Noname manuscript No.
(will be inserted by the editor)

Finite number of fibre products of Kummer covers and curves with many points over finite fields

Ferruh Özbudak · Burcu Gülmez Temür

Received: date / Accepted: date

Abstract We study fibre products of a finite number of Kummer covers of the projective line over finite fields. We determine the number of rational points of the fibre product over a rational point of the projective line, which improves the results of [9] substantially. We also construct explicit examples of fibre products of Kummer covers with many rational points, including a record and two new entries for the current table [12].

Keywords Curves with many points over finite fields · Kummer covers · fibre products

1 Introduction

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

$$N \leq q + 1 + 2g(\mathcal{C})\sqrt{q}. \tag{1}$$

If the bound in (1) is attained and $g(\chi) \geq 1$, then χ is called a maximal curve. There are some improvements on (1) especially when $g(\chi)$ is large [3], [4], [6], [10], [11]. 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 $\mathbb{F}_q$. It is an important problem to determine $N_q(g)$ and to construct explicit curves with many rational points (see [2], and [12] for the current tables). There

Ferruh Özbudak
Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bulvarı, No: 1, 06800, Ankara, Turkey
E-mail: ozbudak@metu.edu.tr

Burcu Gülmez Temür
Department of Mathematics, Atılım University, İncek, Gölbaşı, 06836, Ankara, Turkey
E-mail: bgtemur@atilim.edu.tr

are many applications to areas including coding theory, cryptography and quasi-random points [4], [6], [7], [10], [11].

Some types of fibre products of Kummer covers of the projective line were studied and such explicit curves with many points were found [1], [5], [8], [9]. In particular in [9] we studied the general fibre products of two Kummer covers of the projective line. In this paper we study the general fibre products of a finite number of Kummer covers of the projective line. Namely let $k \geq 2$ and $n_1, n_2, \ldots, n_k \geq 2$ be integers, and $h_1(x), h_2(x), \ldots, h_k(x) \in \mathbb{F}_q(x)$. Consider the fibre product

$$\begin{array}{l} y_1^{n_1} = h_1(x), \\ y_2^{n_2} = h_2(x), \\ \quad \vdots \\ y_k^{n_k} = h_k(x). \end{array} \tag{2}$$

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 (2). We will assume that $[E : \mathbb{F}_q(x)] = n_1 n_2 \ldots n_k$ and the full constant field of E is $\mathbb{F}_q$. The theory of algebraic curves is essentially equivalent to the theory of algebraic function fields. Throughout the paper we use the language of function fields [10]. We call a degree one place of an algebraic function field as a *rational place (or rational point)* of the function field.

Let P be a rational place of the rational function field $\mathbb{F}_q(x)$. In [9] we determined the number of rational places of E over P when $k = 2$ under certain conditions. Here we determine the number of rational places of E over P for an arbitrary $k \geq 2$ under some conditions in Theorems 2 and 3. The conditions in Theorems 2 and 3 allow us to obtain the results systematically for arbitrary $k \geq 2$. However it turns out that these conditions are strong conditions (see Remark 4). In Assumption 1, for arbitrary $k \geq 2$, we develop a weak condition which seems to be the most natural condition (in applying our methods) for determining the number of rational places of E over P. Assumption 1 is also weaker than the conditions of the theorems in [9] when $k = 2$. Therefore we reconsider the case $k = 2$ under Assumption 1 and we improve the theorems of [9] in Theorem 4 (and Remark 7) substantially. The proof of Theorem 4 is more difficult than the proof of the theorems in [9] and we develop further tools in order to handle it in Section 4. The theorems of [9] correspond to a very special subcase of Theorem 4 (see Remark 5).

We also give explicit examples of fibre products of Kummer covers with many rational points. In particular Example 4 is a record; and Examples 5 and 7 are new entries for the table [12].

We notice a mistake in the formulation of the theorems of [9] and we correct it in Remark 6. This mistake does not affect the explicit examples in [9].

The paper is organized as follows. In Section 2 we fix some further notation and introduce Assumption 1. We study the fibre products of an arbitrary number of Kummer covers under a strong condition in Section 3. We study the general fibre products of two Kummer covers under Assumption 1 in Section 4 and we also develop the necessary tools there. Finally explicit examples of fibre products with many rational points are presented in Section 5.

2 Preliminaries

In this section we fix some notation and we introduce Assumption 1.

For an algebraic function field F with full constant field $\mathbb{F}_q$, if $f(x) \in F$ and P is a rational place of F, then we denote the evaluation of $f(x)$ at P by $\mathrm{Ev}_P(f(x))$. We choose $u \in \mathbb{F}_q$ and we denote the rational place of the rational function field corresponding to the zero of $(x-u)$ as P_0. Similarly the rational place corresponding to the pole of x is denoted as P_∞. For $1 \le i \le k$, the evaluation of $f_i(x)$ at P_0 is denoted also by $f_i(u)$. Moreover $\mathbb{F}_q^*$ denotes the multiplicative group $\mathbb{F}_q \setminus \{0\}$.

For $1 \le i \le k$, let a_i be the integer and $f_i(x) \in \mathbb{F}_q(x)$ be the rational function satisfying

$$h_i(x) = (x-u)^{a_i} f_i(x), \text{ and } \nu_{P_0}(f_i(x)) = 0.$$

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

$$\bar{n}_i = \gcd(n_i, a_i), \qquad n_i' = \frac{n_i}{\bar{n}_i}, \qquad \text{and} \qquad a_i' = \frac{a_i}{\bar{n}_i}. \tag{3}$$

Note that if $a_i = 0$, then $n_i' = 1$. We have

$$\gcd(n_i', a_i') = 1 \quad \text{for } 1 \le i \le k. \tag{4}$$

Next we define the positive integers $m_2, m_3, \ldots, m_k$ recursively as follows:

$$\begin{aligned}
m_2 &= \gcd(n_2', n_1'),\\
m_3 &= \gcd\left(n_3', \frac{n_2'}{m_2} n_1'\right) = \gcd\left(n_3', \mathrm{lcm}\ (n_1', n_2')\right),\\
m_4 &= \gcd\left(n_4', \frac{n_3'}{m_3}\frac{n_2'}{m_2} n_1'\right) = \gcd\left(n_4', \mathrm{lcm}\ (n_1', n_2', n_3')\right),\\
&\vdots\\
m_k &= \gcd\left(n_k', \frac{n_{k-1}'}{m_{k-1}}\frac{n_{k-2}'}{m_{k-2}} \cdots \frac{n_2'}{m_2} n_1'\right) = \gcd\left(n_k', \mathrm{lcm}\ (n_1', n_2', \ldots, n_{k-1}')\right).
\end{aligned} \tag{5}$$

Remark 1 For $k \ge 3$ the definitions of $m_2, m_2, \ldots, m_k$ do depend on the order $(n_1', n_2', \ldots, n_k')$ of the positive integers $n_1', n_2', \ldots, n_k'$. For instance let $k = 3$ and consider the order $(n_1', n_2', n_k') = (4, 6, 9)$, from which we get $(m_2, m_3) = (2, 3)$. By a simple reordering we have $(\tilde{n}_1', \tilde{n}_2', \tilde{n}_3') = (9, 4, 6)$, from which we get $(\tilde{m}_2, \tilde{m}_3) = (1, 6)$.

Remark 2 Nevertheless the joint condition

$$m_2 \mid (q-1),\ m_3 \mid (q-1),\ \ldots,\ \text{and} \quad m_k \mid (q-1)$$

is independent from the order. For instance in the case of numerical examples of Remark 1 we get the equivalent joint conditions

$$\{m_2 = 2 \mid (q-1), m_3 = 3 \mid (q-1)\} \quad \text{and} \quad \{\tilde{m}_2 = 1 \mid (q-1), \tilde{m}_3 = 6 \mid (q-1)\}.$$

We prove this independence in Lemma 1 below.

