^{n_2} = h_2(x), \quad \ldots, \quad y_k^{n_k} = h_k(x).\]

Let \(E\) be the algebraic function field \(E = \mathbb{F}_q(x, y_1, y_2, \ldots, y_k)\) with the system of equations in (4).

For \(1 \leq i \leq k\) and \(h_i(x) \in \mathbb{F}_q(x)\), let \(a_i \in \mathbb{Z}\) and \(f_i(x) \in \mathbb{F}_q(x)\) satisfying

\[h_i(x) = (x - u)^{a_i}f_i(x), \quad \text{and} \quad \nu_{P_u}(f_i(x)) = 0.\]

The integer \(a_i\) and the rational function \(f_i(x)\) are uniquely determined by the conditions above. For \(1 \leq i \leq k\), let \(\bar{n}_i\), \(n'_i\) and \(a'_i\) be the integers:

\[\bar{n}_i = \gcd(n_i, a_i), \quad n'_i = \frac{n_i}{\bar{n}_i}, \quad \text{and} \quad a'_i = \frac{a_i}{\bar{n}_i}\]

such that \(\bar{n}_i \mid q - 1\). Note that \(n_i\) can be greater than \(q - 1\). It is clear that

\[\gcd(n'_i, a'_i) = 1 \quad \text{for } 1 \leq i \leq k.\]
We note that if $a_i = 0$, then $n_i' = 1$. Next we define the positive integers $m_i$ for $i = 1, 2, \ldots, k$ as follows:

$$
m_2 = \gcd(n_2', n_1'),
$$
$$
m_3 = \gcd\left(\frac{n_3'}{m_2}, \frac{n_2'}{m_1}\right) = \gcd\left(n_3', \text{lcm}\left(n_1', n_2'\right)\right),
$$
$$
\vdots
$$
$$
m_k = \gcd\left(\frac{n_k'}{m_{k-1}}, \frac{n_{k-2}'}{m_{k-2}}, \ldots, \frac{n_2'}{m_2}\right) = \gcd\left(n_k', \text{lcm}\left(n_1', n_2', \ldots, n_{k-1}'\right)\right).
$$

As $\gcd\left(\frac{n_1'n_2' \cdots n_{k-1}'}{m_{2m_3 \cdots m_{k-1}}}, a_1'n_2'n_3' \cdots n_{k-1}' \cdots, a_{k-1}'n_1'n_2' \cdots n_{k-2}'\right) = 1$ we choose integers $A_i$ such that

$$
A_{i_1} \frac{n_{i_2}'}{m_{2m_3 \cdots m_{k-1}}} + A_{i_2}a_{i_1}' \frac{n_{i_2}'}{m_{2m_3 \cdots m_{k-1}}} + \cdots + A_{i_k}a_{i_{k-1}}' \frac{n_{i_2}'}{m_{2m_3 \cdots m_{k-1}}} = 1
$$

for $i = 2, 3, \ldots, k$ and $j = 1, \ldots, i$. Let $N_{ij} = -A_{ij+1}n_{i_j} \cdots n_{i_1}'a_{i_j}'$ and $s_{ij} = \nu_r(N_{ij})$ for $i = 2, 3, \ldots, k$ and $j = 1, \ldots, i-1$ and $l_i = \nu_r(m_{i+1})$ for $i = 1, 2, \ldots, k-1$. Moreover, if $f_i(u)$ is an $n_i$-power in $\mathbb{F}_q^*$ (that is $f_i(u) = \alpha_i^{n_i}$) then we define $\alpha_i^{-1} = g^{u_i}$ and $\nu_r(u_i) = u_i'$ for $i = 1, \ldots, k$.

3. Main result

In this section, we derive the necessary and sufficient conditions for the existence of a rational place of $E$ over $P_0$. We also obtain the exact number of such rational places. We need a technical lemma before giving the main result.

**Lemma 3.1.** Let $C_1, C_2, \ldots, C_k$ be the subgroups of $\mathbb{F}_q^*$ with $|C_j| = \bar{n}_j$ for $j = 1, 2, \ldots, k$. Let $\tilde{S}_k$ be the subset of $C_1 \times C_2 \times \cdots \times C_k$ consisting of $(c_1, c_2, \ldots, c_k) \in C_1 \times C_2 \times \cdots \times C_k$ such that

- $(\alpha_1 c_1)^{N_{21} c_2} \alpha_2 c_2$ is an $m_2$-power in $\mathbb{F}_q^*$,
- $(\alpha_1 c_1)^{N_{31}} (\alpha_2 c_2)^{N_{32} c_3}$ is an $m_3$-power in $\mathbb{F}_q^*$,

\[ \vdots \]

- $(\alpha_1 c_1)^{N_{kj-1} c_{j-1}} (\alpha_{j-1} c_{j-1})^{N_{ki-1} c_{k-1}} \alpha_k c_k$ is an $m_k$-power in $\mathbb{F}_q^*$.

