Reciprocal polynomials and curves with many points over a finite field

Rohit Gupta1*, Erik A. R. Mendoza 2 and Luciane Quoos 2

*Correspondence: rohitgupta20@gmail.com
1Department of Mathematics, Birla Institute of Technology and Science-Pilani, Hyderabad Campus, Hyderabad, Telangana 500078, India
Full list of author information is available at the end of the article

The research of Luciane Quoos and Erik A. R. Mendoza was partially supported by CNPq (Bolsa de Produtividade 302727/2019-1 and CNPq 141907/2020-7, respectively) and FAPERJ (SEI-260003/002364/2021 and FAPERJ 201.650/2021, respectively)

Abstract
Let $\mathbb{F}_{q^2}$ be the finite field with $q^2$ elements. We provide a simple and effective method, using reciprocal polynomials, for the construction of algebraic curves over $\mathbb{F}_{q^2}$ with many rational points. The curves constructed are Kummer covers or fiber products of Kummer covers of the projective line. Further, we compute the exact number of rational points for some of the curves.

Keywords: Function fields, Algebraic curves, Kummer extensions, Rational points
Mathematics Subject Classification: 11G20, 14G05, 14G15, 14H05

1 Introduction
Let $\mathbb{F}_q$ be the finite field with $q$ elements, where $q$ is a prime power. Let $\mathcal{X}$ be a non-singular, projective, and absolutely irreducible algebraic curve defined over $\mathbb{F}_q$. A celebrated theorem of Hasse–Weil states that
$$\#\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g(\mathcal{X})\sqrt{q},$$
(1)
where $\#\mathcal{X}(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points on the curve $\mathcal{X}$ and $g(\mathcal{X})$ is the genus of the curve $\mathcal{X}$. A curve $\mathcal{X}$ over $\mathbb{F}_q$ is called maximal if the number of $\mathbb{F}_{q^2}$-rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ attains the Hasse–Weil bound in (1). It is well known that the genus of a maximal curve over $\mathbb{F}_{q^2}$ is at most $q(q - 1)/2$, see [10].

In the nineties, Goppa introduced a way to associate an error-correcting code to a linear system on a curve over a finite field, see [7, 8]. In order to construct such codes with good parameters one requires curves with a large number of rational points. This leads to interest in the study of curves over finite fields with many rational points with respect to its genus. Also such curves have applications in low-discrepancy sequences, stream ciphers, hash functions, and finite geometries.

In the last few decades, several methods, such as class field theory, Drinfeld module, and character theory, to find algebraic curves with many points have been studied, see [4, 5, 9, 11, 12, 17, 18, 20, 22, 24]. More explicit details about these methods can be found in [21]. However, the computation of the exact number of rational points on a given curve has always been a challenging problem, and a general method to do such computations seems out of reach. For certain very specific curves, some methods, such as the evaluation of exponential sums and Kloosterman sums, as well as function field theory, have
been helpful. For instance, Coulter [2] used exponential sums to compute the number of rational points on a class of Artin-Schreier curves, and Moisio [13] used exponential sums and Kloosterman sums to compute the number of rational points on some families of Fermat curves. In [15,16], the authors considered fiber products of Kummer covers of the projective line over \( \mathbb{F}_q \). In [14], the authors gave a full description of the number of rational points in some extension \( \mathbb{F}_{q^r} \) of \( \mathbb{F}_q \) in terms of Legendre symbol and quadratic characters for the Artin-Schreier curve \( y^q - y = xP(x) - \lambda \) where \( P(x) = x^q - x \) and \( \lambda \in \mathbb{F}_q \). For more details about these methods, we refer to [2,13–15] and [16].

For a curve \( X \) over \( \mathbb{F}_q \) with \( g(X) \leq 50 \), the webpage www.manypoints.org [23] collects the current intervals in which the number \( #X(\mathbb{F}_q) \) is known to lie for some values of \( q \).

For a pair \((q,g)\), the tables record an interval \([a,b]\) where \( b \) is the best upper bound for the maximum number of points of a curve of genus \( g \) over \( \mathbb{F}_q \), and \( a \) gives a lower bound obtained from an explicit example of a curve \( \mathcal{X} \) defined over \( \mathbb{F}_q \) with \( a \) (or at least \( a \)) rational points. At some places in the manYPoints table in [23], the lower bound \( a \) of the interval \([a,b]\) is replaced by the symbol ‘−’ where ‘−’ represents the lower bound \( L(q,g) \) given in (2).

In this article, we improve upon the lower bounds of many of the intervals in [23] by constructing new examples of curves with many points. We provide a simple and effective construction of Kummer covers and fiber products of Kummer covers of the projective line over finite fields with many rational points using reciprocal polynomials. We give a general lower bound for the number of the rational points under certain hypotheses, see Theorems 4.1, 5.1, 6.1 and 6.3. In fact, we calculate the exact number of rational points for some particular constructions, see Theorem 4.2, Propositions 4.3 and 4.4.

As a consequence of these constructions, we obtain several improvements on the manYPoints table [23]. More precisely, we obtain the following 10 new records.

(i) A curve of genus 13 over \( \mathbb{F}_{74} \) with 3576 rational points (see Example 4.7).
(ii) A curve of genus 17 over \( \mathbb{F}_{74} \) with 3968 rational points (see Example 4.7).
(iii) A curve of genus 15 over \( \mathbb{F}_{172} \) with 708 rational points (see Example 5.2).
(iv) A curve of genus 10 over \( \mathbb{F}_{114} \) with 16952 rational points (see Example 5.2).
(v) A curve of genus 15 over \( \mathbb{F}_{192} \) with 866 rational points (see Example 5.2).
(vi) A curve of genus 13 over \( \mathbb{F}_{172} \) with 648 rational points (see Example 5.3).
(vii) A curve of genus 8 over \( \mathbb{F}_{114} \) with 16566 rational points (see Example 5.4).
(viii) A curve of genus 22 over \( \mathbb{F}_{52} \) with 174 rational points (see Example 6.2).
(ix) A curve of genus 11 over \( \mathbb{F}_{132} \) with 444 rational points (see Example 6.4).
(x) A curve of genus 13 over \( \mathbb{F}_{132} \) with 444 rational points (see Example 6.4).

We also obtain 119 new entries and among these we point out three important new entries: explicit equations for a maximal curve of genus 18 and 36 over \( \mathbb{F}_{54} \) and analogously, for a maximal curve of genus 46 over \( \mathbb{F}_{74} \), see Remark 4.9.

The remainder of this paper is organized as follows. In Sect. 2 we include the preliminaries and the notation used in the development of this work. In Sect. 3 we present a family of Kummer covers of the projective line over \( \mathbb{F}_{q^2} \) defined by an affine equation of the type

\[ y^m = x^s f(x) f^*(x)^e \]

where \( e, \lambda \in \{1, -1\}, s \in \mathbb{N}, q = p^n \) with \( p \nmid m \), \( f(x) \) is a polynomial in \( \mathbb{F}_q[x] \) and \( f^*(x) \) is the reciprocal polynomial of \( f(x) \). We compute the genus of this family of curves, see
Theorem 3.3. In Sect. 4, we study the particular case $\epsilon = -1$ and $\lambda = 1$, and provide the exact number of rational points for some families of curves, see Theorem 4.2, Propositions 4.3 and 4.4. For certain parameters, these families of curves turn out to be maximal over $\mathbb{F}_q$. We also give new examples of curves with many rational points, see Examples 4.6, 4.7, 4.8, 4.9, 4.10, and 4.11. In Sect. 5, we study the case $\epsilon = 1$ and $\lambda = -1$. We again obtain new examples of curves with many points, see Examples 5.2, 5.3, 5.4, 5.5, and 5.6. In Sect. 6, we obtain new curves with many rational points by considering the fiber products of the curves constructed in Sects. 4 and 5, see Examples 6.2 and 6.4. All the examples were obtained using the software Magma [1].

2 Preliminaries and notation
Throughout this article, we let $p$ be a prime number, $q$ a power of the prime $p$, and $\mathbb{F}_q$ the finite field with $q$ elements. For a non-singular, projective, absolutely irreducible algebraic curve $X$ of genus $g(X)$ over $\mathbb{F}_q$, $\mathbb{F}_q(X)$ denotes its function field (where $\mathbb{F}_q$ is its full constant field) and $X(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of the curve. For a function $z \in \mathbb{F}_q(X)$, $(z)_{\mathbb{F}_q(X)}$ stands for the principal divisor of the function $z$ in $\mathbb{F}_q(X)$.

We denote by $K$ the algebraic closure of $\mathbb{F}_q$. Moreover, we denote by $\xi_q$ a primitive element of the finite field $\mathbb{F}_q$ and by $(a, b)$ the greatest common divisor of the elements $a$ and $b$ in a unique factorization ring.