The following will be our main assumption. For a prime ρ, let ν_ρ be the ρ-adic valuation: $\nu_\rho(\rho) = 1$, $\nu_\rho(\rho^2) = 2$ and $\nu_\rho(n) = 0$ if n is an integer with $\gcd(n, \rho) = 1$.

Assumption 1 *For each prime ρ dividing $n'_1 n'_2 \dots n'_k$, the following condition holds:*

Let $e_1, e_2, \dots, e_{k-1}, e_k$ be the nonnegative integers (depending on ρ) defined as

$$e_1 = \nu_\rho(n'_1),\ e_2 = \nu_\rho(n'_2),\ \dots,\ e_{k-1} = \nu_\rho(n'_{k-1}), e_k = \nu_\rho(n'_k).$$

Let $(\hat{e}_1, \hat{e}_2, \dots, \hat{e}_{k-1}, \hat{e}_k)$ be the reordering of $(e_1, e_2, \dots, e_k)$ such that

$$\hat{e}_1 \leq \hat{e}_2 \leq \cdots \leq \hat{e}_{k-1} \leq \hat{e}_k.$$

The condition is:

$$\rho^{\hat{e}_{k-1}} \mid (q-1) \text{ or equivalently } \nu_\rho(q-1) \geq \hat{e}_{k-1}.$$

The following lemma shows that Assumption 1 is equivalent to the joint condition mentioned in Remark 2.

Lemma 1 *Under the notation as above we have that*

$$m_2 \mid (q-1),\ m_3 \mid (q-1),\ \dots,\ \text{and}\ \ m_k \mid (q-1) \tag{6}$$

if and only if Assumption 1 holds.

Proof We keep the notation of Assumption 1. It is enough to prove that for each prime ρ dividing $n'_1 n'_2 \dots n'_k$, we have

$$\max\{\nu_\rho(m_2), \nu_\rho(m_3), \dots, \nu_\rho(m_k)\} = \hat{e}_{k-1}. \tag{7}$$

We prove it by induction on k. The case $k = 2$ holds by definition. Assume that $k \geq 2$ and (7) holds for the case k. Namely we assume that

$$\max\{\nu_\rho(m_2), \dots, \nu_\rho(m_k)\} = \hat{e}_{k-1},$$

where $(\hat{e}_1, \hat{e}_2, \dots, \hat{e}_{k-1}, \hat{e}_k)$ is the reordering of $(e_1, e_2, \dots, e_{k-1}, e_k)$ such that $\hat{e}_1 \leq \hat{e}_2 \leq \cdots \leq \hat{e}_{k-1} \leq \hat{e}_k$.

Let $e_{k+1} = \nu_\rho(n'_{k+1})$ and $m_{k+1} = \gcd\left(n'_{k+1}, \operatorname{lcm}\ \left(n'_1, n'_2, \dots, n'_k\right)\right)$. We need to prove that

$$\max\{\nu_\rho(m_2), \nu_\rho(m_3), \dots, \nu_\rho(m_k), \nu_\rho(m_{k+1})\} = \tilde{e}_k, \tag{8}$$

where $(\tilde{e}_1, \tilde{e}_2, \dots, \tilde{e}_k, \tilde{e}_{k+1})$ is the reordering of $(e_1, e_2, \dots, e_{k-1}, e_k)$ such that $\tilde{e}_1 \leq \tilde{e}_2 \leq \cdots \leq \tilde{e}_k \leq \tilde{e}_{k+1}$. Note that (8) is equivalent to

$$\max\{\hat{e}_{k-1}, \nu_\rho(m_{k+1})\} = \tilde{e}_k. \tag{9}$$

Moreover we have

$$\nu_\rho(m_{k+1}) = \min\{e_{k+1}, \max\{e_1, e_2, \dots, e_k\}\} = \min\{e_{k+1}, \hat{e}_k\}. \tag{10}$$

Assume first that $e_{k+1} \leq \hat{e}_k$. As we have $\hat{e}_k \geq \max\{\hat{e}_1, \hat{e}_2, \dots, \hat{e}_{k-1}\} = \hat{e}_{k-1}$, we conclude that $\tilde{e}_k = \max\{\hat{e}_{k-1}, e_{k+1}\}$. By (9) and (10), this implies (8).

Assume next that $e_{k+1} > \hat{e}_k$. We have $e_{k+1} > \hat{e}_k \geq \hat{e}_{k-1}$ and hence $\tilde{e}_k = \hat{e}_k$. By (9) and (10), this implies (8). The proof is completed.

Remark 3 We observe that Assumption 1 is independent from the order $(n'_1, n'_2, \dots, n'_k)$. Therefore the condition (6) in Lemma 1 is independent from the order as well.

3 Finite number of fibre products under a strong condition

We keep the notation of Section 2. In this section we determine the number of rational places of E over P_0 (and P_∞) for an arbitrary finite number k, but under a strong condition. Theorem 2 is the main result of this section. Its statement and its proof are rather simple because of a nice condition (cf. in (12)). However it turns out that this condition is actually a strong condition (see Remark 4).

We define the positive integers $\hat{n}_1, \hat{n}_2, \dots \hat{n}_k$ recursively as:

$$\begin{aligned}
\hat{n}_1 &= \gcd(n_1, a_1) = \bar{n}_1, \\
\hat{n}_2 &= \gcd\left(n_2, \frac{n_1}{\hat{n}_1} a_2\right), \\
\hat{n}_3 &= \gcd\left(n_3, \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2} a_3\right), \\
&\vdots \\
\hat{n}_k &= \gcd\left(n_k, \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2} \dots \frac{n_{k-1}}{\hat{n}_{k-1}} a_k\right).
\end{aligned} \tag{11}$$

In Lemma 2 below we will show that actually $\hat{n}_i = \bar{n}_i m_i$ for $2 \le i \le k$.

In the proofs of Theorem 2 and 4 below, we will frequently use Proposition 3.7.3 in [10] on Kummer extensions. It allows us to determine the ramification and inertia indices of certain field extensions explicitly. We prefer to cite it once here instead of citing it many times in the proofs.

Theorem 2 *Under the notation as above, assume that the full constant field of E is $\mathbb{F}_q$ and $[E : \mathbb{F}_q(x)] = n_1 n_2 \dots n_k$. Moreover assume that the integers $\hat{n_1}, \hat{n}_2, \dots, \hat{n}_k$ divide $(q-1)$ and also that*

$$\hat{n}_2 \mid a_2, \;\; \hat{n}_3 \mid a_3, \;\; \dots, \;\; \text{and } \hat{n}_k \mid a_k. \tag{12}$$

There exist either no or exactly $(\hat{n}_1 \hat{n}_2 \dots \hat{n}_k)$ rational places of E over P_0. There exists a rational place of E over P_0 if and only if all of the following conditions hold

- *$f_1(u)$ is an $\hat{n}_1$-power in $\mathbb{F}_q^*$,*
- *$f_2(u)$ is an $\hat{n}_2$-power in $\mathbb{F}_q^*$,*

  $\vdots$
- *$f_k(u)$ is an $\hat{n}_k$-power in $\mathbb{F}_q^*$.*

Proof Let $K_0 = \mathbb{F}_q(x)$. Moreover let $K_1, K_2, \dots, K_k$ be the algebraic function fields defined recursively as

- $K_1 = K_0(y_1)$ with $y_1^{n_1} = h_1(x)$,
- $K_2 = K_1(y_2)$ with $y_2^{n_2} = h_2(x)$,

  $\vdots$

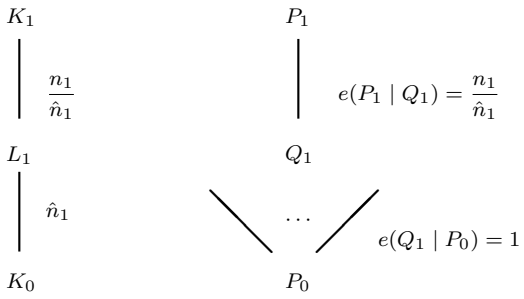

Fig. 1

– $K_k = K_{k-1}(y_k)$ with $y_k^{n_k} = h_k(x)$.