Then $\tilde{S}_k$ is not empty if and only if

$$
l_1 = \min\{s_{21} + u_1', u_2', \ldots, u_k'\},
$$
$$
l_2 = \min\{s_{31} + u_1', s_{32} + u_2', u_3', \ldots, u_k'\},
$$
$$
\vdots
$$
$$
l_{k-1} = \min\{s_{k1} + u_1', s_{k2} + u_2', \ldots, s_{kk-1} u_{k-1}' + u_k'\}.
$$

Moreover, if $\tilde{S}_k$ is not empty, then $|\tilde{S}_k| = \bar{n}_1 \bar{n}_1 \cdots \bar{n}_k$. 

*Advances in Mathematics of Communications* Volume 10, No. 1 (2016), 151–162
Proof. Let $M_i$ be the subgroup of $\mathbb{F}_q^*$ with $|M_i| = \frac{q - 1}{m_i}$ for $i = 2, 3, \ldots, k$. Let

$$\mathcal{K}_k = \{(c_1, \ldots, c_k, d_1, \ldots, d_{k-1}) \in C_1 \times \cdots \times C_k \times M_2 \times \cdots \times M_k :$$

$$\begin{align*}
(\alpha_1 c_1)^N_{a_1} \alpha_2 c_2 &= d_1, \\
(\alpha_1 c_1)^N_{a_1} (\alpha_2 c_2)^N_{a_2} \alpha_3 c_3 &= d_2, \\
\vdots
\end{align*}$$

$$= (\alpha_1 c_1)^N_{a_1} (\alpha_2 c_2)^N_{a_2} \cdots (\alpha_{k-1} c_{k-1})^N_{a_{k-1}} \alpha_k c_k = d_{k-1} \}. $$

It is clear that $|\mathcal{K}_k| = |\mathcal{S}_k|$. Let $D_i = \frac{q - 1}{n_i}$ for $i = 1, 2, \ldots, k$ and $g$ be a primitive element of $\mathbb{F}_q^*$. Let

$$\tilde{U}_k = \{(x_1, x_2, \ldots, x_{2k-1}) \in (\mathbb{F}_q^*)^{2k-1} :$$

$$\begin{align*}
x_1^{D_1} x_2^{D_2} x_{k+1}^{m_2} &= \alpha_1^{-n_1}, \\
x_1^{D_1} x_2^{D_2} x_3^{m_3} &= \alpha_1^{-n_1} \alpha_2^{-n_2}, \\
\vdots
\end{align*}$$

$$x_1^{D_1} \cdots x_{k-1}^{D_{k-1}} x_k x_{2k-1}^{m_k} = \alpha_1^{-n_1} \cdots \alpha_k^{-n_k} \cdot \alpha_k^{-1}. $$

Then

$$|\tilde{U}_k| = \frac{q - 1}{n_1} \frac{q - 1}{n_2} \cdots \frac{q - 1}{n_k} \prod_{i=1}^{k} m_i \mathcal{S}_k. $$

Let $u_i, i_1, j_1$ be the integers such that $\alpha_i^{-1} = g^{u_i}, x_i = g^{j_i}, x_{k+1} = g^{\bar{x}_1}, l = 1, \ldots, k$. We obtain the following equalities:

$$g^{j_1 i_1} x_1^{D_1} x_2^{D_2} x_{k+1}^{m_2} = g^{u_1} x_1^{D_1} x_2^{D_2} x_{k+1}^{m_2},$$

$$g^{j_1 i_1} x_1^{D_1} x_2^{D_2} x_3^{m_3} = g^{u_1} x_1^{D_1} x_2^{D_2} x_3^{m_3},$$

$$\vdots$$

$$g^{j_1 i_1} x_1^{D_1} \cdots x_{k-1}^{D_{k-1}} x_k x_{2k-1}^{m_k} = g^{u_1} x_1^{D_1} \cdots x_{k-1}^{D_{k-1}} x_k x_{2k-1}^{m_k}. $$

Thus, we are looking for the number of solutions $(x_1, x_2, \ldots, x_{2k-1}) \in \mathbb{Z}_{q-1}^{2k-1}$ and the conditions of solvability of the following system of equations over $\mathbb{Z}_{q-1}^{2k-1}:

$$\begin{align*}
D_1 x_1 + D_2 x_2 + m_2 x_{k+1} &= N_{a_1}, \\
D_1 x_1 + D_2 x_2 + D_3 x_3 + m_3 x_{k+2} &= N_{a_2}, \\
&\vdots
\end{align*}$$

