AN EXHAUSTIVE COMPUTER SEARCH FOR FINDING NEW CURVES WITH MANY POINTS AMONG FIBRE PRODUCTS OF TWO KUMMER COVERS OVER $\mathbb{F}_5$ AND $\mathbb{F}_7$

FERRUH ÖZBUDAK, BURCU GÜLMEZ TEMÜR AND OĞUZ YAYLA

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

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

Oğuz Yayla
Institute of Applied Mathematics, Middle East Technical University,
Dumlupınar Bul., No:1, 06800, Ankara, Turkey
e-mail: yayla@metu.edu.tr

Abstract. We make an exhaustive computer search for finding new curves with many points among fibre products of two Kummer covers over $\mathbb{F}_5$ and $\mathbb{F}_7$. At the end of the search, we have 12 records and 6 new entries for the current tables [8]. In particular, we observe that a fibre product

$$y_1^3 = \frac{5(x+2)(x+5)}{x},\ y_2^3 = \frac{3x^2(x+5)}{x+3}$$

over $\mathbb{F}_7$ has genus 7 with 36 rational points. As this coincides with the Oesterlé bound, we conclude that the maximum number $N_7(7)$ of $\mathbb{F}_7$-rational points among all curves of genus 7 is 36. Our exhaustive search has been possible because of the methods given in [5] for determining the number of rational points of such curves. Using these methods, determining the rational points of such curves has been up to 10^7 times faster than the generic method of MAGMA.

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. If $\mathcal{C}$ is an absolutely irreducible, nonsingular and projective curve defined over $\mathbb{F}_q$, then the number N of $\mathbb{F}_q$-rational points of $\mathcal{C}$ is bounded by the well-known Hasse-Weil bound

$$N \leq q + 1 + 2g(\mathcal{C})\sqrt{q}. \tag{1.1}$$

where $g(\mathcal{C})$ denotes the genus of the curve $\mathcal{C}$. If the bound in (1.1) is attained and $g(\mathcal{C}) \geq 1$, then $\mathcal{C}$ is called a maximal curve.

Constructing explicit curves with many rational points has always been challenging as they have many applications in coding theory, cryptography and quasi-random points [2], [3], [4], [6], [7] etc. 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 $\mathbb{F}_q$. For $g \leq 50$ and small finite fields of characteristic $p = 2$ and $p = 3$, van der Geer and van der Vlugt collected the results of $N_q(g)$ in "Tables of Curves with Many Points" [1]. The tables were being updated in the web page of Prof. van der Geer up to October 7, 2009. Presently, together with their references, known upper and lower bounds for $N_q(g)$ (where $g \leq 50$ and $p < 100$) are being collected in "manyPoints-Table of Curves with Many Points" [8].

The theory of algebraic curves is essentially equivalent to the theory of algebraic function fields and throughout the paper we use the language of function fields [6]. We call a degree one place of an algebraic function field as a *rational place* (or *rational point*) of the function field. Let $n_1, n_2 \geq 2$ be integers, and $h_1(x)$ and $h_2(x) \in \mathbb{F}_q(x)$. Consider the fibre product

$$\begin{array}{rcl} y_1^{n_1} & = & h_1(x), \\ y_2^{n_2} & = & h_2(x). \end{array} \tag{1.2}$$

Let E be the algebraic function field $E = \mathbb{F}_q(x, y_1, y_2)$ with the system of equations in (1.2). If the number of rational places of E is more than $N_{max,q,g}/\sqrt{2}$, where $N_{max,q,g}$ is the best known upper bound for $N_q(g)$ (Hasse-Weil, Serre, Ihara, Oesterlé etc.)- this is the case if there is no entry for the lower bound in the tables [8]- then we call it a *new entry*. If the number of rational places of E is more than the existing lower bound in the tables [8], then we call it a *record*.