Note that $K_k = E$. Using the assumption $[K_k : K_0] = n_1 n_2 \dots n_k$ it is not difficult to observe that

$$[K_1 : K_0] = n_1,\ [K_2 : K_1] = n_2,\ \dots\ [K_k : K_{k-1}] = n_k.$$

Let L_1 be the intermediate field $K_0 \subseteq L_1 \subseteq K_1$ defined as

$$L_1 = K_0(w_1) \quad \text{with} \quad w_1^{\hat{n}_1} = f_1(x). \tag{13}$$

Note that $\hat{n}_1$ divides a_1 by definition of $\hat{n}_1$. We observe that

$$K_1 = L_1(y_1) \quad \text{with} \quad y_1^{\frac{n_1}{\hat{n}_1}} = z_1 = (x-u)^{\frac{a_1}{\hat{n}_1}} w_1. \tag{14}$$

Using the fact $[K_1 : K_0] = n_1$, (13) and (14) we get that

$$[L_1 : K_0] = \hat{n}_1, \text{ and } [K_1 : L_1] = \frac{n_1}{\hat{n}_1}.$$

Moreover, the extension L_1/K_0 is a Galois extension as $\hat{n}_1 \mid (q-1)$.

Let Q_1 be a place of L_1 over P_0 (see Figure 1). We have $\nu_{P_0}(f_1(x)) = 0$, $\gcd(\hat{n}_1, \nu_{P_0}(f_1(x))) = \hat{n}_1$ and hence the ramification index $e(Q_1|P_0)$ is 1. As the extension L_1/K_0 is a Galois extension, there are either no or exactly $\hat{n}_1$ rational places of L_1 over P_0. Therefore Q_1 is a rational place if and only if $f_1(u)$ is an $\hat{n}_1$-power in $\mathbb{F}_q^*$.

Assume that Q_1 is a rational place of L_1 over P_0. Let P_1 be a place of K_1 over Q_1 (see Figure 1). We have

$$\nu_{Q_1}(z_1) = \frac{a_1}{\hat{n}_1},\ \nu_{Q_1}(x-u) = 1,\ \gcd\left(\frac{n_1}{\hat{n}_1}, \nu_{Q_1}(z_1)\right) = 1$$

and hence the ramification index $e(P_1|Q_1)$ is $\frac{n_1}{\hat{n}_1}$. In particular $P_1|Q_1$ is a total ramification. Hence P_1 is the unique place of K_1 over Q_1 and P_1 is a rational place. We further have that

$$\nu_{P_1}(x-u) = \frac{n_1}{\hat{n}_1}.$$

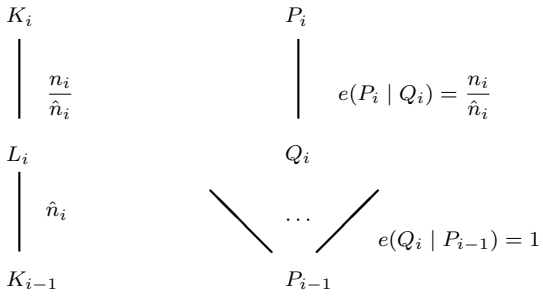

Fig. 2 $(i \geq 2)$

Now we complete the proof by induction. For $2 \leq i \leq k-1$, assume that the statement of the theorem holds and there exists a rational place P_{i-1} of K_{i-1} over P_0 such that

$$\nu_{P_{i-1}}(x-u) = \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2}\cdots\frac{n_{i-1}}{\hat{n}_{i-1}} \text{ if } i \geq 2. \tag{15}$$

Let L_i be the intermediate field $K_{i-1} \subseteq L_i \subseteq K_i$ such that

$$L_i = K_{i-1}(w_i) \text{ with } w_i^{\hat{n}_i} = f_i(x).$$

Note that by the assumption in (12) we have $\hat{n}_i \mid a_i$. We have

$$K_i = L_i(y_i) \text{ with } y_i^{\frac{n_i}{\hat{n}_i}} = z_i = (x-u)^{\frac{a_i}{\hat{n}_i}} w_i.$$

We observe that, as in the case $i = 1$ above,

$$[L_i : K_{i-1}] = \hat{n}_i, \quad [K_i : L_i] = \frac{n_i}{\hat{n}_i},$$

and the extension L_i/K_{i-1} is Galois.

Let Q_i be a place of L_i over P_{i-1} (see Figure 2). We have $\nu_{P_{i-1}}(f_i(x)) = 0$, and Q_i is a rational place if and only if $f_i(u)$ is an $\hat{n}_i$-power in $\mathbb{F}_q^*$. Assume that Q_i is a rational place of L_i over P_{i-1}. Let P_i be a place of K_i over Q_i (see Figure 2). Using (15) we get that

$$\nu_{Q_i}(x-u) = e(Q_i|P_{i-1})\,\nu_{P_{i-1}}(x-u) = \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2}\cdots\frac{n_{i-1}}{\hat{n}_{i-1}}. \tag{16}$$

Then from (16) we obtain that

$$\nu_{Q_i}(z_i) = \frac{a_i}{\hat{n}_i}\nu_{Q_i}(x-u) = \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2}\cdots\frac{n_{i-1}}{\hat{n}_{i-1}}\frac{a_i}{\hat{n}_i}. \tag{17}$$

Moreover

$$\gcd\left(\frac{n_i}{\hat{n}_i}, \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2}\cdots\frac{n_{i-1}}{\hat{n}_{i-1}}\frac{a_i}{\hat{n}_i}\right) = 1. \tag{18}$$

Combining (17) and (18) we conclude that ramification index $e(P_i|Q_i)$ is $\frac{n_i}{\hat{n}_i}$. In particular $P_i|Q_i$ is a total ramification, P_i is the unique place of K_i over Q_i and P_i is a rational place. Moreover

$$\nu_{P_i}(x-u) = \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2}\cdots\frac{n_i}{\hat{n}_i}.$$

This completes the proof.

The following lemma is used in Remark 4 below.

Lemma 2 *Under the notation as above we have*

$$\hat{n}_i = \bar{n}_i m_i \ \text{ for } 2 \leq i \leq k.$$

Proof We prove by induction. Note that $n_2' = n_2/\bar{n}_2$, $a_2' = a_2/\bar{n}_2$ and

$$\hat{n}_2 = \gcd(n_2, n_1' a_2) = \gcd(\bar{n}_2 n_2', n_1' \bar{n}_2 a_2') = \bar{n}_2 \gcd(n_2', n_1' a_2') = \bar{n}_2 m_2,$$

where we use the facts $\gcd(n_2', a_2') = 1$ and $m_2 = \gcd(n_2', n_1')$ in the last equality. For the induction, assume that $2 \leq i \leq k-1$ and

$$\hat{n}_j = \bar{n}_j m_i \ \text{ for each } j \text{ with } 2 \leq j \leq i. \tag{19}$$

We have

$$\begin{aligned}
\hat{n}_{i+1} &= \gcd\left(n_{i+1}, \frac{n_1}{\hat{n}_1}\frac{n_2}{\hat{n}_2}\cdots\frac{n_i}{\hat{n}_i}a_{i+1}\right) \ \text{ by definition in (11),} \\
&= \gcd\left(n_{i+1}, \frac{n_1}{\bar{n}_1}\frac{n_2}{\bar{n}_2 m_2}\cdots\frac{n_i}{\bar{n}_i m_i}a_{i+1}\right) \ \text{ by (19),} \\
&= \gcd\left(\bar{n}_{i+1}n_{i+1}', \frac{\bar{n}_1 n_1'}{\bar{n}_1}\frac{\bar{n}_2 n_2'}{\bar{n}_2 m_2}\cdots\frac{\bar{n}_i n_i'}{\bar{n}_i m_i}\bar{n}_{i+1}a_{i+1}'\right) \ \text{ by definitions in (3),} \\
&= \bar{n}_{i+1}\gcd\left(n_{i+1}', n_1'\frac{n_2'}{m_2}\frac{n_3'}{m_3}\cdots\frac{n_i'}{m_i}a_{i+1}'\right) \\
&= \bar{n}_{i+1}\gcd\left(n_{i+1}', n_1'\frac{n_2'}{m_2}\frac{n_3'}{m_3}\cdots\frac{n_i'}{m_i}\right) \ \text{ as } \gcd(n_{i+1}', a_{i+1}') = 1. \\
&= \bar{n}_{i+1}m_{i+1} \ \text{ by definition in (5).}
\end{aligned}$$

This completes the proof.