(6)

$$D_1 x_1 + D_2 x_2 + D_3 x_3 + m_3 x_{k+2} = N_{a_2} + u_2 x_2 + u_3 x_3.$$ 

We recall that $q - 1 = r^a$. Hence we can suppose that $D_i = r^{k_i}, m_i = r^{l_i}, u_i = \hat{u}_i r^{\hat{u}_i}, N_{ij} = N_{ij} r^{s_{ij}}$, for some integers $k_i, l_i, u_i, s_{ij}$, where $u_i$ and $N_{ij}$ are units in $\mathbb{Z}_{q-1}$, for $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, k - 1$. Then, we look for the number of solutions and the conditions of solvability modulo $r^a$ for the following system

$$\begin{align*}
\tilde{N}_{a_1} x_1^{k_1} x_{k+1} + k_2 x_2 + \hat{u}_2 x_2^{k_2} + u_3 x_3^{k_3} + l_2 x_3^{l_2} x_{k+2} = N_{a_1}, \\
\tilde{N}_{a_2} x_1^{k_2} x_{k+2} + k_3 x_3 + \hat{u}_3 x_3^{k_3} x_{k+3} + u_4 x_4^{u_4} = N_{a_2}, \\
\vdots
\end{align*}$$

$$\tilde{N}_{a_k} x_1^{k_{k-1}} x_{k-1} + \hat{u}_k x_k^{l_k} x_{k+1} + k_{k-1} x_{k-1}^{k_{k-1}} x_{k-1} + u_{k-1} x_{k-1}^{u_{k-1}} + \hat{u}_k x_k^{u_k}. $$

The system above has a solution if and only if $r$-adic valuation of coefficients on the left hand side is not greater than the $r$-adic valuation of coefficients on the right.
hand side. We may assume that \( l_1 \leq l_2 \leq \cdots \leq l_{k-1} \) and \( k \leq k_{k-1} \leq \cdots \leq k_1 \).
Moreover, we have that \( l_{k-1} \leq k_{k} \). Thus the coefficient of \( x_{k+1} \) has the minimum \( r \)-adic valuation, and so we can divide the coefficients of the system by \( r^{l_i} \). Thus we can solve the following system modulo \( r^{l_i} \) and multiply its number of solutions by \( r^{(2k-1)l_i} \) to find \( |\tilde{U}_k| \).

\[
\begin{align*}
\tilde{N}_1 r^{k_1+s_1-l_1} x_1 + r^{k_2-l_1} x_2 + x_{k+1} &= \tilde{N}_2 \tilde{u}_1 r^{s_2} u_1^{-l_1} + \tilde{u}_2 r^{u_2^{-l_1}} \\
\tilde{N}_3 r^{k_1+s_1-l_1} x_1 + \tilde{N}_3 r^{s_2} x_2 + r^{k_3-l_1} x_3 + r^{l_2-l_1} x_{k+2} &= \tilde{N}_3 \tilde{u}_1 r^{s_3} u_1^{-l_1} + \tilde{N}_3 \tilde{u}_2 r^{s_3} u_2^{-l_1} + \tilde{u}_3 r^{u_3^{-l_1}} \\
& \vdots \\
\tilde{N}_k r^{k_1+s_1-l_1} x_1 + \cdots + \tilde{N}_k r^{k_{k-1}+s_{k-1}-l_1} x_{k-1} + r^{k_{k-1}-l_1} x_k + r^{l_{k-1}-l_1} x_{2k-1} &= \tilde{N}_k \tilde{u}_1 r^{s_k} u_1^{-l_1} + \cdots + \tilde{N}_k \tilde{u}_{k-1} r^{s_{k-1}} u_{k-1}^{-l_1} + \tilde{u}_k r^{u_k^{-l_1}} 
\end{align*}
\]

Given \( x_1 \) and \( x_2 \), the variable \( x_{k+1} \) can be uniquely found. Next we consider the new system for given \( x_1, x_2 \) and \( x_{k+1} \). The coefficient of \( x_{k+2} \) has the minimum \( r \)-adic valuation, and so we can divide the coefficients of the system by \( r^{l_i-l_2} \). Thus we can solve the remaining system modulo \( r^{a-l_2} \) and multiply its number of solutions by \( r^{(2k-3)(l_i-l_2)} \) to find \( |\tilde{U}_k| \). Then given \( x_3 \), the variable \( x_{k+2} \) can be uniquely found.

If we continue in this way, the number of solutions is

\[
|\tilde{U}_k| = r^{(2k-1)l_1} r^{2(2k-3)(l_2-l_1)} r^{(2k-3)(l_2-l_1)} r^{a-l_2} r^{(2k-5)(l_3-l_2)} r^{a-l_3} \cdots r^{k_{k-1}-l_{k-2}} r^{a-l_{k-1}}
\]

\[
= (q-1)^k m_2 m_3 \cdots m_k.
\]

Therefore we have that \( |\tilde{S}_k| = n_1 n_2 \cdots n_k \).

**Theorem 3.2.** Under the notation as in Section 2, let \( E = \mathbb{F}_q(x, y_1, y_2, \ldots, y_k) \) be the algebraic function field with

\[
\begin{align*}
y_1^{n_1} &= h_1(x), \\
y_2^{n_2} &= h_2(x), \\
& \vdots \\
y_k^{n_k} &= h_k(x).
\end{align*}
\]

Assume that the full constant field of \( E \) is \( \mathbb{F}_q \) and \( |E: \mathbb{F}_q| = n_1 n_2 \cdots n_k \). Assume that \( q - 1 = r^a \) for some prime number \( r \). Moreover assume that \( n_i \mid (q-1) \) for \( 1 \leq i \leq k \) and \( m_i \mid (q-1) \) for \( 2 \leq i \leq k \). Assume that if \( n_i = p_i r^a \), then \( \alpha_i \leq a \).