In this paper, we made an exhaustive search on n_1, n_2, h_1 and h_2 to find such function fields $E = \mathbb{F}_q(x, y_1, y_2)$ with many rational places over the finite fields $\mathbb{F}_5$ and $\mathbb{F}_7$. We used the method given in [5] to determine the number of rational places of E over $\mathbb{F}_q$ (see also Section 4). We implemented this method in Algorithm 1 in Section 2. At the end of the search, we have 12 records and 6 new entries for the current tables [8] presented in the Tables 1, 2 and 3. Furthermore, we observe that this method for determining the number of rational points of E is upto 10^7 faster than the generic method available in MAGMA [9] (see Tables 4 and 5).

The paper is organized as follows. In Section 2 we explain the details of how we executed the search and give our records and new entries. In Section 3 we compare the implemented counting method of rational places with the method available in MAGMA. In Section 4 we give some background information about fibre products of Kummer covers that our Algorithm 1 depends on.

2. Implementation and Results

Let n_1 and $n_2 \geq 2$ be integers, and $h = (h_{1,1}(x), h_{1,2}(x), h_{2,1}(x), h_{2,2}(x))$ be tuple of polynomials defined over $\mathbb{F}_q$. Let $E_{q,n_1,n_2,h}$ be algebraic function field $E_{q,n_1,n_2,h} = \mathbb{F}_q(x, y_1, y_2)$ with the system of equations of the fibre product

$$y_1^{n_1} = \frac{h_{1,1}(x)}{h_{1,2}(x)},\ y_2^{n_2} = \frac{h_{2,1}(x)}{h_{2,2}(x)}. \tag{2.1}$$

We will assume that $[E_{q,n_1,n_2,h} : \mathbb{F}_q(x)] = n_1 n_2$ and the full constant field of $E_{q,n_1,n_2,h}$ is $\mathbb{F}_q$.

We use the method presented in [5] for counting rational places of $E_{q,n_1,n_2,h}$ to obtain algebraic function fields with many rational places (see Section 4, Theorem 4.1). To begin with, we observed experimentally that counting rational places by this method (i.e. by using Theorem 4.1) is much faster than generic calculation method available in MAGMA [9]. Namely, this method calculates number of rational places up to 10^7 times faster than the method *NumberOfDegreeOnePlacesOverExactConstantField* of MAGMA over $q = 7$ for $n_1 = n_2 = 6$ and $\deg h_{1,1} = 3$, $\deg h_{1,2} = 1$, $\deg h_{2,1} = 3$, $\deg h_{2,2} = 1$ (see Table 4). According to this observation, we made a search for algebraic function fields with many rational places over $\mathbb{F}_5$ and $\mathbb{F}_7$ by using the method given in [5].

We define finite set $S_{q,d}$ of polynomials over $\mathbb{F}_q$ for an integer d as follows

$$S_{q,d} = \{(h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2}) : \sum_{i,j} deg(h_{i,j}) \leq d,\ gcd(h_{i,1}, h_{i,2}) = 1, i = 1, 2\}.$$

And, we define search set $E_{q,d}$ of possible algebraic function fields as

$$E_{q,d} = \{E_{q,n_1,n_2,h} : h \in S_{q,d}, 2 \leq n_1, n_2 \leq q - 1\}.$$

Before we present our results, we state the next fact which reduces set of possible algebraic function fields having many rational places.

Lemma 2.1. *Let $E_{q,n_1,n_2,h}$ and $E'_{q,n_1,n_2,h'}$ be two algebraic function fields defined as in (2.1) for tuples of polynomials $h = (h_{1,2}, h_{1,1}, h_{2,1}, h_{2,2})$ and $h' = (h'_{1,1}, h'_{1,2}, h'_{2,1}, h'_{2,2})$. $E_{q,n_1,n_2,h}$ and $E'_{q,n_1,n_2,h'}$ are equivalent algebraic function field definitions if one of the equalities holds:*