Remark 4 In the proof of Theorem 2, if $2 \leq i \leq k$, then we show that $K_i = L_i(y_i)$, with

$$y_i^{\frac{n_i}{\hat{n}_i}} = (x-u)^{\frac{a_i}{\hat{n}_i}} w_i.$$

Here we essentially use the assumption that $a_i/\hat{n}_i$ is an integer. By Lemma 2 this means that $\hat{n}_i = \bar{n}_i m_i$ divides $a_i = \bar{n}_i a_i'$, which is equivalent to $m_i \mid a_i'$ (see (5) and (4)). Therefore the assumption in (12) of Theorem 2 is the strong assumption $m_2 = m_3 = \cdots = m_k = 1$. It is one of our main objectives to weaken this strong assumption to the case of Assumption 1. In Theorem 4 we fulfill this objective completely when $k = 2$. Its proof is more difficult than the proof of Theorem 2.

Next we give the analog of Theorem 2 for the place P_∞. First we introduce some notation that we use only in the following theorem. For $1 \leq i \leq k$, let $f_{i,1}(x)$ and $f_{i,2}(x)$ be the monic polynomials in $\mathbb{F}_q[x]$ and $c_i \in \mathbb{F}_q^*$ such that $\gcd(f_{i,1}(x), f_{i,2}(x)) = 1$ and

$$h_i(x) = c_i \frac{f_{i,1}(x)}{f_{i,2}(x)}.$$

Moreover let $d_{i,1}$ and $d_{i,2}$ be the degrees of $f_{i,1}(x)$ and $f_{i,2}(x)$, respectively; and let $d_i = d_{i,1} - d_{i,2}$. Replacing a_i by d_i in (3) and (5), we redefine $\bar{n}_i$, n_i' and $m_2, m_3, \ldots, m_k$. Furthermore replacing a_i to d_i in (11), we also redefine $\hat{n}_i$. The proof of the following theorem is similar to the proof of Theorem 2.

Theorem 3 *Under the notation as above, assume that the full constant field of E is $\mathbb{F}_q$ and $[E : \mathbb{F}_q(x)] = n_1 n_2 \cdots n_k$. Moreover assume that the integers $\hat{n_1}, \hat{n}_2, \ldots, \hat{n}_k$ divide $(q-1)$ and also that*

$$\hat{n}_2 \mid d_2, \ \ \hat{n}_3 \mid d_3, \ \ \ldots, \ \ \text{and} \ \ \hat{n}_k \mid d_k.$$

There exist either no or exactly $(\hat{n}_1 \hat{n}_2 \ldots \hat{n}_k)$ rational places of E over P_∞. There exists a rational place of E over P_∞ if and only if all of the following conditions hold

- *c_1 is an $\hat{n}_1$-power in $\mathbb{F}_q^*$,*
- *c_2 is an $\hat{n}_2$-power in $\mathbb{F}_q^*$,*
- $\vdots$
- *c_k is an $\hat{n}_k$-power in $\mathbb{F}_q^*$.*

4 Fibre products of two Kummer covers

In this section we give our results for $k = 2$ under Assumption 1. Before Theorem 4 we develop some tools that we use in its proof.

Proposition 1 *Let C_1, C_2 be subgroups of $\mathbb{F}_q^*$ with $|C_1| = \bar{n}_1$, $|C_2| = \bar{n}_2$. Let m be a positive integer with $m \mid (q-1)$ and N be an arbitrary integer. Let $\mathcal{S} = \{(x_1, x_2) \in C_1 \times C_2 : \text{ there exists } s \in \mathbb{F}_q^* \text{ such that } x_1^N x_2 = s^m\}$. Then the cardinality $|\mathcal{S}|$ of $\mathcal{S}$ is*

$$|\mathcal{S}| = \gcd(\bar{n}_1, N) \gcd\left(\frac{\bar{n_1}}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right) \gcd\left(\text{lcm}\ \left(\frac{\bar{n}_1}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right), \frac{q-1}{m}\right).$$

Moreover let C be the subset of $\mathbb{F}_q^*$ defined as

$$C = \left\{ y \in \mathbb{F}_q^* : \text{there exists } (x_1, x_2) \in C_1 \times C_2 \text{ and } s \in \mathbb{F}_q^* \text{ such that } y = x_1^N x_2 s^m \right\}.$$

Then C is a subgroup of $\mathbb{F}_q^*$ with the cardinality

$$|C| = \text{lcm}\ \left(\text{lcm}\ \left(\frac{\bar{n}_1}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right), \frac{q-1}{m}\right).$$

Proof Let $C_1^{(N)}$ be the subset of $\mathbb{F}_q^*$ defined as $C_1^{(N)} := \{c_1^N : c_1 \in C_1\}$. It is easy to observe that $C_1^{(N)}$ is a subgroup of $\mathbb{F}_q^*$ with

$$|C_1^{(N)}| = \frac{\bar{n}_1}{\gcd(\bar{n}_1, N)} \tag{20}$$

elements. Let $C_1^{(N)} C_2$ be the subset of $\mathbb{F}_q^*$ defined as

$$C_1^{(N)} C_2 = \{x_1^N x_2 : x_1 \in C_1, x_2 \in C_2\}.$$

Similarly, $C_1^{(N)}C_2$ is a subgroup of $\mathbb{F}_q^*$ with

$$|C_1^{(N)}C_2| = \text{lcm } (|C_1^{(N)}|, |C_2|). \tag{21}$$

Note that

$$\begin{aligned} \phi : C_1 \times C_2 &\longrightarrow \mathbb{F}_q^* \\ (x_1, x_2) &\longmapsto x_1^N x_2 \end{aligned}$$

is a group homomorphism from the Cartesian product group $C_1 \times C_2$ to $\mathbb{F}_q^*$. Moreover the image of ϕ is exactly the subgroup $C_1^{(N)}C_2$. Hence

$$|\text{Ker } \phi| = \frac{|C_1||C_2|}{|\text{Im } \phi|} = \frac{|C_1||C_2|}{|C_1^{(N)}C_2|} = \gcd(\bar{n}_1, N) \gcd\left(\frac{\bar{n}_1}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right) \tag{22}$$

where we use (20) and (21). Let M be the subset of $\mathbb{F}_q^*$ defined as

$$M := \{y \in \mathbb{F}_q^* : \text{ there exists } s \in \mathbb{F}_q^* \text{ such that } y = s^m\}.$$

It is clear that M is a subgroup of $\mathbb{F}_q^*$ with $|M| = \dfrac{q-1}{m}$. We observe that if $(x_1, x_2) \in C_1 \times C_2$ then

$$(x_1, x_2) \in \mathcal{S} \text{ if and only if } \phi(x_1, x_2) \in C_1^{(N)}C_2 \cap M. \tag{23}$$

Note that $C_1^{(N)}C_2 \cap M$ is a subgroup of $\mathbb{F}_q^*$ with cardinality

$$|C_1^{(N)}C_2 \cap M| = \gcd(|C_1^{(N)}C_2|, |M|) \tag{24}$$

Using (23) we obtain that $\mathcal{S}$ is exactly the preimage of the subgroup $C_1^{(N)}C_2 \cap M$ under the homomorphism ϕ. As $|M| = \dfrac{q-1}{m}$, combining (22) and (24) we determine the cardinality of $\mathcal{S}$.

It is not difficult to observe that the subset C in the hypothesis of the proposition is exactly $C_1^{(N)}C_2M$. This completes the proof.