Given a polynomial $f$ in $\mathbb{F}_q[x]$ and a subset $\mathcal{A} \subseteq \mathbb{F}_q^2$, we let $N_f(\mathcal{A}) := \#\{\alpha \in \mathcal{A} \mid f(\alpha) = 0\}$ stand for the number of roots of $f$ in $\mathcal{A}$.

We set some notation about curves with many points. We say that a curve $X$ over $\mathbb{F}_q$ with genus $g$ has many points if the number of $\mathbb{F}_q$-rational points of $X$, denoted by $\#X(\mathbb{F}_q)$, satisfies

$$\#X(\mathbb{F}_q) \geq U(q, g) := \left\lfloor \frac{U(q, g) - q - 1}{\sqrt{2}} \right\rfloor + q + 1,$$

where $U(q, g)$ denotes the upper bound given in the manYPoints table [23] for the number of $\mathbb{F}_q$-rational points of a curve over $\mathbb{F}_q$ with genus $g$. In particular, for a pair $(q, g)$ and a curve $X$ over $\mathbb{F}_q$ with genus $g$, we say that $X$ gives a new record (resp. meets the record) if the number $\#X(\mathbb{F}_q)$ is strictly larger than (resp. is equal to) the lower bound registered in the manYPoints table corresponding to $(q, g)$. Further, we say that a curve $X$ over $\mathbb{F}_q$ with genus $g$ is a new entry if there was no earlier lower bound entry in the manYPoints table corresponding to $(q, g)$ and $\#X(\mathbb{F}_q)$ satisfies the relation (2).

In the tables where we provide a new record, the notation OLB (old lower bound) stands for the lower bound on the number $\#X(\mathbb{F}_q)$ of rational points for a curve over $\mathbb{F}_q$ of genus $g$ registered in the table [23]. Instead, when we provide a new entry, the notation OLB stands for the lower bound given in (2). Further, in the tables, the symbol $\dagger$ indicates a maximal curve over $\mathbb{F}_q$.

We point out that throughout the article a rational point on the curve is the same as a rational place in the function field of the curve.

3 A construction of curves over $\mathbb{F}_q^2$
Given a polynomial $f(x)$ in $\mathbb{F}_q[x]$ of degree $d$, denote by $f^*(x) = x^d f(1/x)$ the reciprocal polynomial of $f(x)$. In this section, we propose a construction of algebraic curves over $\mathbb{F}_q^2$ using reciprocal polynomials. We will see that certain specific polynomials provide
interesting algebraic curves with many points. This idea is explored in more detail in the subsequent sections.

**Remark 3.1** For the general theory on Kummer extensions, we refer to the book [19]. We note that an expression for the genus can be obtained from the Riemann–Hurwitz formula and the computation of ramification indices (see [19, Proposition 3.7.3]).

We start by presenting the following proposition that will be useful in the sequel. For a more general version see [15, Theorems 3 and 4].

**Proposition 3.2** Let \( \mathbb{F}_q(x, y)/\mathbb{F}_q(x) \) be a Kummer extension of degree \( m \) with full constant field \( \mathbb{F}_q \) and defined by the equation \( y^m = h(x) \), where \( m \) is a divisor of \( q - 1 \) and \( h \in \mathbb{F}_q(x) \).

(i) For each \( \alpha \in \mathbb{F}_q \), we write

\[
h(x) = (x - \alpha)^{k_\alpha}g_\alpha(x)
\]

where \( k_\alpha \in \mathbb{Z} \), \( g_\alpha(x) \in \mathbb{F}_q(x) \) and \( g_\alpha(\alpha) \notin \{0, \infty\} \). Then for the place \( P_\alpha \) there exist either no or exactly \((m, k_\alpha)\) rational places of \( \mathbb{F}_q(x, y) \) over \( P_\alpha \). In fact, there exists a rational place \( Q \) of \( \mathbb{F}_q(x, y) \) over \( P_\alpha \) if and only if \( g_\alpha(\alpha) \) is a \((m, k_\alpha)\)-th power in \( \mathbb{F}_q^* \) (with ramification index \( e(Q|P_\alpha) = \frac{m}{(m, k_\alpha)} \)).

(ii) For the place \( P_\infty \), suppose that

\[
h(x) = c_\infty \frac{g_1(x)}{g_2(x)}
\]

where \( c_\infty \in \mathbb{F}_q^* \) and \( g_1, g_2 \) are monic polynomials in \( \mathbb{F}_q[x] \) with \( (g_1, g_2) = 1 \). Then there exist either no or exactly \((m, \deg g_2 - \deg g_1)\) rational places of \( \mathbb{F}_q(x, y) \) over \( P_\infty \). In the case of \( P_\infty \), there exists a rational place \( Q \) of \( \mathbb{F}_q(x, y) \) over \( P_\infty \) if and only if \( c_\infty \) is a \((m, \deg g_2 - \deg g_1)\)-th power in \( \mathbb{F}_q^* \) (with ramification index \( e(Q|P_\infty) = \frac{m}{(m, \deg g_2 - \deg g_1)} \)).

An idea to obtain a curve with many points over \( \mathbb{F}_q^2 \) from a rational function \( h(x) \) over \( \mathbb{F}_q \) of Kummer type \( y^m = h(x) \) with \( m \mid (q + 1) \) is to choose \( h \) of “small” degree (since we need a curve with “small” genus) such that the image of \( h(x) \) on a “large” subset of \( \mathbb{F}_q^2 \) goes to \( \mathbb{F}_q^* \). In fact, if \( \alpha \in \mathbb{F}_q^* \) is such that \( h(\alpha) \in \mathbb{F}_q^* \), then \( h(\alpha) \) is a \( m \)-th power in \( \mathbb{F}_q^* \) and thus the point \( x = \alpha \) splits in the extension \( \mathbb{F}_q^2(x, y)/\mathbb{F}_q^2(x) \). This guarantees that many points split in the extension \( \mathbb{F}_q^2(x, y)/\mathbb{F}_q^2(x) \). In order to achieve this, we explore reciprocal polynomials in the present paper. In fact, let \( f \in \mathbb{F}_q[x] \) be a polynomial of degree \( d \) with no roots in \( \mu_{q+1} = \{ b \in \mathbb{F}_q^* \mid b^{q+1} = 1 \} \). For \( a \in \mu_{q+1} \) we have

\[
f^*(a) = a^df(1/a) = a^df(a^g) = a^df(a)^g.
\]

Then,

\[
\frac{f(a)f^*(a)}{a^d} = f(a)^g+1 \in \mathbb{F}_q
\]

and the point \( x = a \) splits in the extension \( \mathbb{F}_q^2(x, y)/\mathbb{F}_q^2(x) \) given by \( y^m = \frac{f(x)f^*(x)}{x^d} \). Thus, we conclude that the number of rational points on the algebraic curve \( \mathcal{X} : y^m = \frac{f(x)f^*(x)}{x^d} \) satisfies

\[
\#\mathcal{X}(\mathbb{F}_q^2) \geq m(q + 1).
\]
A similar argument works for algebraic curves of type \( y^m = \frac{x^d f(x)}{f'(x)} \) where \( m \mid (q - 1) \). In this paper, we explore these ideas in order to construct families of algebraic curves with many rational points.

For an integer \( m \geq 2 \) not divisible by \( p \) and a non-negative integer \( s \), consider the algebraic curve \( X' \) over \( \mathbb{F}_{q^2} \) defined by the affine equation

\[
X': \quad y^m = x^e f(x) f^*(x)^\lambda \quad \text{where } e, \lambda \in \{1, -1\}.
\]

With some assumptions on \( f \), we compute the genus of these curves in the following theorem.