Then there exist either no or exactly \( \tilde{n}_1 n_2 \cdots \tilde{n}_k m_2 m_3 \cdots m_k \) rational places of \( E \) over \( \mathbb{F}_q \). Furthermore, there exists a rational place of \( E \) over \( \mathbb{F}_q \) if and only if both of the following conditions hold:

- **C1:** \( f_i(u) \) is an \( \tilde{n}_i \)-power in \( \mathbb{F}_q^* \), for \( i = 1, 2, \ldots, k \),
- **C2:** the system of inequalities in (3.1) in the above lemma is satisfied.

**Remark 2.** Note that Theorem 2 in [10] (i.e when \( m_2 = m_3 = \cdots = m_k = 1 \)) becomes a subcase of the above theorem.

**Proof of Theorem 3.2.** Let \( K_0 = \mathbb{F}_q(x) \).

**Step 1.** Let \( E_i \) be the intermediate field with \( K_{i-1} \subseteq E_i \subseteq E \) defined as

\[
E_i = K_{i-1}(z_i) \quad \text{and} \quad z_i^{\tilde{n}_i} = (x-u)^{a_i} f_i(x),
\]

or equivalently

\[
\left( \frac{z_i}{(x-u)^{a_i}} \right)^{\tilde{n}_i} = f_i(x).
\]
Let $P_i$ be an arbitrary place of $E_i$ over $P_{i-1}$. The ramification index $e(P_i|P_{i-1})$ is 1. Therefore there are either no or exactly $\tilde{n}_i$ rational places of $E_i$ over $P_i$. Moreover $P_i$ is a rational place of $E_i$ if and only if the evaluation $f_i(u)$ of $f_i(x)$ at $P_{i-1}$ is an $\tilde{n}_i$-power in $\mathbb{F}_{q_i}^*$. Hence from here till the end of the proof we assume that condition C1 in the hypothesis of the theorem holds. Let $K_i$ be the intermediate field with $E_i \subseteq K_i \subseteq E$ defined as

$$K_i = E_i(y_i) \quad \text{and} \quad \frac{n_i'}{y_i} = z_i.$$ 

The ramification index of an arbitrary place $P_{i+1}$ of $K_i$ over $P_i$ is $\frac{n_i'}{m_i}$. In particular $P_{i+1}|P_i$ is a total ramification, $P_{i+1}$ is the unique place of $K_i$ over $P_i$, and $P_i$ is a rational place of $K_i$.

**Step 2.** Let $F_i$ be the intermediate field with $E_i \subseteq F_i \subseteq E$ defined as

$$F_i = E_i(u_i) \quad \text{and} \quad u_i^{m_i} = z_i.$$ 

Let $T_i$ be the set of rational places of $E_i$ over $P_0$. We note that $|T_i| = \tilde{n}_1 \tilde{n}_2 \cdots \tilde{n}_im_2m_3 \cdots m_{i-1}$. Recall also that $\alpha_1, \alpha_2, \ldots, \alpha_i$ are the chosen elements of $\mathbb{F}_q^*$ with $\alpha_1^{n_i'} = f_1(u), \alpha_2^{n_i'} = f_2(u), \ldots, \alpha_i^{n_i'} = f_i(u)$. Let $P_{i+2}$ be an arbitrary place in $T_i$. By the evaluations

$$\beta_1 = \operatorname{Ev}_{P_{i+2}} \left( \frac{z_1}{(x-u)^{a_1}} \right), \beta_2 = \operatorname{Ev}_{P_{i+2}} \left( \frac{z_2}{(x-u)^{a_2}} \right), \ldots, \beta_i = \operatorname{Ev}_{P_{i+2}} \left( \frac{z_i}{(x-u)^{a_i}} \right),$$

we conclude that $\beta_1^{n_1'} = f_1(u), \beta_2^{n_2'} = f_2(u), \ldots, \beta_i^{n_i'} = f_i(u)$. Let $C_1, C_2, \ldots, C_i$ be the subgroups of $\mathbb{F}_q^*$ with $|C_j| = \tilde{n}_j$ for $j = 1, 2, \ldots, i$. Therefore we obtain that the map

$$\varphi : T_i \rightarrow C_1 \times C_2 \times \cdots \times C_i$$

$$P_{i+2} \mapsto \left( \frac{1}{\alpha_1} \operatorname{Ev}_{P_{i+2}} \left( \frac{z_1}{(x-u)^{a_1}} \right), \ldots, \frac{1}{\alpha_i} \operatorname{Ev}_{P_{i+2}} \left( \frac{z_i}{(x-u)^{a_i}} \right) \right)$$

is a $m_2m_3 \cdots m_{i-1}$-to-1 map between the set $T_i$ and the Cartesian product group $C_1 \times C_2 \times \cdots \times C_i$. Let $\tilde{T}_i$ be the subset of $T_i$ consisting of the places $P_{i+2} \in T_i$ such that there exists a rational place of $F_i$ over $P_{i+2}$.