In fact we can simplify the cardinality of $\mathcal{S}$ in Proposition 1. Before giving the simplification we need to prove the following lemma.

Lemma 3 *Let A be an arbitrary integer and m be a positive integer dividing $(q-1)$. If A divides $(q-1)$ then*

$$\gcd\left(A, \frac{q-1}{m}\right) = \frac{A}{m}\hat{m},$$

where $\hat{m}$ is the largest factor of m such that A divides $(q-1)/\hat{m}$.

Proof Assume that $A \mid (q-1)$. Then there exists $r \in \mathbb{Z}$ such that $A = \dfrac{q-1}{r}$. As $r \mid (q-1)$ and $m \mid (q-1)$ we know that lcm (r, m) also divides $(q-1)$. Then we have:

$$\gcd\left(A, \frac{q-1}{m}\right) = \gcd\left(\frac{q-1}{r}, \frac{q-1}{m}\right)$$

$$= \frac{q-1}{\text{lcm }(r,m)} = \frac{q-1}{rm}\gcd(r,m) = \frac{q-1}{\frac{q-1}{A}m}\gcd\left(\frac{q-1}{A}, m\right)$$

$$= \frac{A}{m}\gcd\left(\frac{q-1}{A}, m\right) = \frac{A}{m}\hat{m}.$$

This completes the proof.

Combining Proposition 1 and Lemma 3 we obtain the following Corollary:

Corollary 1 *Under the notations and assumptions of Proposition 1 we further define $\hat{m}$ as the largest factor of m such that A divides $(q-1)/\hat{m}$, where $A =$ lcm $\left(\dfrac{\bar{n}_1}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right)$. Then we have that $|\mathcal{S}| = \dfrac{\bar{n}_1\bar{n}_2}{m}\hat{m}$.*

Proof Using Proposition 1 and the definition of A as above, we have

$$|\mathcal{S}| = \gcd(\bar{n}_1, N)\gcd\left(\frac{\bar{n}_1}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right)\gcd\left(A, \frac{q-1}{m}\right) \tag{25}$$

As $\bar{n}_1 \mid (q-1)$, $\bar{n}_2 \mid (q-1)$, we have $A \mid (q-1)$. Using Lemma 3 and (25) we have:

$$|\mathcal{S}| = \gcd(\bar{n}_1, N)\gcd\left(\frac{\bar{n}_1}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right)\frac{A}{m}\hat{m}$$

$$= \gcd(\bar{n}_1, N)\gcd\left(\frac{\bar{n}_1}{\gcd(\bar{n}_1, N)}, \bar{n}_2\right)\frac{\text{lcm }\left(\frac{\bar{n}_1}{\gcd(\bar{n}_1,N)}, \bar{n}_2\right)}{m}\hat{m}$$

$$= \gcd(\bar{n}_1, N)\frac{\bar{n}_1\bar{n}_2}{\gcd(\bar{n}_1, N)}\frac{\hat{m}}{m} = \frac{\bar{n}_1\bar{n}_2}{m}\hat{m}.$$

This completes the proof.

The following theorem is one of our main results.

Theorem 4 *Under the notation as in Section 2, let $m_2 = \gcd(n_2', n_1')$ and $E = \mathbb{F}_q(x, y_1, y_2)$ be the algebraic function field with*

$$\begin{aligned} y_1^{n_1} &= h_1(x), \\ y_2^{n_2} &= h_2(x). \end{aligned} \tag{26}$$

Assume that the full constant field of E is $\mathbb{F}_q$ and $[E : \mathbb{F}_q(x)] = n_1n_2$. Moreover assume that $\bar{n}_1 \mid (q-1), \bar{n}_2 \mid (q-1)$ and Assumption 1 holds for the case $k = 2$. As $\gcd(n_1', a_1') = 1$, we choose integers A_1 and B_1 such that $A_1n_1' + B_1a_1' = 1$. Let

$$A = \text{lcm }\left(\frac{\bar{n}_1}{\gcd(-a_2'B_1, \bar{n}_1)}, \bar{n}_2\right).$$

Let $\hat{m}_2$ be the largest positive divisor of m_2 such that A divides $(q-1)/\hat{m}_2$. Then there exist either no or exactly $(\bar{n}_1\bar{n}_2\hat{m}_2)$ rational places of E over P_0. Furthermore, there exists a rational place of E over P_0 if and only if all of the following conditions hold:

C1: $f_1(u)$ is an $\bar{n}_1$-power in $\mathbb{F}_q$.

C2: $f_2(u)$ is an $\bar{n}_2$-power in $\mathbb{F}_q$.

C3: Assume that the conditions in items C1, C2 above hold and let $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$ such that $\alpha_1^{\bar{n}_1} = f_1(u)$ and $\alpha_2^{\bar{n}_2} = f_2(u)$. Let

$$B = \operatorname{lcm}\left(A, \frac{q-1}{m_2}\right).$$

Then

$$\left(\alpha_1^{-a_2' B_1}\alpha_2\right)^B = 1.$$

Proof Let $K_0 = \mathbb{F}_q(x)$. We divide the proof into three steps. In Step 1 we consider certain intermediate fields E_1, K_1 and E_2 with $K_0 \subseteq E_1 \subseteq K_1 \subseteq E_2 \subseteq E$ and the extensions E_1/K_0, K_1/E_1 and E_2/K_1 (see Figure 3). In Step 2 we consider an intermediate field F_2 with $E_2 \subseteq F_2 \subseteq E$ and the extension F_2/E_2 (see Figure 4). This is the main part of the proof. We use Corollary 1 in this part. In Step 3 we consider the extension E/F_2 and we complete the proof (see Figure 5).

Step 1

Let E_1 be the intermediate field with $K_0 \subseteq E_1 \subseteq E$ defined as

$$\begin{aligned} E_1 = K_0(z_1) \text{ and } \qquad & z_1^{\bar{n}_1} = (x-u)^{a_1} f_1(x), \\ \text{or equivalently} \qquad & \left(\frac{z_1}{(x-u)^{a_1'}}\right)^{\bar{n}_1} = f_1(x), \end{aligned} \tag{27}$$

where we use the facts that $\bar{n}_1$ divides a_1 and a_1' is the integer with $a_1'\bar{n}_1 = a_1$. The extension E_1/K_0 is Galois as $\bar{n}_1$ divides $(q-1)$. Let P_1 be an arbitrary place of E_1 over P_0 (see Figure 3). We have

$$\nu_{P_0}(x-u) = 1, \qquad \nu_{P_0}(f_1(x)) = 0, \qquad \gcd\left(\bar{n}_1, \nu_{P_0}(f_1(x))\right) = \bar{n}_1,$$

and hence the ramification index $e(P_1|P_0)$ is 1. Therefore there are either no or exactly $\bar{n}_1$ rational places of E_1 over P_0. Moreover P_1 is a rational place of E_1 if and only if the evaluation $f_1(u)$ of $f_1(x)$ at P_0 is an $\bar{n}_1$-power in $\mathbb{F}_q^*$. Hence from here till the end of the proof we assume that the condition C1 in the hypothesis of the theorem holds. Let P_1 be a rational place of E_1 over P_0.