i. $(h'_{1,1}, h'_{1,2}, h'_{2,1}, h'_{2,2}) = (h_{1,2}, h_{1,1}, h_{2,1}, h_{2,2})$
ii. $(h'_{1,1}, h'_{1,2}, h'_{2,1}, h'_{2,2}) = (h_{1,2}, h_{1,1}, h_{2,2}, h_{2,1})$
iii. $(h'_{1,1}, h'_{1,2}, h'_{2,1}, h'_{2,2}) = (h_{1,1}, h_{1,2}, h_{2,2}, h_{2,1})$

iv. $(h'_{1,1}, h'_{1,2}, h'_{2,1}, h'_{2,2}) = (c_1h_{1,1}, c_1h_{1,2}, c_2h_{2,1}, c_2h_{2,2})$, *for* c_1 *and* c_2 *in* $\mathbb{F}_q$.

Proof. Assume the equality in the first case holds. As $E'_{q,n_1,n_2,h'}$ is defined as $E'_{q,n_1,n_2,h'} = \mathbb{F}_q(x, \frac{1}{y_1}, y_2)$, and $\mathbb{F}_q(x, \frac{1}{y_1}, y_2)$ is an equivalent definition of the function field $E_{q,n_1,n_2,h}$, we have the equality of function fields $E_{q,n_1,n_2,h} = E'_{q,n_1,n_2,h}$. The proof of other cases is similar. Therefore, we complete the proof. □

By using Lemma 2.1, we reduce set $E_{q,d}$ to $E'_{q,d}$

$$E'_{q,d} = \{E_{q,n_1,n_2,h} : h \in S'_{q,d}, 2 \le n_1, n_2 \le q-1\},$$

where $S'_{q,d}$ defined as

$$S'_{q,d} = \{h \in S_{q,d} : degh_{1,1} \ge degh_{1,2},\ degh_{2,1} \ge degh_{2,2}\}$$

for monic polynomials $h_{1,2}$ and $h_{2,2}$.

Algorithm 1 Search for algebraic function fields with many rational places

Input: *Table* available in [8] and parameters q, d.
Output: Sets of *Records*, *New Entries* and *Best Known Results*.

Define $N_{max,q,g}$ (resp. $N_{min,q,g}$) as the best known upper (resp. lower) bound for $N_q(g)$ given in *Table*. And, set $N_{min,q,g} = 0$ if there exists no result for $N_{min,q,g}$ in *Table*.
Initialize sets *RecordsNewEntries* $= \{\}$ and *BestKnownResults* $= \{\}$.
for $E_{q,n_1,n_2,h}$ in $E''_{q,d}$ **do**
  Find genus g of $E_{q,n_1,n_2,h}$ by Proposition 4.2.
  if $g \ge 1$ **then**
    Find number of rational places N of $E_{q,n_1,n_2,h}$ by Theorem 4.1.
    if $N > \frac{N_{max,q,g}}{\sqrt{2}}$ **then**
      if $N \ge N_{min,q,g}$ **then**
        if $E_{q,n_1,n_2,h}$ defines an algebraic function field **then**
          if full constant field of $E_{q,n_1,n_2,h}$ is $\mathbb{F}_q$ **then**
            if extension degree satisfies $[E_{q,n_1,n_2,h} : \mathbb{F}_q(x)] = n_1n_2$ **then**
              if $N > N_{min,q,g}$ **then**
                Save $E_{q,n_1,n_2,h}$ into the set *RecordsNewEntries*.
              else
                Save $E_{q,n_1,n_2,h}$ into the set *BestKnownResults*.
              end if
            end if
          end if
        end if
      end if
    end if
  end if
end for
return *RecordsNewEntries* and *BestKnownResults*