Let $N_{ij}$ be the integers $N_{ij} = -A_{ij+1} \alpha_1^{n_{i+1}'-n_{i-1}'}u_{i+1}'$ for $j = 1, 2, \ldots, i - 1$. Let $t_i = (x-u)^{A_1}y_1^{A_{i+1}}y_2^{A_{i+2}} \cdots y_{i-1}^{A_{i-1}} \in E_i$. Recall that

$$A_{i+1} \frac{n_1'n_2' \cdots n_{i-1}'}{m_2m_3 \cdots m_{i-1}} + A_{i+2} \frac{n_2'n_3' \cdots n_{i-2}'}{m_2m_3 \cdots m_{i-2}} + \cdots + A_{i}a_{i-1} \frac{n_{i-1}'n_i' \cdots n_{i-2}'}{m_2m_3 \cdots m_{i-2}} = 1.$$ 

Then $\nu_{P_{i+2}}(t_i) = 1$. In particular $t_i$ is a local parameter of $E_i$ for all places in $\tilde{T}_i$.

We also get $\nu_{P_{i+2}} \left( \frac{z_i}{t_i^{n_i'm_i'-m_{i-1}'a_i'}} \right) = 0$. An alternative definition of $F_i$ is

$$F_i = E_i \left( \frac{w_i}{t_i^{n_i'm_i'-m_{i-1}'a_i'}} \right) \quad \text{and} \quad \left( \frac{w_i}{t_i^{n_i'm_i'-m_{i-1}'a_i'}} \right)^{m_i} = \frac{z_i}{t_i^{n_i'm_i'-m_{i-1}'a_i'}}.$$
Hence $\mathcal{T}_i$ is exactly the subset of $\mathcal{T}_i$ consisting of the places $P_{i+2} \in \mathcal{T}_i$ such that

$$\text{Ev}_{P_{i+2}} \left( \frac{z_i}{\frac{n_i^1 n_i^2 \cdots n_i^{i-1}}{m_i^1 m_i^2 m_i^3 \cdots m_i^{i-1} a_i}} \right) \text{ is an } m_i\text{-power in } \mathbb{F}_q^*.$$  

We also have the following

$$\frac{z_i}{\frac{n_i^1 n_i^2 \cdots n_i^{i-1}}{m_i^1 m_i^2 m_i^3 \cdots m_i^{i-1} a_i}} = \frac{z_i}{(x-u)^{a_i}} \left( \frac{z_1}{(x-u)^{a_1}} \right)^{N_i} \left( \frac{z_2}{(x-u)^{a_2}} \right)^{N_2} \cdots \left( \frac{z_{i-1}}{(x-u)^{a_{i-1}}} \right)^{N_{i-1}}.$$  

Let $\varphi(P_{i+2}) = (c_1, c_2, \ldots, c_i)$. Then by definition of $\varphi$ we get $\text{Ev}_{P_{i+2}} \left( \frac{z_i}{(x-u)^{a_i}} \right) = \alpha_i c_i$. We obtain that

$$\text{Ev}_{P_{i+2}} \left( \frac{z_i}{\frac{n_i^1 n_i^2 \cdots n_i^{i-1}}{m_i^1 m_i^2 m_i^3 \cdots m_i^{i-1} a_i}} \right) = (\alpha_1 c_1)^{N_1} (\alpha_2 c_2)^{N_2} \cdots (\alpha_{i-1} c_{i-1})^{N_{i-1}} \alpha_i c_i.$$  

Let $\mathcal{S}_i$ be the subset of $C_1 \times C_2 \times \cdots \times C_i$ consisting of $(c_1, c_2, \ldots, c_i) \in C_1 \times C_2 \times \cdots \times C_i$ $(\alpha_1 c_1)^{N_1} (\alpha_2 c_2)^{N_2} \cdots (\alpha_i c_i)^{N_i}$ is an $m_i$-power in $\mathbb{F}_q^*$. $(\alpha_1 c_1)^{N_1} (\alpha_2 c_2)^{N_2} \cdots (\alpha_i c_i)^{N_i}$ is an $m_i$-power in $\mathbb{F}_q^*$. $(\alpha_1 c_1)^{N_1} (\alpha_2 c_2)^{N_2} \cdots (\alpha_i c_i)^{N_i}$ is an $m_i$-power in $\mathbb{F}_q^*$.

Note that $|\mathcal{T}_i| = m_2 m_3 \cdots m_{i-1} |\mathcal{S}_i|$. Let $P_{i+3}$ be an arbitrary place $F_i$ over $P_{i+2}$. The extension $F_i/E_i$ is Galois, the ramification $e(P_{i+2}|P_{i+2})$ and the inertia $f(P_{i+2}|P_{i+2})$ indices are 1 and hence there are exactly $m_i$ rational places of $F_i$ over $P_{i+2}$. Therefore there are exactly $m_2 m_3 \cdots m_{i-1} m_i |\mathcal{S}_i|$ rational places of $F_i$ over $P_0$.