**Theorem 3.3** Let \( d > 0 \) and \( f(x) = a_0 + a_1 x + \cdots + a_d x^d \) in \( \mathbb{F}_q[x] \) be a separable polynomial of degree \( d \) satisfying \( f(0) \neq 0 \). Let \( s \) be a non-negative integer, \( d_1 \) be the degree of \( (f, f^*) \) and \( m \geq 2 \) be such that \( p \nmid m \). If \( d_1 < d \), then the algebraic function field \( K(x, y) \) defined by the affine equation

\[
y^m = x^e f(x) f^*(x)^\lambda, \quad \text{where } e, \lambda \in \{1, -1\},
\]

has genus

\[
g = (m - 1)d + 1 - \frac{(m, s) + (m, es + d + d\lambda) + d_1 (m, \lambda + 1) + d_1 (m - 2)}{2}.
\]

**Proof** At first, we write

\[
x^e f(x) f^*(x)^\lambda = x^e (f(x)/h(x)) (f^*(x)/h(x))^\lambda h(x)^{1+\lambda}
\]

where \( h = (f, f^*) \). The polynomials \( h, f/h \) and \( f^*/h \) are separable and \( \alpha \in K \) is a root of \( f \) if and only if \( \alpha^{-1} \) is a root of \( f^* \). So, without loss of generality, we can suppose that

\[
f/h = \beta_1 \prod_{i=1}^{d-d_1} (x - \alpha_i), \quad f^*/h = \beta_2 \prod_{j=1}^{d-d_1} (x - \gamma_j) \quad \text{and} \quad h = \beta \prod_{k=d-d_1+1}^{d} (x - \alpha_k),
\]

where \( \beta_1, \beta_2, \beta \) are in \( K \), and for all \( 1 \leq i \leq d \), and \( \alpha_i, \gamma_j, \alpha_k \) are pairwise distinct for all \( 1 \leq i \leq d-d_1 \) and \( d-d_1+1 \leq k \leq d \).

The principal divisor of the function \( x^e f(x) f^*(x)^\lambda \) in \( K(x) \) is given by

\[
(x^e f(x) f^*(x)^\lambda)_{K(x)} = \epsilon s P_0 - P_{\infty} + \sum_{i=1}^{d-d_1} P_{\alpha_i} - (d - d_1) P_{\infty} + \lambda \sum_{j=1}^{d-d_1} P_{\gamma_j} - \lambda (d - d_1) P_{\infty} + (\lambda + 1) \sum_{k=d-d_1+1}^{d} P_{\alpha_k} - d_1 (\lambda + 1) P_{\infty}
\]

\[
= \epsilon s P_0 + \sum_{i=1}^{d-d_1} P_{\alpha_i} + \lambda \sum_{j=1}^{d-d_1} P_{\gamma_j} + (\lambda + 1) \sum_{k=d-d_1+1}^{d} P_{\alpha_k} - (\epsilon s + d + d\lambda) P_{\infty}.
\]

This implies that the extension \( K(x, y)/K(x) \) is a Kummer extension of degree \( m \) and for a place \( P \) of \( K(x, y) \), the ramification index is given by

\[
e(P) = \begin{cases} 
  m/(m, s), & \text{if } P \text{ is over } P_0, \\
  m, & \text{if } P \text{ is over } P_{\alpha} \text{ or } P_{\gamma}, \text{ for } i = 1, \ldots, d - d_1, \\
  m/(m, \lambda + 1), & \text{if } P \text{ is over } P_{\alpha_i}, \text{ for } i = d - d_1 + 1, \ldots, d, \\
  m/(m, \lambda + 1), & \text{if } P \text{ is over } P_{\infty}, \\
  1, & \text{otherwise.}
\end{cases}
\]
In view of Remark 3.1, using the Riemann–Hurwitz formula, we see that the genus \( g \) of \( K(x, y) \) satisfies
\[
2g - 2 = -2m + m - (m, s) + 2(m - 1)(d - d_1) + d_1(m - (m, \lambda + 1)) + m - (m, \epsilon s + d + d\lambda),
\]
which gives
\[
g = (m - 1)d + 1 - \frac{(m, s) + (m, \epsilon s + d + d\lambda) + d_1(m, \lambda + 1) + d_1(m - 2)}{2}.
\]
\( \square \)

In the subsequent sections, we investigate the number of \( \mathbb{F}_{q^2} \)-rational points on the curve given in (3) for the cases \( \epsilon = -1 \) and \( \lambda = 1 \), and \( \epsilon = 1 \) and \( \lambda = -1 \) separately. Note that the curves \( \mathcal{X} \) for \( \epsilon = \lambda = 1 \) and \( \epsilon = \lambda = -1 \) are isomorphic to the curves with \( \epsilon = -1 \) and \( \lambda = 1 \), and \( \epsilon = 1 \) and \( \lambda = -1 \) respectively.

4 Curves over \( \mathbb{F}_{q^2} \) from Sect. 3: the case of \( \epsilon = -1 \) and \( \lambda = 1 \)

In this section, we restrict ourselves to the curve \( \mathcal{X} \) in (3) with \( \epsilon = -1 \) and \( \lambda = 1 \). We impose certain conditions on the polynomial \( f \in \mathbb{F}_q[x] \) to provide an explicit expression and a lower bound for the number of \( \mathbb{F}_{q^2} \)-rational points on the curve \( \mathcal{X} \). Moreover, for some of these algebraic curves, we compute the exact number of \( \mathbb{F}_{q^2} \)-rational points, see Theorem 4.2, Propositions 4.3 and 4.4.

**Theorem 4.1** Let \( m \geq 2 \) be a divisor of \( q + 1 \), \( f \in \mathbb{F}_q[x] \) be a separable polynomial of degree \( d \) satisfying \( f(0) \neq 0 \) and \( (f, f^*) = 1 \), and \( s \) be an integer \( 0 \leq s < m \). Then the algebraic curve defined by
\[
\mathcal{X} : \quad y^m = \frac{f(x)f^*(x)}{x^s}
\]
has genus
\[
g = (2md - 2(d - 1) - (m, s) - (m, 2d - s))/2.
\]

Further, if \( (f, x^{d+1} - 1) = 1 \), then the number of rational points of \( \mathcal{X} \) over \( \mathbb{F}_{q^2} \) satisfies
\[
\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m[(q + 1, 2(d - s)) + q - 3 - 2N_f(\mathbb{F}_q^*)] + 2N_f(\mathbb{F}_q^2).
\]

In particular, for \( s = d \), we have \( \#\mathcal{X}(\mathbb{F}_{q^2}) \geq 2m(q - 1 - N_f(\mathbb{F}_q^*)) + 2N_f(\mathbb{F}_q^2) \).

**Proof** A direct application of Theorem 3.3 gives the genus of the curve defined in (4). We now provide an expression for the number of \( \mathbb{F}_{q^2} \)-rational points on this curve. Let \( \alpha \in \mathbb{F}_{q^2}^* \) be such that \( f(\alpha)f^*(\alpha) \neq 0 \). Then \( \frac{f(\alpha)f^*(\alpha)}{\alpha^s} \) is a \( m \)-th power in \( \mathbb{F}_{q^2} \) if and only if
\[
\left( \frac{f(\alpha)f^*(\alpha)}{\alpha^s} \right)^{\frac{q^2 - 1}{m}} = 1,
\]
which is equivalent to
\[
\left( \left( \frac{f(\alpha)f^*(\alpha)}{\alpha^s} \right)^{q - 1} - 1 \right) \left( \sum_{i=0}^{\#+1} \left( \frac{f(\alpha)f^*(\alpha)}{\alpha^s} \right)^{(q - 1)i} \right) = 0,
\]
that is,
\[
((f(\alpha)f^*(\alpha))^{q - 1} - \alpha^{s(q - 1)}) \left( \sum_{i=0}^{\#+1} (f(\alpha)f^*(\alpha))^{(q - 1)i}\alpha^{s(q - 1)(\#+1-1-i)} \right) = 0.
\]
Let 
\[ h_1(x) = (f(x)f^*(x))^q \cdot \alpha^{(q-1)} - x^{(q-1)} \] and 
\[ h_2(x) = \sum_{i=0}^{\frac{q+1}{m}-1} (f(x)f^*(x))^{(q-1)i} \beta^{i(q-1)} \left( \frac{q+1}{m} - 1 - i \right). \]

Then \( h_1 \) and \( h_2 \) are coprime polynomials. In fact, if \( \alpha \) is a root of \( h_1 \), then \((f(\alpha)f^*(\alpha))^q - \alpha^{(q-1)}\) and

\[ h_2(\alpha) = \sum_{i=0}^{\frac{q+1}{m}-1} (f(\alpha)f^*(\alpha))^{(q-1)i} \beta^{i(q-1)} \left( \frac{q+1}{m} - 1 - i \right) \]
\[ = \sum_{i=0}^{\frac{q+1}{m}-1} \alpha^{i(q-1)} \beta^{i(q-1)} \left( \frac{q+1}{m} - 1 - i \right) \]
\[ = \left( \frac{q+1}{m} \right) \beta^{(q+1) \left( \frac{q+1}{m} - 1 \right)} \neq 0. \]

It is also clear that \((h_1, f^*) = (h_2, f^*) = 1\). We conclude that

\[ \# \left\{ \alpha \in \mathbb{F}_q^* \mid f(\alpha)f^*(\alpha) \neq 0 \text{ and } \frac{f(\alpha)f^*(\alpha)}{\alpha^s} \text{ is a } m \text{-th power in } \mathbb{F}_q^2 \right\} \]
\[ = N_{h_1}(\mathbb{F}_q^2) + N_{h_2}(\mathbb{F}_q^2). \]