Furthermore, we restricted the search on function fields $E_{q,n_1,n_2,h}$ satisfying $n_1 \mid q-1$ or $n_2 \mid q-1$. In addition, we assume that $degh_{1,1} \geq 1$ and $degh_{2,1} \geq 1$ as these cases correspond to the case $k=1$. Therefore, we restrict set $E'_{q,d}$ to $E''_{q,d}$ defined as

$$E''_{q,d} = \{E_{q,n_1,n_2,h} : h \in S''_{q,d}, n_1 \mid q-1,\ n_2 \mid q-1\},$$

where set $S''_{q,d}$ is defined as

$$S''_{q,d} = \{h \in S'_{q,d} : degh_{1,1} \geq 1,\ degh_{2,1} \geq 1\}.$$

We explain the steps of our exhaustive search method over $E''_{q,d}$ for algebraic function fields with many rational places in Algorithm 1. We implemented Algorithm 1 for $q=5$ and $q=7$, and we present the the results below.

2.1. $\mathbb{F}_5$**.** We made an exhaustive search over the set

$$E''_{5,10} = \{E_{5,n_1,n_2,h} : h \in S''_{5,10}, n_1 \mid 4,\ n_2 \mid 4\}$$

by using Algorithm 1. In addition, we observed experimentally while searching on $E''_{5,10}$ that algebraic function fields defined as $E_{5,4,4,h}$ for some h are very likely to have many rational places. So, we extended the search to include polynomials $h_{1,1}(x), h_{1,2}(x), h_{2,1}(x)$ and $h_{2,2}(x)$ satisfying

$$degh_{1,1} + degh_{1,1} + degh_{1,1} + degh_{1,1} = 11$$

for $n_1 = 4$ and $n_2 = 4$ Then we observed 4 records for the table [8]. We present examples of records in Table 1, where N and g denote the number of rational places and genus of $E_{5,n_1,n_2,h}$ for $h = (h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2})$.

Remark 2.2. We remark that algebraic function fields over $\mathbb{F}_q$ defined with equations having degrees greater than $q-1$ may have many rational places with respect to their lower degree counter parts. For instance, function field $E_{5,4,4,h_1}$ defined over $\mathbb{F}_5$ as

$$y_1^4 = \frac{x^6 + 3x^4 + 4x^3 + x^2 + 2x + 2}{x+2},\ y_2^5 = 3x^4 + 4x^3 + 2x^2 + x + 1$$

has genus 29 and 64 rational places. On the other hand, function field $E_{5,4,4,h_2}$ defined over $\mathbb{F}_5$ as

$$y_1^4 = \frac{x^2 + 3x^4 + 4x^3 + x^2 + 2x + 2}{x+2},\ y_2^5 = 3x^4 + 4x^3 + 2x^2 + x + 1$$

has genus 45 and 64 rational places. The former has many rational places, in fact an example of a record for the table [8]; but the later does not. Therefore, even $E_{5,4,4,h_1}$ consists of a polynomial having degree bigger than the polynomial occurring in $E_{5,4,4,h_2}$, $E_{5,4,4,h_1}$ has smaller genus. This also implies that it is required to search function fields consisting of polynomials whose degrees are greater than $q-1$.

Table 1. Algebraic function fields with many rational places over $\mathbb{F}_5$ (Records)

n_1	n_2	$h_1(x) = \frac{h_{1,1}(x)}{h_{1,2}(x)}$	$h_2(x) = \frac{h_{2,1}(x)}{h_{2,2}(x)}$	g	N	$N_{min,q,g}$
2	2	$\frac{3x^3+2x^2+2x+1}{x^2+2x+4}$	$\frac{2x^3+4x^2+1}{x^2+2x+4}$	6	22	21
4	4	$\frac{(x)(x^2+x+2)}{x+4}$	$\frac{(x+4)(x^2+2x+4)}{x}$	25	56	52
4	4	$\frac{(x+4)(x^2+4x+2)}{x+3}$	$\frac{4(x+4)(x^2+3x+4)}{(x+3)^2}$	27	56	52
4	4	$\frac{x^6+3x^4+4x^3+x^2+2x+2}{x+2}$	$\frac{3x^4+4x^3+2x^2+x+1}{1}$	29	64	52

2.2. $\mathbb{F}_7$. We made an exhaustive search over the set

$$E''_{7,8} = \{E_{7,n_1,n_2,h} : h \in S''_{7,8}, n_1 \mid 6,\ n_2 \mid 6\}$$

by using Algorithm 1. Then we observed 8 records and 6 new entries for the table [8]. We present results within two tables. Tables 2 and 3 consist of examples of our results which are records and new entries according to the table [8], respectively.

