Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2013) 37: 908 – 913
© TÜBİTAK
doi:10.3906/mat-1206-26

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,[1] **Burcu GÜLMEZ TEMÜR,**[2] **Oğuz YAYLA**[3,*]
[1]Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bulvarı, No: 1, 06800, Ankara, Turkey
[2]Department of Mathematics, Atılım University, İncek, Gölbaşı, 06836, Ankara, Turkey
[3]Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bulvarı, No:1, 06800, Ankara, Turkey

Received: 13.06.2012 • **Accepted:** 19.10.2012 • **Published Online:** 23.09.2013 • **Printed:** 21.10.2013

Abstract: In this paper we make an exhaustive computer search for finding new curves with many points among fibre products of 2 Kummer covers of the projective line 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 Table of Curves with Many Points. In particular, we observe that the 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 Ihara 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 the recent work by Özbudak and Temür (2012) for determining the number of rational points of such curves.

Key words: 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 [3, 7, 8, 16, 17]. In this paper, we consider fibre products of 2 Kummer covers having many points. Some types of fibre products of Kummer covers of the projective line were studied and such explicit curves with many points were found [2, 5, 9, 10]. There are also

*Correspondence: yayla@metu.edu.tr
2010 *AMS Mathematics Subject Classification:* Primary 14H05, 94B27; Secondary 11R58, 14Q05.

recent studies on searching for new curves with many points by using methods from class field theory; see for instance [12, 13, 14, 15, 19].

We denote $N_q(g)$ as the maximum number of $\mathbb{F}_q$-rational points among the absolutely irreducible, nonsingular, and projective curves of genus g defined over $\mathbb{F}_q$. Together with their references, the best 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" [6].

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 [16]. We call a degree one place of an algebraic function field 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). Let g be the genus of E. Assume that $[E : \mathbb{F}_q(x)] = n_1 n_2$, and the full constant field of E is $\mathbb{F}_q$.

Let $\mathrm{UpperN}_q(g)$ be the best known upper bound for $N_q(g)$ (see also [6]). There is an entry for a lower bound of $N_q(g)$ in the tables [6] only if the existence of a curve of genus g with the number of rational points greater than $\mathrm{UpperN}_q(g)/\sqrt{2}$ is known. Otherwise the lower bound in tables [6] for q and g is empty. If there is no entry for the lower bound of $N_q(g)$ in the tables [6] and the number of rational points of E is greater than $\mathrm{UpperN}_q(g)/\sqrt{2}$, then we call it a *new entry*. If the number of rational places of E is greater than the existing lower bound in the tables [6], 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 [11] to determine the number of rational places of E over $\mathbb{F}_q$ (see also Section 3). 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 [6] presented in Tables 1, 2, and 3. Furthermore, we observe that this method for determining the number of rational points of E is up to 10^7 faster than the generic method available in MAGMA [1].

The paper is organised as follows. In Section 2 we explain the details of our search and present our records and new entries. In Section 3 we give some background information about fibre products of Kummer covers that our search algorithm depends on.

2. Implementation and Results

Let n_1 and $n_2 \geq 2$ be integers, and $h = (h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2})$ be a tuple of polynomials defined over $\mathbb{F}_q$. Let $E_{q,n_1,n_2,h}$ be the 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 $\mathbb{F}_q$.

Algorithm 1 Search for algebraic function fields with many rational places.

Input: *Table* available in [6] and parameters q, d.
Output: Sets of *Records* and *New Entries*.

Define $\mathrm{UpperN}_q(g)$ (resp. $\mathrm{LowerN}_q(g)$) as the best known upper (resp. lower) bound for $N_q(g)$ given in the *Table*. And, set $\mathrm{LowerN}_q(g) = 0$ if there exists no result for $\mathrm{LowerN}_q(g)$ in the *Table*.
for $n_1 \mid q-1,\ n_2 \mid q-1$ and $\sum deg(h_{i,j}) \leq d$ **do**
    Find genus g of $E_{q,n_1,n_2,h}$ by Proposition 3.2.
    If $g \geq 1$, find number of rational places N of $E_{q,n_1,n_2,h}$ by Theorem 3.1.
    If $N \geq \max\{\frac{\mathrm{UpperN}_q(g)}{\sqrt{2}}, \mathrm{LowerN}_q(g)\}$, save $E_{q,n_1,n_2,h}$ into the set *RecordsNewEntries*.
end for
return *RecordsNewEntries*