**Step 3.** Let $L_i$ be the field defined as

$$L_i = F_i(y_i) \quad \text{and} \quad \frac{n_i^y}{m_i} = z_i.$$  

Let $P_{i+4}$ be an arbitrary place of $L_i$ over $P_{i+3}$. We obtain that

$$\gcd \left( \frac{n_i^y}{m_i}, \nu_{P_{i+2}}(z_i) \right) = \gcd \left( \frac{n_i^y}{m_i}, \frac{n_i^1 n_i^2 \cdots n_i^{i-1} a_i}{m_i^1 m_i^2 m_i^3 \cdots m_i^{i-1}} \right) = 1.$$  

Therefore the ramification index $e(P_{i+4}|P_{i+3})$ is $\frac{n_i^y}{m_i}$, $P_{i+4}|P_{i+3}$ is a total ramification; and $P_{i+4}$ is a rational place of $L_i$, which is also the unique place of $L_i$ over $P_{i+3}$.

Hence, for $i = k$ we know that $|\mathcal{S}_k| = \tilde{n}_1 \tilde{n}_2 \cdots \tilde{n}_k$ by Lemma 2. Thus $|\mathcal{T}_k| = \tilde{n}_1 \tilde{n}_2 \cdots \tilde{n}_k m_2 m_3 \cdots m_{k-1}$. Therefore, we proved the theorem.

**Remark 3.** We can obtain the analog of Theorem 3.2 for the place $P_\infty$. We do not state it explicitly here as it can be easily derived as we did in [10, Theorem 3].

The following example illustrates how Theorem 3.1 is applied.
Example 1. Let $E = \mathbb{F}_9(x, y_1, y_2, y_3, y_4, y_5)$ be the function field over $\mathbb{F}_9$ given by the following equations:

$$
\begin{align*}
y_1^2 &= w^3x^2 + wx + w^3, \\
y_2^2 &= w^7x^2 + w, \\
y_3^2 &= w^5x^4 + x^3 + w^6x^2 + 2x + w^3, \\
y_4^2 &= w^3x^3 + 2w^2x^2 + 2x, \\
y_5^2 &= \frac{x + w}{x + w^3}.
\end{align*}
$$

where $w$ is a primitive element of $\mathbb{F}_9$. This is an example of a function field $E$ with genus $g = 17$ and number of rational places $N(E) = 32$. Let $P_0, P_1, \ldots, P_5$ denote the rational places of the rational function field $\mathbb{F}_9(x)$ corresponding to the zeros of the polynomials $x, (x-1), (x-w), (x-w^2), \ldots, (x-w^7)$ respectively. Similarly, let $P_\infty$ denote the rational place of $\mathbb{F}_9(x)$ corresponding to the pole of $x$. First we compute the number of rational places of $E$ over each of the rational places $P_0, P_1, \ldots, P_5, P_\infty$ by applying Theorem 3.1 for each of them separately. Then summing these numbers up we get the number $N(E)$ of rational places of $E$. We explain the computations in detail as follows:

- **Over $P_0$:** We have

  $$
  n_1 = 2, a_1 = 1, \bar{n}_1 = \gcd(n_1, a_1) = 1, n'_1 = \frac{n_1}{\bar{n}_1} = 2,
  $$

  $$
  n_2 = 2, a_2 = 1, \bar{n}_2 = \gcd(n_2, a_2) = 1, n'_2 = \frac{n_2}{\bar{n}_2} = 2,
  $$

  $$
  n_3 = 2, a_3 = 0, \bar{n}_3 = \gcd(n_3, a_3) = 2, n'_3 = \frac{n_3}{\bar{n}_3} = 1,
  $$

  $$
  n_4 = 2, a_4 = 0, \bar{n}_4 = \gcd(n_4, a_4) = 2, n'_4 = \frac{n_4}{\bar{n}_4} = 1,
  $$

  $$
  n_5 = 2, a_5 = 0, \bar{n}_5 = \gcd(n_5, a_5) = 2, n'_5 = \frac{n_5}{\bar{n}_5} = 1.
  $$

Then $m_2 = \gcd(n'_1, n'_2) = 2, m_3 = m_4 = m_5 = 1$. Moreover we have:

$$
\begin{align*}
f_1(0) &= w^3 \text{is an } \bar{n}_1\text{-power in } \mathbb{F}_9^*, \\
f_2(0) &= w \text{ is an } \bar{n}_2\text{-power in } \mathbb{F}_9^*, \\
\text{But } f_3(0) &= \frac{w^3}{w^6} = w^{-3} \text{ is not an } \bar{n}_3\text{-power in } \mathbb{F}_9^*. 
\end{align*}
$$

Then there are no rational places of $E$ lying over $P_0$.