Table 2. Algebraic function fields with many rational places over $\mathbb{F}_7$ (Records)

n_1	n_2	$h_1(x) = \frac{h_{1,1}(x)}{h_{1,2}(x)}$	$h_2(x) = \frac{h_{2,1}(x)}{h_{2,2}(x)}$	g	N	$N_{min,q,g}$
3	2	$\frac{4x^2+4x+5}{1}$	$\frac{2(x^2+x+3)(x^2+3x+1)}{1}$	5	26	24
2	3	$\frac{6(x+6)(x^2+1)}{1}$	$\frac{4(x+5)(x^2+1)^2}{1}$	6	27	25
3	3	$\frac{5(x+2)(x+5)}{x}$	$\frac{3x^2(x+5)}{x+3}$	7	36	30
3	3	$\frac{x^2+1}{x}$	$\frac{x^2+4}{1}$	10	39	36
3	6	$\frac{6(x^2+1)}{1}$	$\frac{(x+1)(x+6)^2}{x+5}$	16	54	45
2	6	$\frac{6(x+3)(x^2+x+3)}{1}$	$\frac{4(x+3)^2(x^2+3x+6)}{x+2}$	18	52	51
3	6	$\frac{x(x+1)}{x+4}$	$\frac{(x+4)^3}{x(x+5)}$	19	63	54
6	6	$\frac{3x^2(x+1)}{x+3}$	$\frac{2x(x+1)(x+3)}{x+1}$	22	72	63

Table 3. Algebraic function fields with many rational places over $\mathbb{F}_7$ (New Entries)

n_1	n_2	$h_1(x) = \frac{h_{1,1}(x)}{h_{1,2}(x)}$	$h_2(x) = \frac{h_{2,1}(x)}{h_{2,2}(x)}$	g	N	$\lceil \frac{N_{max,q,g}}{\sqrt{2}} \rceil$
2	6	$\frac{6(x+3)(x^2+x+3)}{1}$	$\frac{4x^2(x^2+x+3)}{x+5}$	14	44	41
2	6	$\frac{2(x+3)(x+4)(x+6)}{1}$	$\frac{3(x+3)^2(x^2+2x+3)}{x+4}$	15	52	43
2	6	$\frac{4(x+2)(x^2+4)}{1}$	$\frac{2(x+2)^2(x+5)(x^2+x+3)}{1}$	20	54	53
3	6	$\frac{6(x+6)(x^2+6x+4)}{x+4}$	$\frac{3(x+6)^2(x^2+5x+5)}{1}$	28	72	68
6	6	$\frac{3x(x+2)(x+3)}{1}$	$\frac{6x^2(x+4)}{(x+3)^2}$	40	108	90
6	6	$\frac{4(x+1)(x+5)(x+6)}{1}$	$\frac{3(x+6)^2(x^2+4x+5)}{x+1}$	49	114	107

Remark 2.3. Algebraic function field $E_{7,3,3,h}$, $h = (5(x+2)(x+5), x, 3x^2(x+5), x+3)$ having 36 rational places is not only a record for $N_7(7)$, but also it attains the best known upper bound (i.e. Oesterlé bound) for $N_7(7)$. We also note that we observed many such examples for $N_7(7)$.