From Proposition 3.2, each \( \alpha \in \mathbb{F}_q^2 \) such that \( f(\alpha)f^*(\alpha) = 0 \) gives one rational point on the curve. From Proposition 3.2, we also conclude that each one of \( x = 0 \) and \( x = \infty \) contributes \((m, s)\) and \((m, 2d - s)\) rational points on the curve respectively. So the number of rational points on the curve \( \mathcal{X}' \) is

\[ \# \mathcal{X}(\mathbb{F}_q^2) = (m, s) + (m, 2d - s) + 2N_f(\mathbb{F}_q^2) + m(N_{h_1}(\mathbb{F}_q^2) + N_{h_2}(\mathbb{F}_q^2)). \]

(5)

Now we assume that \((f, x^q+1 - 1) = 1\). Note that, for \( \beta \in \{ a \in \mathbb{F}_q^2 \mid a^{(q+1, 2d-s)} = 1 \} \), we have \( \beta^q = \beta^{-1} \) and thus we write

\[ h_1(\beta) = (f(\beta)f^*(\beta))^q - \beta^{(q-1)} = \frac{f(\beta)f^*(\beta))^q}{f(\beta)f^*(\beta)} - \beta^{-2s} = \frac{f(\beta)f^*(\beta)}{f(\beta)f^*(\beta)} - \beta^{-2s} = \beta^{-2d} - \beta^{-2s} = 0. \]

Also, for \( \beta \in \mathbb{F}_q^* \) such that \( f(\beta)f^*(\beta) \neq 0 \), we have \( h_1(\beta) = 0 \). Therefore

\[ N_{h_1}(\mathbb{F}_q^2) \geq (q + 1, 2(d - s)) + q - 1 - 2N_f(\mathbb{F}_q^2) - (q - 1, 2). \]

Hence we get

\[ \# \mathcal{X}(\mathbb{F}_q^2) \geq 2N_f(\mathbb{F}_q^2) + m[(q + 1, 2(d - s)) + q - 3 - 2N_f(\mathbb{F}_q^2)]. \]

□

In what follows we compute the genus and the exact number of rational points for some families of algebraic curves as constructed in (4).
Theorem 4.2 Let \( b \in \mathbb{F}_q^* \), \( b^2 \neq 1 \) and \( d \) be a positive divisor of \( q + 1 \). Then the algebraic curve defined by
\[
X : y^{q+1} = bx^{2d} + (b^2 + 1)x^d + b
\]
has genus
\[
g = d(q - 1) + 1
\]
and its number of \( \mathbb{F}_q^2 \)-rational points is given by
\[
\#X(\mathbb{F}_q^2) = d(q^2 - 1) + (d, 2)(q + 1)^2 + 4d - d(q + 1)((q - 1, 2) + 2).
\]
In particular, if \( q \) is odd, \( d = 2 \), and \( q \geq 17 \), then this curve has many points.

Proof The curve \( X \) corresponds to the construction in (4) for \( f(x) = x^d + b \), \( s = d \) and \( m = q + 1 \). Since \( b^2 \neq 1 \), we have \((f, f^*) = 1 \). The genus of the curve follows from Theorem 4.1. Now we compute the number of \( \mathbb{F}_q^2 \)-rational points on the curve following the proof and notation as in Theorem 4.1. Since \( b \in \mathbb{F}_q^* \) and \( d \) is a divisor of \( q + 1 \), each one of \( f \) and \( f^* \) has \( d \) distinct roots in \( \mathbb{F}_q^* \) and therefore \( N_{ff^*}(\mathbb{F}_q^2) = 2d \). Note that each root of \( ff^* \) contributes one rational point on the curve. From Proposition 3.2, we also conclude that each one of \( x = 0 \) and \( x = \infty \) contributes \((q + 1, d) = d \) rational points on the curve respectively.

On the other hand, we have that
\[
\# \left\{ \alpha \in \mathbb{F}_q^* \mid f(\alpha)f^* (\alpha) \neq 0 \text{ and } \frac{f(\alpha)f^*(\alpha)}{\alpha^d} \text{ is a } (q + 1)\text{-th power in } \mathbb{F}_q^* \right\}
\]
where
\[
h_1(x) = (f(x)f^*(x))^{q-1} - x^{d(q-1)} = \frac{h(x^{d(q+1)} - 1)(x^{d(q-1)} - 1)}{f(x)f^*(x)} \quad \text{and} \quad h_2(x) \equiv 1.
\]
Clearly \( N_{h_2}(\mathbb{F}_q^2) = 0 \). Next we show that the polynomial \( h_1 \in \mathbb{F}_q[x] \) has \( d(q - 1) + 2(q + 1) - 4d \) distinct roots in \( \mathbb{F}_q^* \). In fact, since
\[
(x^{d(q+1)} - 1, x^{q-1} - 1) = x^{(d,2)(q+1)} - 1,
\]
\[
(x^{d(q+1)} - 1, x^{q-1} - 1) = x^{d(q-1)} - 1
\]
and
\[
(x^{(d,2)(q+1)} - 1, x^{d(q-1)} - 1) = x^{d(q-1,2)} - 1,
\]
we obtain \( d(q - 1) + (d, 2)(q + 1) - d(q - 1, 2) \) distinct roots of \((x^{d(q+1)} - 1)(x^{d(q-1)} - 1)\) in \( \mathbb{F}_q^* \). Since \( N_{ff^*}(\mathbb{F}_q^2) = 2d \), we conclude that \( h_1 \) has \( d(q - 1) + (d, 2)(q + 1) - d(q - 1, 2) - 2d \) distinct roots in \( \mathbb{F}_q^* \). Hence the number of \( \mathbb{F}_q^2 \)-rational points on the curve \( X \) is given by
\[
\#X(\mathbb{F}_q^2) = 4d + (q + 1)(d(q - 1) + (d, 2)(q + 1) - d(q - 1, 2) - 2d)
\]
\[
= d(q^2 - 1) + (d, 2)(q + 1)^2 + 4d - d(q + 1)((q - 1, 2) + 2).
\]

Next, we show that for \( q \) odd, \( d = 2 \) and \( q \geq 17 \) this curve has many points. From (2), a curve is considered to have many points if and only if \( L(q^2, g) \leq \#X(\mathbb{F}_q^2) \). From the
Hasse–Weil bound, we have
\[ L(q^2, g) \leq \left\lfloor \frac{q^2 + 1 + 2gq - q^2 - 1}{\sqrt{2}} \right\rfloor + q^2 + 1 = \lfloor \sqrt{2}gq \rfloor + q^2 + 1. \]

In particular, algebraic curves satisfying \( \sqrt{2}gq + q^2 + 1 \leq \#X(q^{-1}) \) have many points. Therefore the curve \( X \) has many points if
\[
\sqrt{2}q(d(q-1)+1) + q^2 + 1 \leq d(q^2 - 1) + (d, 2)(q+1)^2 + 4d - d(q+1)(q-1, 2) + 2.
\]

The condition (6) is never satisfied when \( q \) is even or when \( q \) is odd and \( d \neq 2 \). For \( q \) odd and \( d = 2 \), this condition is satisfied if and only if \( q \geq 17 \). \( \square \)

Note that for \( b^2 = 1 \) the curve \( X \) in Theorem 4.2 is isomorphic to the curve with affine equation \( y^{q+1} = (x^d + b)^2/x^d \). In order to complete the analysis of the curve \( X \) given in Theorem 4.2, we study an absolutely irreducible component of the curve \( X \) in Proposition 4.3 (for \( d \) even) and in Proposition 4.4 (for \( d \) odd).

**Proposition 4.3** Assume \( q \) is odd. Let \( d \geq 1 \) be a positive integer such that \( 4d \) divides \( q^2 - 1 \) and \( b \in \mathbb{F}_q \) be such that \( b^2 = 1 \). Then the algebraic curve \( X \) defined by the affine equation
\[
y^{(q+1)/2} = \frac{x^{2d} + b}{x^d}
\]
has genus
\[ g = \frac{d(q-1) + 2 - (2d, q+1)}{2} \]
and its number of \( \mathbb{F}_{q^2} \)-rational points is given by
\[ \#X(\mathbb{F}_{q^2}) = \frac{(q+1)^2(2d, q-1) + (q^2 + 1)(2d, q+1) - 2d(3q+1)}{2}. \]

In particular, this curve is maximal over \( \mathbb{F}_{q^2} \) if and only if \( (2d, q+1)(2d, q-1) = 2(d+1) \).