- **Over $P_1$:** We have

  $$
  n_1 = 2, a_1 = 0, \bar{n}_1 = \gcd(n_1, a_1) = 2, n'_1 = \frac{n_1}{\bar{n}_1} = 1,
  $$

  $$
  n_2 = 2, a_2 = 0, \bar{n}_2 = \gcd(n_2, a_2) = 2, n'_2 = \frac{n_2}{\bar{n}_2} = 1, a'_2 = 0,
  $$

  $$
  n_3 = 2, a_3 = 2, \bar{n}_3 = \gcd(n_3, a_3) = 2, n'_3 = \frac{n_3}{\bar{n}_3} = 1, a'_3 = 1,
  $$

  $$
  n_4 = 2, a_4 = 0, \bar{n}_4 = \gcd(n_4, a_4) = 2, n'_4 = \frac{n_4}{\bar{n}_4} = 1, a'_4 = 0,
  $$

  $$
  n_5 = 2, a_5 = 0, \bar{n}_5 = \gcd(n_5, a_5) = 2, n'_5 = \frac{n_5}{\bar{n}_5} = 1, a'_5 = 0.
  $$

$$
Then $m_2 = \gcd(n'_1, n'_2) = 1$, $m_3 = m_4 = m_5 = 1$. Moreover we have:

- $f_1(1) = 2w^3 + w$ is an $\bar{n}_1$-power in $F_9^*$,
- $f_2(1) = w^7 + w$ is an $\bar{n}_2$-power in $F_9^*$,
- $f_3(1) = \frac{w^6 + w^5 + w^3 + 3}{w^6 + w^3 + 1}$ is an $\bar{n}_3$-power in $F_9^*$,
- $f_4(1) = \frac{w^3 + 4}{w + 1}$ is an $\bar{n}_4$-power in $F_9^*$,
- $f_5(1) = \frac{w^5 + w^3 + w^2}{w^3 + 1}$ is an $\bar{n}_5$-power in $F_9^*$,

We have $D_1 = \frac{q - 1}{n_1} = \frac{8}{2} = 4, D_2 = D_3 = D_4 = D_5 = 4$ and

- $N_{21} = -A_{22} \frac{n'_1 n'_2 n'_3 n'_4}{n'_1 m_2 m_3 m_4} a'_2 = 0$ since $a'_2 = 0$,
- $N_{31} = -A_{32} \frac{n'_1 n'_2 n'_3 n'_4}{n'_1 m_2 m_3 m_4} a'_3 = -A_{32},$
- $N_{32} = -A_{33} \frac{n'_1 n'_2 n'_3 n'_4}{n'_2 m_2 m_3 m_4} a'_3 = -A_{33},$
- $N_{41} = -A_{42} \frac{n'_1 n'_2 n'_3 n'_4}{n'_1 m_2 m_3 m_4} a'_4 = 0$ since $a'_4 = 0$,
- $N_{42} = -A_{43} \frac{n'_1 n'_2 n'_3 n'_4}{n'_2 m_2 m_3 m_4} a'_4 = 0$ since $a'_4 = 0$,
- $N_{43} = -A_{44} \frac{n'_1 n'_2 n'_3 n'_4}{n'_3 m_2 m_3 m_4} a'_4 = 0$ since $a'_4 = 0$,

and $N_{51} = N_{52} = N_{53} = N_{54} = 0$ since $a'_5 = 0$.

So we get the following system of equations:

- $4.0 + 4x_2 + x_6 = u_2 \mod q - 1$
- $-4A_{32}x_1 + 4(-A_{33})x_2 + 4x_3 + x_7 = -A_{32}u_1 - A_{33}u_2 + u_3 \mod q - 1$
- $4.0 + 4.0 + 4x_4 + x_7 = 0u_1 + 0u_2 + 0u_3 + u_4 \mod q - 1$
- $4.0 + 4.0 + 4.0 + 4x_5 + x_9 = u_5 \mod q - 1$.

Solving the linear system above we get $\bar{n}_1 \bar{n}_2 \bar{n}_3 \bar{n}_4 \bar{n}_5 m_2 m_3 m_4 m_5 = 32$ rational places of $E$ over $P_1$.

Over $P_2, P_3, \ldots, P_7$ and $P_{\infty}$, condition C1 of Theorem 3.1 is not satisfied so there are no rational places over these places. Therefore there are totally 32 rational places. We compute the genus using the Hurwitz genus formula.

4. Examples

Example 2. Let $E = \mathbb{F}_{17}(x,y_1,y_2,y_3)$ be the function field over $\mathbb{F}_{17}$ given by the following equations:

- $y_1^2 = x^2 + 1$
- $y_2^2 = 3x^2 + x + 14$
- $y_3^2 = 3x^2 + 16x + 14$
Further results on fibre products of Kummer covers

The genus of $E$ is $g(E) = 5$ and $N(E) = 48$. This number is a new entry in the table [13]. By using Theorem 3.2, we obtain that there are 8 rational places over each of the places $P_{x-1}, P_{x-5}, P_{x-7}, P_{x-10}, P_{x-12}$ and $P_{x-16}$ of rational function field.

**Example 3.** Let $E = F_{17}(x, y_1, y_2, y_3)$ be the function field over $F_{17}$ given by the following equations:

\[
\begin{align*}
y_1^2 &= x^2 + 1 \\
y_2^2 &= 4x^2 + 1 \\
y_3^2 &= \frac{13x^2 + 15x + 9}{x + 4} 
\end{align*}
\]

The genus of $E$ is $g(E) = 7$ and we obtain that $N(E) = 60$ by using Theorem 3.2. This number is a new entry in the table [13]. We note that $m_2 = 2$ over $P_\infty$.