3. Comparison

Let E be the algebraic function field $E = \mathbb{F}_q(x, y_1, y_2)$ with the system of equations in (1.2) In this section, we compare time consumption of the counting method of rational places of E given in [5] with the method available in MAGMA [9] (namely, with the command *NumberOfPlacesOfDegreeOneOverExactConstantField*). Furthermore, we compare genus calculation of E by using Proposition 4.2 with the generic genus calculation method available in MAGMA (namely, with the command *Genus*). Finally, we compare time consumption necessary for searching for algebraic function fields with many rational places, where search algorithms are designed with our methods and with the methods available in MAGMA.

Firstly, we randomly choose 100 tuples $(h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2})$ of polynomials over $\mathbb{F}_q[x]$ of degrees $degh_{1,1} = 3$, $degh_{1,2} = 1$, $degh_{2,1} = 3$, $degh_{2,2} = 1$ for $q \in \{5, 7\}$. In order to see the difference better we perform the algorithms for two distinct n_i, $i = 1, 2$ values. Namely, we measure the time consumption of the algorithms mentioned above for $n_i = q - 1$, $i = 1, 2$ and for $n_i = 2$, $i = 1, 2$. We present the results in Tables 4 and 5.

Table 4. Time Consumption: $n_1 = n_2 = q - 1$ (seconds)

	$q = 5$	$q = 7$
Number of rational points by Theorem 4.1	0,030	0,050
Number of rational points by MAGMA	2963,672	1875784,390
Genus by Proposition 4.2	0,015	0,020
Genus by MAGMA	2630,777	1838117,550
Search by Theorem 4.1 and Proposition 4.2	0,045	0,070
Search by MAGMA	2983,327	1865715,560

Table 5. Time Consumption: $n_1 = n_2 = 2$ (seconds)

	$q = 5$	$q = 7$
Number of rational points by Theorem 4.1	0,030	0,050
Number of rational points by MAGMA	5,635	7,300
Genus by Proposition 4.2	0,015	0,020
Genus by MAGMA	24,490	6,170
Search by Theorem 4.1 and Proposition 4.2	0,042	0,050
Search by MAGMA	5,765	10,050

As it is seen from implementation results given in tables that the method given in [5] is faster than MAGMA for any case. On the other hand, for larger n_i, $i = 1, 2$ values the method given in [5] is much faster than MAGMA. In other words, increasing n_i, $i = 1, 2$ values affects the speed of MAGMA functions more than increasing finite field size.

4. An Explanation of the Method

In this section, we briefly explain the method given in [5] which enables us to determine the exact number of rational places of fibre products of two Kummer covers of the projective line over finite fields $\mathbb{F}_q$. And, we state a proposition for calculation of their genus.

For each element $u \in \mathbb{F}_q$, let P_0 denote the rational place of $\mathbb{F}_q(x)$ which corresponds to the zero of $(x - u)$ and similarly let P_∞ denote the rational place of the rational function field $\mathbb{F}_q(x)$ corresponding to the pole of x. Furthermore the evaluation of $f_i(x)$ at P_0 is denoted by $f_i(u)$ for $i = 1, 2$.

For $i = 1, 2$, we write $h_i(x)$ in (1.2) in the following form:

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

where $a_i \in \mathbb{Z}$ and $f_i(x) \in \mathbb{F}_q(x)$. In this setting, a_i and $f_i(x)$ are uniquely determined.

For $1 \le i \le 2$, let $\bar{n}_i$, n'_i and a'_i be the integers:

$$\bar{n}_i = \gcd(n_i, a_i), \qquad n'_i = \frac{n_i}{\bar{n}_i}, \qquad \text{and} \qquad a'_i = \frac{a_i}{\bar{n}_i}. \tag{4.1}$$

When we define n'_i and a'_i as above we get that

$$\gcd(n'_i, a'_i) = 1 \quad \text{for } 1 \le i \le 2. \tag{4.2}$$

Note that if $a_i = 0$, then $n'_i = 1$. We define

The following theorem is the main result used in our computer search.