**Proof** The computation of the genus follows from the Riemann–Hurwitz formula and the expression of the ramification indices given in Proposition 3.2. On the other hand, again by Proposition 3.2, each one of the points \( x = 0 \) and \( x = \infty \) contributes with \( (d, q^{-1}) \) rational points on the curve. Now we consider the roots of \( x^{2d} + b \). Since \( 4d \mid q^2 - 1 \), we have \( \#\{\alpha \in \mathbb{F}_{q^2} : \alpha^{2d} + b = 0\} = 2d \) and each root of \( x^{2d} + b \) contributes with one rational point. On the other hand, for \( \alpha \in \mathbb{F}_{q^1}^* \) such that \( \alpha^{2d} + b \neq 0 \), we have
\[
\alpha^{2d} + b = (q+1)^{-1} \text{ in } \mathbb{F}_{q^2}^* \iff \left( \frac{\alpha^{2d} + b}{\alpha^d} \right)^{2(q-1)} = 1
\]
\[
\iff (\alpha^{4d} + 2b\alpha^{2d} + 1)^{q-1} = \alpha^{2d(q-1)}
\]
\[
\iff \alpha^{4dq} + 2b\alpha^{2dq} + 1 = \alpha^{2d(q-1)}(\alpha^{4d} + 2b\alpha^{2d} + 1)
\]
\[
\iff \alpha^{4dq} - \alpha^{2d(q+1)} - \alpha^{2d(q-1)} + 1 = 0
\]
\[
\iff (\alpha^{2d(q+1)} - 1)(\alpha^{2d(q-1)} - 1) = 0.
\]
Since
\[
(x^{2d(q+1)} - 1, x^{q^2-1} - 1) = x^{(q+1)(2d,q-1)} - 1,
\]
\[
(x^{2d(q-1)} - 1, x^{q^2-1} - 1) = x^{(q-1)(2d,q+1)} - 1
\]
and
\[
(x^{(q+1)(2d,q-1)} - 1, x^{(q-1)(2d,q+1)} - 1) = x^{4d} - 1,
\]
we obtain that there are \((q+1)(2d, q - 1) + (q - 1)(2d, q + 1) - 4d\) elements \(\alpha \in \mathbb{F}_{q^2}^*\) satisfying (8). Also, since
\[
x^{2d} + b \mid (x^{2d(q+1)} - 1)(x^{2d(q-1)} - 1),
\]
we conclude that the polynomial \((x^{2d(q+1)} - 1)(x^{2d(q-1)} - 1)\) has \((q+1)(2d, q - 1) + (q - 1)(2d, q + 1) - 6d\) distinct roots in \(\mathbb{F}_{q^2}^* \setminus \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{2d} + b = 0\}\). Consequently,
\[
\#\mathcal{X}(\mathbb{F}_{q^2}) = 2d + 2 \left( \frac{d}{2} \right) + \frac{q + 1}{2}((q + 1)(2d, q - 1) + (q - 1)(2d, q + 1) - 6d)
\]
\[
= \frac{(q + 1)^2(2d, q - 1) + (q^2 + 1)(2d, q + 1) - 2d(3q + 1)}{2}.
\]
Finally, we note that
\[
\#\mathcal{X}(\mathbb{F}_{q^2}) - q^2 - 1 - 2gq = \frac{(q + 1)^2}{2}((2d, q - 1) + (2d, q + 1) - 2 - 2d).
\]
This completes the proof. \(\square\)

**Proposition 4.4** Assume \(q\) is odd. Let \(d \geq 1\) be an odd integer such that \(p \nmid d\) and \(b \in \mathbb{F}_q\) be such that \(b^2 = 1\). Then the algebraic curve \(\mathcal{X}\) defined by the equation
\[
y^{q+1} = \frac{(x^d + b)^2}{xd}
\]
has genus
\[
g = \frac{d(q - 1) + 2 - 2(d, q + 1)}{2}
\]
and its number of \(\mathbb{F}_{q^2}\)-rational points is given by
\[
\#\mathcal{X}(\mathbb{F}_{q^2}) = (q^2 + 1)(d, q + 1) + (q + 1)^2(d, q - 1) - (3q + 1)(d, q^2 - 1).
\]
In particular, for a divisor \(d\) of \(q^2 - 1\), the curve \(\mathcal{X}\) is \(\mathbb{F}_{q^2}\)-maximal if and only if either \((d, q + 1) = 1\) or \((d, q - 1) = 1\).

**Proof** The computation of the genus follows from [19, Proposition 3.7.3] and the computation of the number of \(\mathbb{F}_{q^2}\)-rational points on the curve is analogous to the proof of Proposition 4.3. For a divisor \(d\) of \(q^2 - 1\), we have
\[
\#\mathcal{X}(\mathbb{F}_{q^2}) - q^2 - 1 - 2gq = (q^2 + 1)(d, q + 1) + (q + 1)^2(d, q - 1) - (3q + 1)(d - q^2 - 1)
\]
\[
\quad - dq(q + 1) + 2dq + 2q(d, q + 1) - 2q
\]
\[
= (q + 1)^2((d, q + 1) + (d, q - 1) - 1) - d(q + 1)^2
\]
\[
= (q + 1)^2((d, q + 1) + (d, q - 1) - 1) - d
\]
\[
= -(q + 1)^2((d, q + 1) - 1)((d, q - 1) - 1).
\]
This completes the proof. \(\square\)
Remark 4.5 The curve in Proposition 4.4 is isomorphic to $y^{q+1} = x^{q+1-d}(x^d + b)^2$. We point out that for some values of $d$ (for instance, when $d$ is a divisor of $q+1$), this curve has appeared in [6, Example 6.4 (case 2)] as a subcover of the Hermitian curve over $\mathbb{F}_{q^2}$ given by
\[ y^m = (-1)^k x^{bm}(x^m + 1)^k, \]
where $m, m_1$ are divisors of $q+1$, and $k, b$ are positive integers.

We now provide examples of curves with many points from the constructions obtained in this section.

Example 4.6 Let $f(x) = x + b$ where $b \in \mathbb{F}_q^*$ is such that $b^2 \neq 1$. In the following tables, we list $q, m, b, s, g$ and $\#X(\mathbb{F}_{q^2})$ where $m, s, X$ and $f$ satisfy the hypotheses of Theorem 4.1.

| $q$ | $m$ | $b$ | $s$ | $g$ | $\#X(\mathbb{F}_{q^2})$ |
|-----|-----|-----|-----|-----|-------------------------|
| $3^2$ | 5 | $\xi_{32}^5$ | 3 | 4 | 154† |
| $3^2$ | 10 | $\xi_{32}^{10}$ | 4 | 8 | 226† |
| 5 | 6 | 2 | 4 | 4 | 66† |
| $5^2$ | 13 | $\xi_{52}^{13}$ | 0 | 6 | 926† |
| $5^2$ | 13 | 2 | 1 | 12 | 1226† |
| $5^2$ | 26 | 2 | 4 | 24 | 1826† |
| 7 | 4 | 2 | 3 | 3 | 92† |
| $7^2$ | 5 | $\xi_{72}^5$ | 1 | 4 | 2794† |
| $7^2$ | 10 | 3 | 4 | 8 | 3186† |
| $7^2$ | 25 | $\xi_{72}^{25}$ | 0 | 12 | 3578† |
| $7^2$ | 50 | $\xi_{72}^{50}$ | 10 | 44 | 6174† |
| $7^2$ | 50 | $\xi_{72}^{50}$ | 4 | 48 | 7106† |
| 13 | 14 | 2 | 0 | 6 | 326† |
| 13 | 14 | 5 | 4 | 12 | 482† |
| $13^2$ | 10 | $\xi_{132}^{10}$ | 3 | 9 | 31504 |
| $13^2$ | 34 | 8 | 4 | 32 | 39378† |
| 17 | 18 | 2 | 0 | 8 | 562† |
| 17 | 18 | 4 | 6 | 14 | 766† |
| 17 | 18 | 4 | 4 | 16 | 834† |
| 19 | 5 | 2 | 0 | 2 | 438† |
| 19 | 20 | 2 | 0 | 9 | 704† |

New entry

| $q$ | $m$ | $b$ | $s$ | $g$ | $\#X(\mathbb{F}_{q^2})$ | OLB |
|-----|-----|-----|-----|-----|-------------------------|-----|
| $7^2$ | 50 | $\xi_{72}^5$ | 5 | 47 | 5708 | 5658 |