**Example 4.** Let $E = F_{17}(x, y_1, y_2, y_3)$ be the function field over $F_{17}$ given by the following equations:

\[
\begin{align*}
y_1^2 &= 14x^3 + x^2 + 11x + 15 \\
y_2^2 &= 13x^3 + 7x^2 + 8x + 5 \\
y_3^2 &= 14x^4 + 6x^3 + 15x^2 + 11 
\end{align*}
\]

The genus of $E$ is $g(E) = 9$ and we obtain that $N(E) = 72$ by using Theorem 3.2. This number is a new entry in the table [13].

**Example 5.** Let $E = F_{17}(x, y_1, y_2, y_3)$ be the function field over $F_{17}$ given by the following equations:

\[
\begin{align*}
y_1^2 &= 2x^3 + 4x^2 + 15x + 4 \\
y_2^2 &= 3x^3 + 4x^2 + 14x + 15 \\
y_3^2 &= 2x^4 + 3x^3 + 4x^2 + 5x + 2 
\end{align*}
\]

The genus of $E$ is $g(E) = 11$ and we obtain that $N(E) = 76$ by using Theorem 3.2. This number is a new entry in the table [13].

**Example 6.** Let $E = F_{17}(x, y_1, y_2, y_3)$ be the function field over $F_{17}$ given by the following equations:

\[
\begin{align*}
y_1^2 &= 14x^3 + 15x^2 + 3x + 1 \\
y_2^2 &= 14x^3 + 2x^2 + 13x + 6 \\
y_3^2 &= 16x^4 + x^3 + 3x^2 + 3x + 3 
\end{align*}
\]

The genus of $E$ is $g(E) = 13$ and we obtain that $N(E) = 84$ by using Theorem 3.2. This number is a new entry in the table [13]. We note that $m_2 = 2$ over $P_\infty$ and $P_{x-7}$.

**Example 7.** Let $E = F_{17}(x, y_1, y_2, y_3)$ be the function field over $F_{17}$ given by the following equations:

\[
\begin{align*}
y_1^2 &= 13x^3 + 8x^2 + 12x + 2 \\
y_2^2 &= 10x^3 + 9x^2 + 15x + 8 \\
y_3^2 &= 15x^4 + 2x^3 + 2x^2 + 14x + 16 
\end{align*}
\]
The genus of $E$ is $g(E) = 15$ and we obtain that $N(E) = 84$ by using Theorem 3.2. This number is a new entry in the table [13].

**Example 8.** Let $E = \mathbb{F}_5(x, y_1, y_2, y_3)$ be the function field over $\mathbb{F}_5$ given by the following equations:

- $y_1^4 = x^2 + 1$
- $y_2^4 = 3x^2 + 4x + 1$
- $y_3^4 = 2x^3 + 4x + 1$

The genus of $E$ is $g(E) = 33$ and $N(E) = 64$. This number is the best value known in the table [13]. We obtain that there are 64 rational places over the place $P_x$ of the rational function field, by using Theorem 3.2.

**Acknowledgments**

We would like to thank the anonymous referees for their useful comments that improved the paper.

**References**

[1] A. Garcia and A. Garzon, On Kummer covers with many rational points over finite fields, *J. Pure Appl. Algebra*, 185 (2003), 177–192.

[2] G. van der Geer and M. van der Vlugt, Tables of curves with many points, *Math. Comput.*, 69 (2000), 797–810.

[3] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd edition, The Clarendon Press, New York, 1998.

[4] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Univ. Press, Princeton, 2008.

[5] B. Huppert and N. Blackburn, *Finite Groups II* Springer-Verlag, New York, 1981.

[6] M. Q. Kawakita, Kummer curves and their fibre products with many rational points, *Appl. Algebra Engy. Comm. Comput.*, 14 (2003), 55–64.

[7] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields*, Cambridge Univ. Press, Cambridge, 2001.

[8] H. Niederreiter and C. Xing, *Algebraic Geometry in Coding Theory and Cryptography*, Princeton Univ. Press, Princeton, 2009.

[9] F. Özbudak and H. Stichtenoth, Curves with many points and configurations of hyperplanes over finite fields, *Finite Fields Appl.*, 5 (1999), 436–449.

[10] F. Özbudak and B. G. Temür, Finite number of fibre products of Kummer covers and curves with many points over finite fields, *Des. Codes Crypt.*, 70 (2014), 385–404.

[11] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[12] M. A. Tsfasman, S. G. Vlăduţ and D. Nogin, *Algebraic Geometric Codes: Basic Notions*, Amer. Math. Soc., Providence, 2007.

[13] Manypoints-Table of Curves with Many Points, available online at [http://www.manypoints.org](http://www.manypoints.org)

Received December 2014; revised December 2015.

*E-mail address:* ozbudak@metu.edu.tr  
*E-mail address:* burcu.temur@atilim.edu.tr  
*E-mail address:* oguz.yayla@hacettepe.edu.tr