Theorem 4.1. [5] *Let $m_2 = \gcd(n'_2, n'_1)$ and $E = \mathbb{F}_q(x, y_1, y_2)$ be the algebraic function field with*

$$\begin{aligned} y_1^{n_1} &= h_1(x), \\ y_2^{n_2} &= h_2(x). \end{aligned} \tag{4.3}$$

Assume that the full constant field of E is $\mathbb{F}_q$ and $[E : \mathbb{F}_q(x)] = n_1 n_2$. Moreover assume that $\bar{n}_1 \mid (q-1), \bar{n}_2 \mid (q-1)$ and $m_2 \mid (q-1)$. As $\gcd(n'_1, a'_1) = 1$, we choose integers A_1 and B_1 such that $A_1 n'_1 + B_1 a'_1 = 1$. Let

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

Let $\hat{m}_2 = \gcd\left(\frac{q-1}{A}, m_2\right)$. 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

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

One can also state a similar theorem for the number of rational places lying over P_∞ (see [5, Remark 5]).

Next, we represent the genus computation for fibre products of two Kummer covers over finite fields $\mathbb{F}_q$.

Here we assume that the full constant field of E is $\mathbb{F}_q$, $[E : \mathbb{F}_q(x)] = n_1 n_2$ and $\gcd(n_1, q) = \gcd(n_2, q) = 1$. We compute the genus $g(E)$ of E using Hurwitz Genus Formula (see Theorem 3.4.12 in [6]) and Abyhankar's Lemma (see Proposition 3.8.9 in [6]). Let F_1 and F_2 be the intermediate fields $\mathbb{F}_q(x) \subseteq F_i \subseteq E$ where $F_i = \mathbb{F}_q(x, y_i)$ for $i = 1, 2$. Let $\bar{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. Let $E' = E\bar{\mathbb{F}}_q$, $F_1' = F_1\bar{\mathbb{F}}_q$ and $F_2' = F_2\bar{\mathbb{F}}_q$ be the constant field extensions of E, F_1 and F_2, respectively. It is well known that the full constant field of E', F_1' and F_2' is $\bar{\mathbb{F}}_q$ (see Proposition 3.6.1 in [6]). Furthermore, the genus $g(E')$ of E' is the same as the genus $g(E)$ of E (see Theorem 3.6.3 in [6]) and E' is the compositum $F_1'F_2'$ of F_1' and F_2'. Note that E' is an extension of the rational function field $\bar{\mathbb{F}}_q(x)$ and $[E' : \bar{\mathbb{F}}_q(x)] = [E : \mathbb{F}_q(x)] = n_1 n_2$. For a place P of the rational function field $\bar{\mathbb{F}}_q(x)$ and a place Q of E' lying over P, let $d(Q|P)$ denote the different exponent of Q over P. Using Hurwitz Genus Formula, for the genus $g(E')$ of E' (and hence for g(E)) we obtain that

$$2g(E) - 2 = 2g(E') - 2 = n_1 n_2(-2) + \sum_{P}\sum_{Q|P} d(Q|P) \deg Q, \tag{4.4}$$

where P runs through the places of $\bar{\mathbb{F}}_q(x)$ which are ramified in the extension $E'/\bar{\mathbb{F}}_q(x)$ and Q runs through the places of E' lying over P.

Suppose that $h_1(x)$ and $h_2(x)$ are factorized into linear polynomials over $\bar{\mathbb{F}}_q$ as follows:

$$\begin{aligned} h_1(x) &= c_1\frac{h_{1,1}(x)}{h_{1,2}(x)} = \frac{r_1(x)r_2(x)\cdots r_a(x)}{s_1(x)s_2(x)\cdots s_b(x)}, \\ h_2(x) &= c_2\frac{h_{2,1}(x)}{h_{2,2}(x)} = \frac{u_1(x)u_2(x)\cdots u_m(x)}{v_1(x)v_2(x)\cdots v_n(x)} \end{aligned}$$

where $c_i \in \mathbb{F}_q^*$, r_i, s_j, u_k, v_l are monic degree one polynomials in $\bar{F}_q[x]$ with $\gcd(r_i, s_j) = 1$ for $i = 1, 2$. We determine $d(Q|P)$ using Abhyankar's Lemma in each case and get the following Proposition for computing the genus.