Example 4.7 Let $f(x) = x^2 + b$ where $b \in \mathbb{F}_q^*$ is such that $b^2 \neq 1$. We list $q, m, b, s, g$ and $\#X(\mathbb{F}_{q^2})$ in the following tables where $m, s, X$ and $f$ satisfy the hypotheses of Theorem 4.1. We note that if $m = q + 1$ and $s = 2$ in the following tables, then the genus $g$ and the number of $\mathbb{F}_{q^2}$-rational points $\#X(\mathbb{F}_{q^2})$ satisfy Theorem 4.2.
Meet record

| $q$  | $m$ | $b$ | $s$ | $g$ | $\#\mathcal{X}(\mathbb{F}_{q^2})$ |
|------|-----|-----|-----|-----|----------------------------------|
| $3^2$ | 5   | $\xi_{3^2}$ | 0   | 6   | $190^+$                         |
| $3^2$ | 10  | $\xi_{3^2}$  | 2   | 17  | 288                             |
| 5    | 6   | 2   | 5   | 10  | $126^+$                         |
| $5^2$ | 26  | $\xi_{5^2}$ | 2   | 49  | 2400                            |
| $7^2$ | 5   | $\xi_{7^2}$ | 0   | 6   | $2990^+$                        |
| $7^2$ | 25  | 3   | 0   | 36  | $5930^+$                        |
| 11   | 2   | 3   | 1   | 2   | $166^+$                         |
| 11   | 3   | 3   | 2   | 4   | $210^+$                         |
| 11   | 6   | 3   | 5   | 10  | $342^+$                         |
| 13   | 2   | 5   | 1   | 2   | $222^+$                         |
| 13   | 14  | 2   | 2   | 25  | 624                             |
| 13   | 14  | 5   | 9   | 26  | $846^+$                         |
| $13^2$ | 5   | 8   | 2   | 8   | $31266^+$                       |
| $13^2$ | 10  | 5   | 2   | 17  | 34208                           |
| 17   | 2   | 3   | 1   | 2   | $358^+$                         |
| 17   | 3   | 3   | 2   | 4   | $426^+$                         |
| 17   | 6   | 3   | 5   | 10  | $630^+$                         |
| 17   | 9   | 5   | 0   | 12  | $698^+$                         |
| $17^2$ | 5   | 4   | 2   | 8   | $88146^+$                       |
| 19   | 5   | 4   | 0   | 6   | $590^+$                         |
| 19   | 10  | 14  | 5   | 16  | $970^+$                         |

New entry

| $q$  | $m$ | $b$ | $s$ | $g$ | $\#\mathcal{X}(\mathbb{F}_{q^2})$ | OLB |
|------|-----|-----|-----|-----|----------------------------------|-----|
| $7^2$ | 25  | $\xi_{7^2}$ | 5   | 46  | $6910^+$                        | 5589|
| $13^2$ | 34  | $\xi_{13^2}$ | 0   | 49  | 41112                           | 40273|
| 17   | 18  | 2   | 2   | 33  | 1088                            | 1083 |
| $17^2$ | 10  | 5   | 2   | 17  | 92928                           | 90470|
| 19   | 20  | 2   | 2   | 37  | 1368                            | 1356 |

New record

| $q$  | $m$ | $b$ | $s$ | $g$ | $\#\mathcal{X}(\mathbb{F}_{q^2})$ | OLB |
|------|-----|-----|-----|-----|----------------------------------|-----|
| $7^2$ | 10  | $\xi_{7^2}$ | 0   | 13  | 3576                            | 3258|
| $7^2$ | 10  | $\xi_{7^2}$ | 2   | 17  | 3968                            | 3808|

Example 4.8 Let $f(x) = x^3 + b \in \mathbb{F}_q[x]$, $m \geq 2$ be a divisor of $q + 1$ and $s$ be an integer $0 \leq s < m$. We consider the algebraic curve defined by

$$\mathcal{X} : \ y^m = \frac{f(x)f^s(x)}{x^s}.$$ 

The following tables consist of $q, m, b, s, g$ and $\#\mathcal{X}(\mathbb{F}_{q^2})$ which leads to meet record/new entry in the manYPoints table in [23]. Further, if $m = q + 1$, $s = 3$ and $b^2 = 1$ then the genus $g$ and the number of $\mathbb{F}_{q^2}$-rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ satisfy Proposition 4.4.
Remark 4.9 For $q = 5^2$ in Example 4.8, we obtain an explicit equation for a maximal curve of genus 36 over $\mathbb{F}_{5^4}$ given by $y^{26} = \frac{(x^2+1)^2}{x^3}$. The covered curve $y^{13} = \frac{(x^2+1)^2}{x^3}$ of genus 18 also provides a maximal curve. Moreover, in Example 4.7 we get a new maximal curve over $\mathbb{F}_{7^4}$ of genus 46. These genera have already appeared in [3] as the genus of this curve is covered by the Hermitian curve, however explicit equations for such curves were not provided in [3].

These three examples of explicit maximal curves are new entries in the manYPoints table [23] and rise a natural question, to decide if these curves are or not covered by the Hermitian curve.

Since there is no known method in general, it is a challenging problem to decide if two curves are birationally equivalent or not. Nevertheless, for some cases, it is possible to solve this problem using the software Magma [1]. For instance, we obtain the maximal curves $y^{13} = \frac{(x^2+1)^2}{x^3}$, for $i = 1, 3, 4, 5, 6, 7$, of genus 12 over $\mathbb{F}_{5^4}$. For $i = 1$ this curve is isomorphic to the maximal curve $y^{25} + y = x^2$ of genus 12 over $\mathbb{F}_{5^4}$ given in the manYPoints table. Furthermore, for $i = 3, 4, 5, 6, 7$, the curves $y^{13} = \frac{(x^2+1)^2}{x^3}$ over $\mathbb{F}_{5^4}$ are not isomorphic. Therefore, in this case, we obtain six non-isomorphic maximal curves of genus 12 over $\mathbb{F}_{5^4}$.

Example 4.10 Let $f(x) = x^4 + b$ where $b \in \mathbb{F}_q^*$ is such that $b^2 \neq 1$. In the following table, we list $q, m, b, s, g$ and $\#\mathcal{X}(\mathbb{F}_{q^2})$ where $m, s, \mathcal{X}$ and $f$ satisfy the hypotheses of Theorem 4.1.
Example 4.11 In the following tables, we list $q, m, f, s, g$ and $\#X(F_{q^2})$ where $m, s, X$ and $f \in \mathbb{F}_q[x]$ satisfy the hypotheses of Theorem 4.1.

| $q$ | $m$ | $f$ | $s$ | $g$ | $\#X(F_{q^2})$ |
|-----|-----|-----|-----|-----|-----------------|
| 2   | 3   | $x^3 + x + 1$ | 0   | 4   | 15$^+$          |
| 3   | 4   | $x^2 + 2x + 2$ | 0   | 3   | 28$^+$          |
| 3$^2$| 5   | $x^4 + x^2 + 2$ | 4   | 16  | 370$^+$         |
| 7   | 4   | $x^4 + x^2 + 5$ | 0   | 5   | 120$^+$         |
| 7   | 8   | $x^2 + 3x + 3$ | 6   | 9   | 176$^+$         |
| 7$^2$| 5   | $x^4 + 2x^2 + 3$ | 4   | 16  | 3970$^+$        |
| 11  | 6   | $x^2 + 3x + 10$ | 0   | 7   | 276$^+$         |
| 11  | 6   | $x^2 + 3x + 10$ | 2   | 9   | 320$^+$         |
| 11  | 12  | $x^2 + 3x + 10$ | 0   | 15  | 452$^+$         |
| 11  | 12  | $x^2 + 3x + 10$ | 8   | 19  | 540$^+$         |
| 19  | 10  | $x^2 + 6x + 18$ | 0   | 13  | 856$^+$         |
| 19  | 10  | $x^2 + 6x + 18$ | 2   | 17  | 1008$^+$        |
| 19  | 20  | $x^2 + 6x + 18$ | 8   | 35  | 1692$^+$        |
| 19  | 10  | $x^4 + x^2 + 7$ | 9   | 36  | 1730$^+$        |

Inspired by the previous constructions, we present some improvements obtained by using Artin-Schreier extensions.

Example 4.12 Let $X$ be the curve defined by the equation

$$X: \quad y^q + y = \frac{f(x)f'(x)}{x^s}$$

where $f \in \mathbb{F}_q[x]$ and $s \geq 0$ is an integer. We have the following improvements in the manYPoints table in [23].

| $q$ | $f(x)$ | $s$ | $g$ | $\#X(F_{q^2})$ | OLB |
|-----|--------|-----|-----|-----------------|-----|
| 7   | $x^4 + 1$ | 2   | 12  | 170             | 165 |
| 11  | $x^4 + 1$ | 2   | 20  | 442             | 430 |
| 13  | $x^4 + 1$ | 2   | 24  | 626             | 611 |
5 Curves over $\mathbb{F}_{q^2}$ from Sect. 3: the case of $\epsilon = 1$ and $\lambda = -1$

In this section, we consider the curve $\mathcal{X}$ in (3) with $\epsilon = 1$ and $\lambda = -1$. As in Sect. 4, we provide a lower bound for the number of $\mathbb{F}_{q^2}$-rational points on the curve $\mathcal{X}'$ when the polynomial $f \in \mathbb{F}_q[x]$ satisfies certain conditions. We also provide some examples of curves with many points.