Let K_1 be the intermediate field with $E_1 \subseteq K_1 \subseteq E$ defined as

$$K_1 = E_1(y_1) \qquad \text{and} \qquad y_1^{n_1'} = z_1. \tag{28}$$

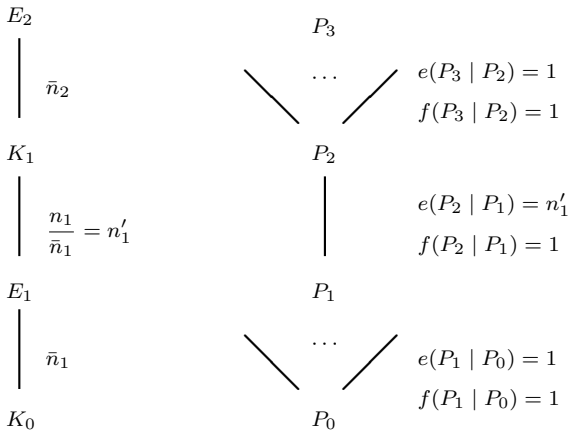

Fig. 3

Here the extension K_1/E_1 is not necessarily Galois. Let P_2 be an arbitrary place of K_1 over P_1 (see Figure 3). We have

$$\nu_{P_1}(x-u) = 1, \qquad \nu_{P_1}(z_1) = a_1',$$

and using (4) we obtain

$$\gcd\left(n_1', \nu_{P_1}(z_1)\right) = \gcd(n_1', a_1') = 1.$$

Therefore the ramification index $e(P_2|P_1)$ is n_1'. In particular $P_2|P_1$ is a total ramification, P_2 is the unique place of K_1 over P_1, and P_2 is a rational place of K_1. We further have that

$$\nu_{P_2}(x-u) = n_1', \quad \nu_{P_2}(y_1) = a_1', \quad \text{and} \quad \nu_{P_2}(z_1) = a_1' n_1'. \tag{29}$$

Let E_2 be the intermediate field with $K_1 \subseteq E_2 \subseteq E$ defined as

$$\begin{aligned} &E_2 = K_1(z_2) \text{ and } && z_2^{\bar{n}_2} = (x-u)^{a_2} f_2(x), \\ &\text{or equivalently} && \left(\frac{z_2}{(x-u)^{a_2'}}\right)^{\bar{n}_2} = f_2(x). \end{aligned} \tag{30}$$

The extension E_2/K_1 is a Galois extension. Let P_3 be an arbitrary place of E_2 over P_2 (see Figure 3). The extension E_2/K_1 is comparable to the extension E_1/K_0. We have

$$\nu_{P_2}(x-u) = n_1', \qquad \nu_{P_2}(f_2(x)) = 0, \qquad \gcd\left(\bar{n}_2, \nu_{P_2}(f_2(x))\right) = \bar{n}_2,$$

and hence the ramification index $e(P_3|P_2)$ is 1. There are either no or exactly $\bar{n}_2$ rational places of E_2 over P_2; and P_2 is a rational place of E_2 if and only if $f_2(u)$ is an $\bar{n}_2$-power in $\mathbb{F}_q^*$. Note that the evaluation of $f_2(x)$ at P_2 is equal to the evaluation of $f_2(x)$ at P_0. Hence from here till the end of the proof we also assume that condition C2 in the hypothesis of the theorem holds. Let P_2 be a rational place of E_2 over P_1. Using (29) we further obtain that

$$\begin{aligned} &\nu_{P_3}(x-u) = n_1', \nu_{P_3}(y_1) = a_1', \\ &\nu_{P_3}(z_1) = a_1' n_1', \text{ and } \quad \nu_{P_3}(z_2) = a_2' n_1'. \end{aligned} \tag{31}$$

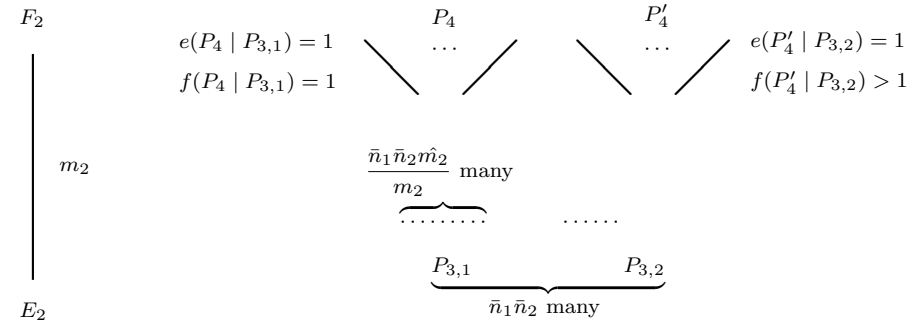

Fig. 4

Step 2

Let F_2 be the intermediate field with $E_2 \subseteq F_2 \subseteq E$ defined as

$$F_2 = E_2(w) \qquad \text{and} \qquad w^{m_2} = z_2. \tag{32}$$

The extension F_2/E_2 is Galois as m_2 divides $(q-1)$. Recall that, as we have already assumed that the conditions C1 and C2 hold, the number of rational places of E_2 over P_0 is $\bar{n}_1\bar{n}_2$. Let $\mathcal{T}$ be the set of rational places of E_2 over P_0. Recall also that α_1 and α_2 are the chosen elements of $\mathbb{F}_q^*$ with $\alpha_1^{\bar{n}_1} = f_1(u)$ and $\alpha_2^{\bar{n}_2} = f_2(u)$. Let P_3 be an arbitrary place in $\mathcal{T}$. Using (27), (30) and (31), for the evaluations

$$\beta_1 = \mathrm{Ev}_{P_3}\left(\frac{z_1}{(x-u)^{a_1'}}\right) \quad \text{and} \quad \beta_2 = \mathrm{Ev}_{P_3}\left(\frac{z_2}{(x-u)^{a_2'}}\right),$$

we conclude that $\beta_1^{\bar{n}_1} = f_1(u)$ and $\beta_2^{\bar{n}_2} = f_2(u)$. Let C_1 and C_2 be the subgroups of $\mathbb{F}_q^*$ with $|C_1| = \bar{n}_1$ and $|C_2| = \bar{n}_2$. Therefore we obtain that the map

$$\begin{aligned} \varphi : \mathcal{T} &\to C_1 \times C_2 \\ P_3 &\mapsto \left(\tfrac{1}{\alpha_1}\mathrm{Ev}_{P_3}\left(\tfrac{z_1}{(x-u)^{a_1'}}\right), \tfrac{1}{\alpha_2}\mathrm{Ev}_{P_3}\left(\tfrac{z_2}{(x-u)^{a_2'}}\right)\right) \end{aligned}$$

is a bijection between the set $\mathcal{T}$ and the cartesian product group $C_1 \times C_2$.

Now we state the main difficulty in Step 2. Note that in all the extensions in Step 1, the places over P_0 are all rational or all non-rational, depending on the conditions C1 and C2. We will see that this is not the case in the extension F_2/E_2 in general. Let $\mathcal{T}_1$ be the subset of $\mathcal{T}$ consisting of the places $P_3 \in \mathcal{T}$ such that there exists a rational place of F_2 over P_3. Let $\mathcal{T}_2 = \mathcal{T} \setminus \mathcal{T}_1$. A generic element of $\mathcal{T}_1$ is indicated as $P_{3,1}$ in Figure 4. Similarly a generic element of $\mathcal{T}_2$ is indicated as $P_{3,2}$ in Figure 4. We will prove that the cardinality of $\mathcal{T}_1$ is $\dfrac{\bar{n}_1\bar{n}_2\hat{m}_2}{m_2}$, where $\hat{m}_2$ is the positive integer defined in the hypothesis of the theorem.