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	Previous $\mathrm{LowerN}_q(g)$
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

We use the method presented in [11] for counting rational places of $E_{q,n_1,n_2,h}$ to obtain algebraic function fields with many rational places (see Section 3, Theorem 3.1). We explain the steps of our exhaustive search method over the fibre products given by (2.1) in Algorithm 1. We implemented Algorithm 1 for $q = 5$ and $q = 7$, and we present the results and the details in 2 cases below.

Case $\mathbb{F}_5$: By using Algorithm 1, we made an exhaustive search on fibre products $E_{5,n_1,n_2,h}$ given by (2.1) over the finite field $\mathbb{F}_5$ satisfying $n_1 \mid 4,\ n_2 \mid 4$ and $deg(h_{1,1}) + deg(h_{1,2}) + deg(h_{2,1}) + deg(h_{2,2}) \leq 11$. Then we obtained 4 records for the table [6]. We present examples of the records in Table 1, where N and g denote the number of rational places and the genus of $E_{5,n_1,n_2,h}$ for $h = (h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2})$.

Case $\mathbb{F}_7$: We performed an exhaustive search, by using Algorithm 1, on the fibre products $E_{7,n_1,n_2,h}$ given by (2.1) over the finite field $\mathbb{F}_7$ satisfying $n_1 \mid 6,\ n_2 \mid 6$ and $deg(h_{1,1}) + deg(h_{1,2}) + deg(h_{2,1}) + deg(h_{2,2}) \leq 8$. Then we obtained 8 records and 6 new entries for the table [6]. We present the results within 2 tables. Tables 2 and 3 consist of examples of our results that are records and new entries, respectively, according to the table [6].

Remark 2.1 *For $q = 7$, the algebraic function field $E_{7,3,3,h}$, where $h = (5(x+2)(x+5), x, 3x^2(x+5), x+3)$, given in the Table 2 has 36 rational places, and its genus is 7. Note that the Ihara bound [4, page 722] states that $2N_q(g) \leq \sqrt{(8q+1)g^2 + (4q^2-4q)g} - (g-2q-2)$. It is easy to check that for $q = 7$ and $g = 7$, we have $\sqrt{(8q+1)g^2 + (4q^2-4q)g} - (g-2q-2) = 72$. Therefore, $E_{7,3,3,h}$ attains the Ihara bound for $q = 7$ and $g = 7$.*

3. An Explanation of the Method

In this section, we briefly explain the method given in [11], which enables us to determine the exact number of rational places of fibre products of 2 Kummer covers of the projective line over finite fields $\mathbb{F}_q$. We also state a

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	Previous LowerN$_q(g)$
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	$\lceil \frac{\text{UpperN}_q(g)}{\sqrt{2}} \rceil$
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

proposition for calculation of their genus.

For each element $u \in \mathbb{F}_q$, let P_0 denote the rational place of $\mathbb{F}_q(x)$ that 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 $1 \leq i \leq 2$, let $\bar{n}_i$, n'_i, and a'_i be the integers:

$$\bar{n}_i = \gcd(n_i, a_i), \qquad n'_i = \frac{n_i}{\bar{n}_i}, \qquad \text{and} \qquad a'_i = \frac{a_i}{\bar{n}_i}. \tag{3.1}$$

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

$$\gcd(n'_i, a'_i) = 1 \quad \text{for } 1 \leq i \leq 2. \tag{3.2}$$

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

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

Theorem 3.1 *[11] Let $m_2 = \gcd(n'_2, n'_1)$ and $E = \mathbb{F}_q(x, y_1, y_2)$ be the algebraic function field with*

$$\begin{aligned} y_1^{n_1} &= h_1(x), \\ y_2^{n_2} &= h_2(x). \end{aligned} \tag{3.3}$$

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

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

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 [11, Remark 5]).