**Theorem 5.1** Let $m \geq 2$ be a divisor of $q - 1$, $f \in \mathbb{F}_q[x]$ be a separable polynomial of degree $d$, satisfying $f(0) \neq 0$ and $(f, f^*) = 1$, and $s$ be an integer $0 \leq s < m$. Then the algebraic curve defined by the affine equation

$$\mathcal{X} : \ y^m = x^d f(x) / f^*(x)$$

has genus

$$g = d(m - 1) + 1 - (m, s).$$

Further if $(f, x^{q+1} - 1) = 1$, then the number of rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ over $\mathbb{F}_{q^2}$ satisfies

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m(q + 1) + 2N_f(\mathbb{F}_{q^2}).$$

**Proof** A direct application of Theorem 3.3 gives the genus of the curve defined in (10). To obtain an expression for the number of rational points for this curve, we observe that

$$\left(\frac{\alpha f(\alpha)}{f^*(\alpha)}\right)^{q^2 - 1} = 1,$$

which is equivalent to

$$((\alpha f(\alpha))^{q + 1} - f^*(\alpha)^{q + 1}) \left(\sum_{i=0}^{q-1} (\alpha f(\alpha))(q+1)i f^*(\alpha)^{(q+1)(\frac{q-1}{m} - 1 - i)}\right) = 0.$$

Let

$$h_1(x) = (x^d f(x))^{q+1} - f^*(x)^{q+1} \text{ and } h_2(x) = \sum_{i=0}^{q-1} (x^d f(x))(q+1)i f^*(x)^{(q+1)(\frac{q-1}{m} - 1 - i)}.$$

Then $h_1$ and $h_2$ are coprime. In fact, if $\alpha$ is a root of $h_1$, we have $(\alpha f(\alpha))^{q+1} = f^*(\alpha)^{q+1}$ and

$$h_2(\alpha) = \sum_{i=0}^{q-1} (\alpha f(\alpha))(q+1)i f^*(\alpha)^{(q+1)(\frac{q-1}{m} - 1 - i)} = \sum_{i=0}^{q-1} f^*(\alpha)^{(q+1)} f^*(\alpha)^{((q+1)(\frac{q-1}{m} - 1 - i)} = 0.$$

Also, since $(h_1, f^*) = (h_2, f^*) = 1$, we obtain

$$\# \left\{ \alpha \in \mathbb{F}_{q^2} | f(\alpha)f^*(\alpha) \neq 0 \text{ and } \frac{\alpha f(\alpha)}{f^*(\alpha)} \text{ is a } m\text{-th power in } \mathbb{F}_{q^2} \right\} = N_{h_1}(\mathbb{F}_{q^2}) + N_{h_2}(\mathbb{F}_{q^2}).$$

On the other hand, from Proposition 3.2, we know that each root in $\mathbb{F}_{q^2}$ of the polynomial $ff^*$ gives one rational point on the curve. Thus

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq 2N_f(\mathbb{F}_{q^2}) + m(N_{h_1}(\mathbb{F}_{q^2}) + N_{h_2}(\mathbb{F}_{q^2})).$$

(11)
Next we assume \((f, x^{q+1} - 1) = 1\). Then for \(\beta \in \mathbb{F}_{q^2}\) such that \(\beta^{q+1} = 1\), we have

\[
h_1(\beta) = (\beta^{s} f(\beta))^{q+1} - f^{*}(\beta)^{q+1} = \beta^d(\beta)^{q+1} - \beta^{d(q+1)} f(\beta)^{q+1} = 0.
\]

Therefore \(N_{h_1}(\mathbb{F}_{q^2}) \geq q + 1\). Hence the assertion follows from (11).

From the constructions given in Theorem 5.1, we obtain the following examples of curves with many points.

**Example 5.2** Let \(f(x) = x + b \in \mathbb{F}_{q^2}[x]\) be such that \(b \neq 0\) and \(b^2 \neq 1\), and \(m, s, \mathcal{X}\) be as defined in Theorem 5.1. Then \((f, f^*) = (f, x^{q+1} - 1) = 1\) and the curve \(\mathcal{X}\) has genus \(g = m - (m, s)\). We obtain the following tables of curves with many points.

| New entry | \(q\) | \(m\) | \(b\) | \(s\) | \(#\mathcal{X}(\mathbb{F}_{q^2})\) | OLBP |
|-----------|------|------|------|-----|----------------|------|
| \(5^2\)   | 24   | \(\xi_{5^2}^3\) | 8    | 16  | 1202           | 1191 |
| \(5^2\)   | 24   | 2    | 4    | 20  | 1450           | 1333 |
| \(5^2\)   | 16   | \(\xi_{5^2}^3\) | 6    | 14  | 3558           | 3372 |
| \(7^2\)   | 16   | \(\xi_{7^2}^3\) | 7    | 15  | 3684           | 3441 |
| \(7^2\)   | 24   | \(\xi_{7^2}^{13}\) | 5    | 23  | 4276           | 3995 |
| \(11^2\)  | 15   | \(\xi_{11^2}^{2}\) | 4    | 14  | 17674          | 17037|
| \(11^2\)  | 24   | \(\xi_{11^2}^{23}\) | 8    | 16  | 18050          | 17379|
| \(11^2\)  | 24   | 5    | 3    | 21  | 18968          | 18235|
| \(11^2\)  | 24   | \(\xi_{11^2}^{21}\) | 7    | 23  | 19204          | 18577|
| \(11^2\)  | 30   | \(\xi_{11^2}^{9}\) | 3    | 27  | 19988          | 19262|
| \(11^2\)  | 30   | \(\xi_{11^2}^{5}\) | 4    | 28  | 20106          | 19433|
| \(11^2\)  | 40   | \(\xi_{11^2}^{11}\) | 4    | 36  | 20962          | 20802|
| \(11^2\)  | 40   | \(\xi_{11^2}^{13}\) | 6    | 38  | 22246          | 21144|
| \(13^2\)  | 12   | \(\xi_{13^2}^{23}\) | 5    | 11  | 31972          | 31191|
| \(13^2\)  | 14   | \(\xi_{13^2}^{10}\) | 9    | 13  | 32260          | 31669|
| \(13^2\)  | 21   | \(\xi_{13^2}^{3}\) | 5    | 20  | 34318          | 33342|
| \(13^2\)  | 24   | \(\xi_{13^2}^{5}\) | 5    | 23  | 35428          | 34059|
| \(13^2\)  | 28   | \(\xi_{13^2}^{5}\) | 9    | 27  | 35452          | 35015|
| \(13^2\)  | 42   | \(\xi_{13^2}^{11}\) | 7    | 35  | 37550          | 36927|
| \(17^2\)  | 12   | \(\xi_{17^2}^{4}\) | 9    | 9   | 87938          | 87200|
| \(17^2\)  | 12   | \(\xi_{17^2}^{6}\) | 5    | 11  | 88828          | 88017|
| \(17^2\)  | 16   | \(\xi_{17^2}^{7}\) | 5    | 15  | 91044          | 89652|
| \(17^2\)  | 24   | \(\xi_{17^2}^{4}\) | 5    | 23  | 94996          | 92922|
| \(17^2\)  | 32   | \(\xi_{17^2}^{5}\) | 5    | 31  | 97604          | 96191|
| \(17^2\)  | 48   | \(\xi_{17^2}^{4}\) | 5    | 47  | 105124         | 102731|

**New record**

| \(q\) | \(m\) | \(b\) | \(s\) | \(#\mathcal{X}(\mathbb{F}_{q^2})\) | OLBP |
|-------|------|------|-----|----------------|------|
| \(17\) | 16   | 3    | 9   | 15  | 708       | 692  |
| \(11^2\) | 15   | \(\xi_{11^2}^{26}\) | 5    | 10  | 16952     | 16942|
| \(19\) | 18   | 2    | 3   | 15  | 866       | 782  |
Example 5.3  Let \( f(x) = x^2 + b \in \mathbb{F}_q[x] \) be such that \( b \neq 0 \) and \( b^2 \neq 1 \), and \( m, s, \mathcal{X} \) be as defined in Theorem 5.1. Then \( (f, f^*) = 1 \) and the curve \( \mathcal{X} \) has genus \( g = 2m - 1 - (m, s) \).