Proposition 4.2. *Let $F_1 = \mathbb{F}_q(x, y_1)$ and $F_2 = \mathbb{F}_q(x, y_2)$ be the algebraic function fields with $y_1^{n_1} = h_1(x) = \frac{h_{1,1}(x)}{h_{1,2}(x)}$ and $y_2^{n_2} = h_2(x) = \frac{h_{2,1}(x)}{h_{2,2}(x)}$ respectively, where $h_{1,1}(x), h_{1,2}(x), h_{2,1}(x), h_{2,2}(x) \in \mathbb{F}_q[x]$ then the compositum $F_1F_2 = E = \mathbb{F}_q(x, y_1, y_2)$ and the genus $g(E)$ of E is equal to:*

$$\begin{aligned} g(E) &= 1 - n_1n_2 + \tfrac{1}{2}n_1n_2\left(1 - \frac{1}{\operatorname{lcm}\left(\frac{n_1}{\gcd(n_1,|d_1|)}, \frac{n_2}{\gcd(n_2,|d_2|)}\right)}\right) \\ &+ \tfrac{1}{2}n_1n_2 \sum_{p(x)\in R}\left(1 - \frac{1}{\operatorname{lcm}\left(\frac{n_1}{\gcd(n_1,a_{p,1})}, \frac{n_2}{\gcd(n_2,a_{p,2})}\right)}\right)\deg(p(x)). \end{aligned}$$

where $d_1 = \deg h_{1,2}(x) - \deg h_{1,1}(x)$, $d_2 = \deg h_{2,2}(x) - \deg h_{2,1}(x)$, R is the set of all irreducible polynomials in the polynomial ring $\mathbb{F}_q[x]$ and $a_{p,i}$ is the multiplicity of $p(x) \in R$ as a zero or pole of $h_i(x)$ for $i = 1, 2$. If $p(x) \in R$ is neither a zero nor a pole of $h_i(x)$ then obviously $a_{p,i} = 0$ and the summation is finite as each rational function has finitely many zeros and poles.

The proposition can be proved using Proposition 3.7.3 in [6] on Kummer extensions and Abhyankar's lemma (see Proposition 3.8.9 in [6]). We also refer to [5, Example 1] for some details.

We note that calculation of the genus by this proposition is also much faster than generic calculation of the genus by MAGMA (see Table 4).

Acknowledgments. The authors are partially supported by TÜBİTAK under Grant No. TBAG–109T672.

References

[1] G. van der Geer, M. van der Vlugt, "Tables of curves with many points", *Math. Comput.*, vol. 69, no.230, pp.797-810 (2000)

[2] 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)

[3] H. Niederreiter, C. Xing, Rational Points on Curves over Finite Fields, Cambridge University Press, Cambridge (2001).

[4] H. Niederreiter, C. Xing, Algebraic geometry in coding theory and cryptography, Princeton Univ. Press, Princeton, NJ (2009).

[5] F. Özbudak, B.G. Temür, "Finite number of fibre products of Kummer covers and curves with many rational points over finite fields", *Designs, Codes and Cryptography*, accepted.

[6] H. Stichtenoth, Algebraic Function Fields and Codes, Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin (2009).

[7] M. A. Tsfasman, S. G. Vlǎdut, D. Nogin, Algebraic geometric codes: basic notions, Mathematical Surveys and Monographs, 139. American Mathematical Society, Providence, RI (2007).

[8] manypoints-Table of Curves with Many Points, http://www.manypoints.org (Accessed May 24, 2012).

[9] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.*, 24, 235-265 (1997).