Next, we present the genus computation for fibre products of 2 Kummer covers over finite fields $\mathbb{F}_q$.

Proposition 3.2 *Let $h_{1,1}(x), h_{1,2}(x), h_{2,1}(x), h_{2,2}(x) \in \mathbb{F}_q[x]$. Let $E = \mathbb{F}_q(x, y_1, y_2)$ be the algebraic function field with $y_1^{n_1} = \dfrac{h_{1,1}(x)}{h_{1,2}(x)}$ and $y_2^{n_2} = \dfrac{h_{2,1}(x)}{h_{2,2}(x)}$. Assume that $[E : \mathbb{F}_q(x)] = n_1 n_2$, and the full constant field of E is $\mathbb{F}_q$. Let R be the set of all irreducible polynomials in the polynomial ring $\mathbb{F}_q[x]$. Let $h_1(x) = \dfrac{h_{1,1}(x)}{h_{1,2}(x)}$ and $h_2(x) = \dfrac{h_{2,1}(x)}{h_{2,2}(x)}$, which are rational functions in $\mathbb{F}_q(x)$. For $i = 1, 2$ and $p(x) \in R$, let $a_{p,i} \in \mathbb{Z}$ be the integer such that the multiplicity of $p(x)$ in $h_i(x)$ is $a_{p,i}$. Then the genus $g(E)$ is given by*

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

Note that the summation in Proposition 3.2 is finite as $a_{p,1} \neq 0$ or $a_{p,2} \neq 0$ only for finitely many $p(x) \in R$.

Acknowledgments

We would like to thank the anonymous reviewer for the detailed and diligently prepared suggestions, which improved the paper. The authors are partially supported by TÜBİTAK under Grant No. TBAG–109T672.

References

[1] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24, 235–265 (1997).

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

[3] Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves over a Finite Field. Princeton Series in Applied Mathematics. Princeton Univ. Press, Princeton, NJ (2008).

[4] Ihara, Y.: Some remarks on the number of rational points of algebraic curves. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28, 721–724 (1982).

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

[6] ManyPoints Table of Curves with Many Points, http://www.manypoints.org (Accessed June 13, 2012).

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

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

[9] Özbudak, F., Stichtenoth, H. Curves with many points and configurations of hyperplanes over finite fields. Finite Fields Appl. 5, no. 4, 436–449 (1999).

[10] Özbudak, F., Temür, B. G.: Fibre products of Kummer covers and curves with many rational points. Appl. Algebra Engrg. Comm. Comput. 18, 433–443 (2007).

[11] Özbudak, F. Temür, B. G.: Finite number of fibre products of Kummer covers and curves with many rational points over finite fields. Des. Codes Cryptogr. DOI 10.1007/s10623-012-9706-2.

[12] Rökaeus, K.: Computer search for curves with many points among abelian covers of genus 2 curves. arXiv:1106.5176v1 (2011).

[13] Rökaeus, K.: New curves with many points over small finite fields. arXiv:1204.4355v1, (2012)

[14] Rökaeus, K.: Computer search for curves with many points among unramified covers of genus 2 curves over $\mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_9$ and $\mathbb{F}_{11}$. Report, available under manYPoints.org, http://manypoints.org/upload/1369548137.pdf

[15] Rökaeus, K.: Computer search for curves with many points among abelian covers of genus 2 curves over $\mathbb{F}_{13}$. Report, available under manYPoints.org, http://manypoints.org/upload/1225383491.pdf

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

[17] Tsfasman, M.A. Vlădut, S.G. Nogin, D.: Algebraic Geometric Codes: Basic Notions. Mathematical Surveys and Monographs 139. American Mathematical Society, Providence, RI (2007).

[18] van der Geer G., van der Vlugt M.: Tables of curves with many points. Math. Comput. 69 no.230, 797–810 (2000).

[19] van der Geer, G.: Hunting for curves with many points. In IWCC2009 (Eds.: Xing, C. et al.) Lecture Notes in Computer Science 5557, 82–96 (2009).