Recall that A_1 and B_1 are the integers with $A_1n_1' + B_1a_1' = 1$. Let t be the element of E_2 given by

$$t = (x-u)^{A_1}y_1^{B_1}.$$

Let P_3 be an arbitrary element of $\mathcal{T}$. Using (31) we get

$$\nu_{P_3}(t) = A_1 n_1' + B_1 a_1' = 1.$$

In particular t is a local parameter of E_2 for all places in $\mathcal{T}$. Using (31) we also get that

$$\nu_{P_3}\left(\frac{z_2}{t^{n_1' a_2'}}\right) = 0.$$

Recall that m_2 divides n_1'. An alternative definition of F_2, which is equivalent to the one in (32) is

$$F_2 = E_2\left(\frac{w}{t^{a_2' \frac{n_1'}{m_2}}}\right) \quad \text{and} \quad \left(\frac{w}{t^{a_2' \frac{n_1'}{m_2}}}\right)^{m_2} = \frac{z_2}{t^{a_2' n_1'}}.$$

Hence $\mathcal{T}_1$ is exactly the subset of $\mathcal{T}$ consisting of $P_3 \in \mathcal{T}$ such that

$$\mathrm{Ev}_{P_3}\left(\frac{z_2}{t^{a_2' n_1'}}\right) \text{ is an } m_2\text{-power in } \mathbb{F}_q^*.$$

Let N be the integer $N = -B_1 a_2'$. We also have the following

$$\begin{aligned}
\frac{z_2}{t^{a_2' n_1'}} &= \frac{z_2}{(x-u)^{a_2'}} \frac{(x-u)^{a_2'}}{t^{a_2' n_1'}} = \frac{z_2}{(x-u)^{a_2'}} \frac{(x-u)^{a_2'(A_1 n_1' + B_1 a_1')}}{t^{a_2' n_1'}}, \\
&= \frac{z_2}{(x-u)^{a_2'}} \frac{(x-u)^{a_2'(A_1 n_1' + B_1 a_1')}}{(x-u)^{A_1 a_2' n_1'} y_1^{B_1 a_2' n_1'}} \quad \text{by definition of } t, \\
&= \frac{z_2}{(x-u)^{a_2'}} \frac{(x-u)^{B_1 a_1' a_2'}}{y_1^{B_1 a_2' n_1'}}, \qquad (33) \\
&= \frac{z_2}{(x-u)^{a_2'}} \left(\frac{(x-u)^{a_1'}}{z_1}\right)^{B_1 a_2'} \quad \text{by (28)}, \\
&= \frac{z_2}{(x-u)^{a_2'}} \left(\frac{z_1}{(x-u)^{a_1'}}\right)^{N} \quad \text{by definition of } N.
\end{aligned}$$

Let $\varphi(P_3) = (c_1, c_2)$. Then by definition of φ

$$\mathrm{Ev}_{P_3}\left(\frac{z_1}{(x-u)^{a_1'}}\right) = \alpha_1 c_1 \text{ and } \mathrm{Ev}_{P_3}\left(\frac{z_2}{(x-u)^{a_2'}}\right) = \alpha_2 c_2. \qquad (34)$$

Combining (33) and (34) we obtain that

$$\mathrm{Ev}_{P_3}\left(\frac{z_2}{t^{a_2' n_1'}}\right) = (\alpha_1 c_1)^N \alpha_2 c_2. \qquad (35)$$

Let $\widetilde{\mathcal{S}}$ be the subset of $C_1 \times C_2$ consisting of $(c_1, c_2) \in C_1 \times C_2$ such that $(\alpha_1 c_1)^N \alpha_2 c_2$ is an m_2-power in $\mathbb{F}_q^*$. Using (35) and the arguments above we conclude that $|\mathcal{T}_1| = |\widetilde{\mathcal{S}}|$. In fact φ also gives a bijection between $\mathcal{T}_1$ and $\widetilde{\mathcal{S}}$.

We determine $|\widetilde{\mathcal{S}}|$ using a related subset of $C_1 \times C_2$ and a related subset of $\mathbb{F}_q^*$. Let $\mathcal{S}$ be the subset of $C_1 \times C_2$ consisting of $(c_1, c_2) \in C_1 \times C_2$ such that $c_1^N c_2$ is an m_2-power in $\mathbb{F}_q^*$ (cf. Proposition 1 above). Let C be the subset of $\mathbb{F}_q^*$ consisting of $y \in \mathbb{F}_q^*$ such that there exist $(x_1, x_2) \in C_1 \times C_2$ and $s \in \mathbb{F}_q^*$ satisfying $y = x_1^N x_2 s^{m_2}$ (cf. Proposition 1). In fact C is a subgroup of $\mathbb{F}_q^*$ as proved in Proposition 1. We claim that $\widetilde{\mathcal{S}}$ is nonempty if and only if $\alpha_1^N \alpha_2 \in C$. Assume that $\widetilde{\mathcal{S}} \neq \emptyset$ and $(c_1, c_2) \in \widetilde{\mathcal{S}}$. Then there exists $s \in \mathbb{F}_q^*$ such that $(\alpha_1 c_1)^N \alpha_2 c_2 = s^{m_2}$. Therefore

$$\alpha_1^N \alpha_2 = \left(\frac{1}{c_1}\right)^N \frac{1}{c_2} s^{m_2},$$

and hence $\alpha_1^N \alpha_2 \in C$. Conversely if $\alpha_1^N \alpha_2 \in C$, then there exists $(x_1, x_2) \in C_1 \times C_2$ and $s \in \mathbb{F}_q^*$ such that $\alpha_1^N \alpha_2 = x_1^N x_2 s^{m_2}$. This implies that $\left(\frac{1}{x_1}, \frac{1}{x_2}\right) \in \widetilde{\mathcal{S}}$, and in particular $\widetilde{\mathcal{S}}$ is not empty. We further know the cardinality of the group C by Proposition 1. Therefore $|\mathcal{T}_1| \neq 0$ if and only if $\left(\alpha_1^N \alpha_2\right)^{|C|} = 1$, which is condition C3 of the hypothesis of the theorem. From here till the end of the proof we further assume that condition C3 in the hypothesis of the theorem holds.

Next we determine the cardinality $|\mathcal{T}_1|$. Let $(x_1, x_2) \in C_1 \times C_2$ and $s \in \mathbb{F}_q^*$ such that

$$\alpha_1^N \alpha_2 = x_1^N x_2 s^{m_2}.$$

Let θ be the map

$$\begin{aligned} \theta : \mathcal{S} &\to \widetilde{\mathcal{S}} \\ (c_1, c_2) &\mapsto \left(\frac{c_1}{x_1}, \frac{c_2}{x_2}\right). \end{aligned}$$

It is not difficult to observe that θ is a bijection between $\mathcal{S}$ and $\widetilde{\mathcal{S}}$. Using Corollary 1 we conclude that

$$|\mathcal{T}_1| = |\widetilde{\mathcal{S}}| = |\mathcal{S}| = \frac{\bar{n}_1 \bar{n}_2}{m_2} \hat{m}_2.$$

Let $P_{3,1}$ be a place of $\mathcal{T}_1$. Let P_4 be an arbitrary place F_2 over $P_{3,1}$ (see Figure 4). The extension F_2/E_2 is Galois, the ramification $e(P_4|P_{3,1})$ and the inertia $f(P_4|P_{3,1})$ indices are 1 and hence there are exactly m_2 rational places of F_2 over $P_{3,1}$. Therefore the number of rational places of F_2 over P_0 is

$$\left(\frac{\bar{n}_1 \bar{n}_2}{m_2} \hat{m}_2\right) m_2 = \bar{n}_1 \bar{n}_2 \hat{m}_2.$$

Furthermore we have

$$\begin{aligned} &\nu_{P_4}(x - u) = n_1', \ \nu_{P_4}(y_1) = a_1', \\ &\nu_{P_4}(z_2) = a_2' n_1', \ \text{ and } \quad \nu_{P_4}(w) = a_2' \frac{n_1'}{m_2}. \end{aligned} \tag{36}$$

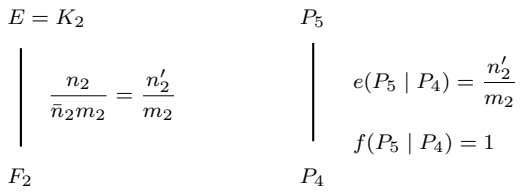

Fig. 5

Step 3

Let K_2 be the intermediate field defined as

$$K_2 = F_2(y_2) \qquad \text{and} \qquad y_2^{\frac{n_2'}{m_2}} = w.$$

It is not difficult to observe that $K_2 = E$. Moreover the extension K_2/F_2 is not necessarily Galois. Let P_5 be an arbitrary place of K_2 over P_4 (see Figure 5). Using (36), (4) and (5) we obtain that

$$\gcd\left(\frac{n_2'}{m_2}, \nu_{P_4}(w)\right) = \gcd\left(\frac{n_2'}{m_2}, a_2'\frac{n_1'}{m_2}\right) = 1.$$

Therefore the ramification index $e(P_5|P_4)$ is $\frac{n_2'}{m_2}$, $P_5|P_4$ is a total ramification; and P_5 is a rational place of K_2, which is also the unique place of K_2 over P_4. This completes the proof.

Remark 5 We compare Theorem 4 and Theorems 2.2 and 2.5 of [9] in this remark. We keep the notation of Theorem 4. One of the main conditions of Theorems 2.2 and 2.5 of [9] is $m_2\text{lcm}\,(\bar{n}_1, \bar{n}_2) \mid (q-1)$ (see [9, C3 in Theorem 2.2] and [9, D3 in Theorem 2.5]). We will show that

$$m_2\text{lcm}\,(\bar{n}_1, \bar{n}_2) \mid (q-1) \implies \hat{m}_2 = m_2. \tag{37}$$

Therefore there are either no or exactly $\bar{n}_1\bar{n}_2m_2$ rational places over P_0 (or P_∞) (see also Remark 7 below). The extra condition $m_2\text{lcm}\,(\bar{n}_1, \bar{n}_2) \mid (q-1)$ corresponds to a special subcase of Theorem 4, in which one does not need most of the tools developed for its proof. Therefore the proofs of Theorems 2.2 and 2.5 of [9] are much easier than the proof of Theorem 4 here. Now we show (37). As $m_2\text{lcm}\,(\bar{n}_1, \bar{n}_2) \mid (q-1)$ and A divides $\text{lcm}\,(\bar{n}_1, \bar{n}_2)$ by its definition, we get that $(m_2A) \mid (q-1)$ and hence $\hat{m}_2 = m_2$.

Remark 6 There is a mistake in the formulation of Theorems 2.2 and 2.5 of [9]. The condition C3 in the statement of Theorem 2.2 should be moved above. Namely the phrase "$\bar{n}_1, \bar{n}_2$ and m divide $q-1$" should be corrected to the phrase "$m\text{lcm}\,(\bar{n}_1, \bar{n}_2) \mid (q-1)$ and C3 should be removed form the list of the conditions. The same correction should be made for the condition D3 in Theorem 2.5 of [9].

Remark 7 Recall that in the end of Section 2, introducing the notation including c_i and d_i and redefining certain parameters by changing a_i to d_i, we have obtained the analog of Theorem 2 for the place P_∞ in Theorem 3. Theorem 3 uses c_i in its statement instead of $f_i(u)$. Similarly we obtain the analog of Theorem 4 for the place P_∞. We do not to state it explicitly here as it can be easily derived from Theorem 4 (see also [9, Theorems 2.2 and 2.5]).

5 Examples

In this section, using Theorem 4 and Remark 7, we obtain explicit examples of fibre products of Kummer extensions with many rational places. In particular Example 4 is a record; and Example 5 and Example 7 are new entries for the table in [12]. As also indicated in the homepage (http://www.science.uva.nl/~geer) of Prof. Dr. Gerard van der Geer, the tables in [2] were last updated on October 7, 2009 and the current updated table of curves with many points is in the website [12].

Throughout this section, for the algebraic function field E in the examples, $N(E)$ and $g(E)$ denote the number of rational places and the genus of the function field E, respectively.

Example 1 Let $E = \mathbb{F}_5(x, y_1, y_2)$ be the function field over $\mathbb{F}_5$ given by the following equations:

$$\begin{aligned} y_1^2 &= x(x^2 - 2) \\ y_2^2 &= x^3 - 2x^2 - x - 2 \end{aligned}$$

The genus of E is $g(E) = 4$ and $N(E) = 18$. This is the best value known in the table [12].

Example 2 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:

$$\begin{aligned} y_1^2 &= x(x^2 - 2) \\ y_2^2 &= x^3 - 2x^2 - x - 2 \\ y_3^2 &= x(x^4 + 2x^3 - 2x^2 - 2x + 2) \end{aligned}$$

The genus of E is $g(E) = 5$ and $N(E) = 20$. This is the best value known in the table [12].

Example 3 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:

$$\begin{aligned} y_1^2 &= x(x^2 - 2) \\ y_2^2 &= x^3 - 2x^2 - x - 2 \\ y_3^2 &= x^6 + 4x^4 + 3x^2 + 1 \end{aligned}$$

The genus of E is $g(E) = 13$ and $N(E) = 36$. This is the best value known in the table [12].

Example 4 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:

$$\begin{aligned} y_1^2 &= x(x^2 - 2) \\ y_2^2 &= x^3 - 2x^2 - x - 2 \\ y_3^2 &= x(x^4 + x^2 + 2) \end{aligned}$$

The genus of E is $g(E) = 15$ and $N(E) = 36$. This is a new record. In this case the best known lower bound is 35 in the table [12].

Example 5 Let $E = \mathbb{F}_{5^3}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{5^3}$ given by the following equations:

$$\begin{aligned} y_1^2 &= x^3 + x \\ y_2^2 &= x^3 + x + 2 \end{aligned}$$

The genus of E is $g(E) = 4$ and $N(E) = 170$. This is a new entry for the table [12].

Example 6 Let $E = \mathbb{F}_7(x, y_1, y_2)$ be the function field over $\mathbb{F}_7$ given by the following equations:

$$\begin{aligned} y_1^2 &= 1 + x^2 + 2x^3 + 6x^5 + x^6 \\ y_2^2 &= x^6 + 1 \end{aligned}$$

The genus of E is $g(E) = 9$ and $N(E) = 32$. This is the best value known in the table [12].

Example 7 Let $E = \mathbb{F}_{11^2}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{11^2}$ given by the following equations:

$$\begin{aligned} y_1^2 &= x^3 + x \\ y_2^{12} &= x^2(1 - x^2) \end{aligned}$$

The genus of E is $g(E) = 31$ and $N(E) = 612$. This is a new entry for the table [12].

Example 8 Let $E = \mathbb{F}_{13^2}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{13^2}$ given by the following equations:

$$\begin{aligned} y_1^2 &= x^7 + 1 \\ y_2^7 &= -x^7 - 1 \end{aligned}$$

The genus of E is $g(E) = 36$ and $N(E) = 1106$. This function field is maximal.

Acknowledgements The authors were partially supported by TÜBİTAK under Grant No. TBAG–109T672.

References

1. A. Garcia and A. Garzon, "On Kummer covers with many rational points over finite fields", *J. Pure Appl. Algebra*, vol. 185, pp. 177-192 (2003).
2. G. van der Geer, M. van der Vlugt, "Tables of curves with many points", *Math. Comput.*, vol. 69, no.230, pp.797-810 (2000)
3. J. W. P. Hirschfeld, Projective Geometries over Finite Fields, second ed., Oxford Mathematical Monographs. The Clarendon Press, Oxford Univ. Press, New York (1998)
4. J. W. P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics. Princeton Univ. Press, Princeton, NJ (2008)
5. M. Q. Kawakita, "Kummer curves and their fibre products with many rational points", *Appl. Algebra Engrg. Comm. Comput.*, vol. 14, pp. 55-64 (2003).
6. H. Niederreiter, C. Xing, Rational Points on Curves over Finite Fields, Cambridge University Press, Cambridge (2001).
7. H. Niederreiter, C. Xing, Algebraic geometry in coding theory and cryptography, Princeton Univ. Press, Princeton, NJ (2009).
8. F. Özbudak, H. Stichtenoth, "Curves with many points and configurations of hyperplanes over finite fields", *Finite Fields Appl.*, vol. 5, no 4, pp. 436-449 (1999).
9. F. Özbudak, B.G. Temür, "Fibre products of Kummer covers and curves with many rational points", *Appl. Algebra Engrg. Comm. Comput.*, vol. 18, pp. 433-443 (2007).
10. H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin (1993).
11. M. A. Tsfasman, S. G. Vlădut, D. Nogin, Algebraic geometric codes: basic notions, Mathematical Surveys and Monographs, 139. American Mathematical Society, Providence, RI (2007).
12. manypoints-Table of Curves with Many Points, http://www.manypoints.org (Accessed 03 November 2011).