We have the following tables.

| \( q \) | \( m \) | \( b \) | \( s \) | \( g \) | \#\( \mathcal{X}(\mathbb{F}_q) \) |
|---|---|---|---|---|---|
| 7 | 6 | 2 | 4 | 4 | 102 |
| 11 | 8 | \( \xi_{30} \) | 4 | 7 | 15610† |
| 24 | 5 | \( \xi_{12} \) | 3 | 7 | 16308 |
| 13 | 12 | 2 | 4 | 8 | 362 |

### New entry

| \( q \) | \( m \) | \( b \) | \( s \) | \( g \) | \#\( \mathcal{X}(\mathbb{F}_q) \) | OLBM |
|---|---|---|---|---|---|---|
| 5 | 8 | \( \xi_{5} \) | 2 | 13 | 1128 | 1085 |
| 7 | 24 | \( \xi_{5} \) | 4 | 11 | 16940 | 16524 |
| 11 | 12 | \( \xi_{7} \) | 2 | 13 | 17480 | 16866 |
| 11 | 10 | \( \xi_{9} \) | 2 | 17 | 18128 | 17551 |
| 11 | 12 | \( \xi_{9} \) | 4 | 19 | 18436 | 17893 |
| 11 | 15 | \( \xi_{2} \) | 5 | 24 | 18964 | 18748 |
| 11 | 15 | \( \xi_{31} \) | 3 | 26 | 19564 | 19091 |
| 11 | 30 | \( \xi_{11} \) | 0 | 29 | 19684 | 19604 |
| 24 | 20 | \( \xi_{26} \) | 5 | 34 | 20644 | 20460 |
| 24 | 20 | \( \xi_{22} \) | 8 | 35 | 20964 | 20631 |
| 24 | 15 | \( \xi_{22} \) | 2 | 37 | 21528 | 20973 |
| 24 | 24 | \( \xi_{22} \) | 4 | 43 | 22372 | 22000 |
| 24 | 12 | \( \xi_{22} \) | 2 | 45 | 22472 | 22342 |
| 24 | 12 | \( \xi_{5} \) | 4 | 19 | 33748 | 33103 |
| 24 | 12 | \( \xi_{44} \) | 1 | 22 | 34374 | 33820 |
| 24 | 14 | \( \xi_{8} \) | 2 | 25 | 35400 | 34537 |
| 24 | 21 | \( \xi_{8} \) | 3 | 28 | 38314 | 37644 |
| 24 | 24 | \( \xi_{23} \) | 10 | 45 | 40136 | 39317 |
| 17 | 16 | \( \xi_{112} \) | 0 | 27 | 972 | 939 |
| 17 | 8 | \( \xi_{17} \) | 6 | 13 | 89224 | 88835 |
| 17 | 18 | \( \xi_{17} \) | 7 | 34 | 97494 | 97418 |
| 19 | 18 | \( \xi_{17} \) | 6 | 29 | 1156 | 1141 |
| 19 | 6 | \( \xi_{19} \) | 1 | 10 | 136782 | 135427 |
| 19 | 12 | \( \xi_{19} \) | 0 | 11 | 136612 | 135937 |
| 19 | 9 | \( \xi_{19} \) | 3 | 14 | 138208 | 137469 |
| 19 | 9 | \( \xi_{19} \) | 2 | 16 | 139650 | 138490 |
| 19 | 24 | \( \xi_{19} \) | 0 | 23 | 142372 | 142064 |
Example 5.4 Let \( f(x) = x^3 + b \in \mathbb{F}_q[x] \) be such that \( b \neq 0 \) and \( b^2 \neq 1 \), and \( m, s, \mathcal{X} \) be as defined in Theorem 5.1. Then \( (f, f^*) = 1 \) and the curve \( \mathcal{X} \) has genus \( g = 3m - 2 - (m, s) \). We have the following tables.

| New record |
|-------------|
| \( q \) | \( m \) | \( b \) | \( s \) | \( g \) | \( \#X(\mathbb{F}_{q^2}) \) | OLB |
|-------------|
| 17 | 8 | 4 | 2 | 13 | 648 | 612 |

| New entry |
|-------------|
| \( q \) | \( m \) | \( b \) | \( s \) | \( g \) | \( \#X(\mathbb{F}_{q^2}) \) |
|-------------|
| \( 7^2 \) | 12 | \( \xi_{12}^2 \) | 3 | 31 | 4680 | 4550 |
| \( 11^2 \) | 8 | \( \xi_{11}^{15} \) | 4 | 18 | 18486 | 17722 |
| \( 11^2 \) | 12 | \( \xi_{11}^1 \) | 0 | 22 | 19080 | 18406 |
| \( 11^2 \) | 12 | \( \xi_{11}^1 \) | 3 | 31 | 20820 | 19946 |
| \( 11^2 \) | 15 | \( \xi_{11}^1 \) | 6 | 40 | 22242 | 21486 |
| \( 11^2 \) | 24 | \( \xi_{11}^1 \) | 0 | 46 | 22608 | 22513 |
| \( 13^2 \) | 7 | \( \xi_{13}^2 \) | 3 | 18 | 33980 | 32864 |
| \( 13^2 \) | 12 | \( \xi_{13}^2 \) | 3 | 31 | 36792 | 35971 |
| \( 13^2 \) | 14 | \( \xi_{13}^2 \) | 7 | 33 | 37568 | 36449 |
| \( 13^2 \) | 14 | \( \xi_{13}^2 \) | 3 | 39 | 38732 | 37883 |
| 19 | 9 | 4 | 6 | 22 | 972 | 953 |

Example 5.5 Let \( f(x) = x^4 + b \in \mathbb{F}_q[x] \) be such that \( b \neq 0 \) and \( b^2 \neq 1 \), and \( m, s, \mathcal{X} \) be as defined in Theorem 5.1. Then \( (f, f^*) = 1 \) and the curve \( \mathcal{X} \) has genus \( g = 4m - 3 - (m, s) \). We have the following table of curves with many points.

| New entry |
|-------------|
| \( q \) | \( m \) | \( b \) | \( s \) | \( g \) | \( \#X(\mathbb{F}_{q^2}) \) |
|-------------|
| \( 7^2 \) | 8 | 3 | 5 | 28 | 4522 | 4342 |
| \( 11^2 \) | 6 | \( \xi_{11}^{20} \) | 0 | 15 | 17672 | 17208 |
| \( 11^2 \) | 8 | \( \xi_{11}^{21} \) | 4 | 25 | 19456 | 18919 |
| \( 11^2 \) | 12 | \( \xi_{11}^{14} \) | 6 | 39 | 22184 | 21315 |
| 13 | 6 | 2 | 1 | 20 | 554 | 537 |
| \( 13^2 \) | 6 | \( \xi_{13}^{22} \) | 0 | 15 | 32216 | 32147 |
| \( 13^2 \) | 8 | \( \xi_{13}^8 \) | 0 | 21 | 34584 | 33581 |
| \( 13^2 \) | 12 | \( \xi_{13}^{12} \) | 8 | 41 | 38784 | 38361 |
| \( 17^2 \) | 6 | \( \xi_{17}^{12} \) | 5 | 20 | 91826 | 91696 |

We finish this section by giving some additional improvements in the manYPoints table in [23].
Proof We start by computing the genus of the function field $K(x, y_1, y_2)$. By Theorem 4.1, we have $g(K(x, y_1)) = (2m_1d_1 - 2(d_1 - 1) - (m_1, s_1) - (m_1, 2d_1 - s_1))/2$. Also, for the
roots $\gamma_1, \ldots, \gamma_d$, of $f_1$ in $K$, we have the following ramification indices $e(P)$ in the extension $K(x, y_1)/K(x)$:

$$e(P) = \begin{cases} 
    m_1/(m_1, s_1), & \text{if } P \text{ is over } P_{0b}, \\
    m_1, & \text{if } P \text{ is over } P_{y_1} \text{ or } P_{y_1^{-1}}, \\
    m_1/(m_1, 2d_1 - s_1), & \text{if } P \text{ is over } P_{\infty}, \\
    1, & \text{otherwise}.
\end{cases}$$

Now we show that the extension $K(x, y_1, y_2)/K(x, y_1)$ is a Kummer extension. Let $\alpha_1, \ldots, \alpha_d \in K$ be the roots of $f_2$. The principal divisors of the function $x^{-s_2}f_2(x)f_2^{*}(x)$ in $K(x)$ is given by

$$(x^{-s_2}f_2(x)f_2^{*}(x))(x) = \sum_{i=1}^{d_2} (P_{\alpha_i} + P_{\alpha_i^{-1}}) - s_2P_0 - (2d_2 - s_2)P_{\infty},$$

and consequently

$$(x^{-s_2}f_2(x)f_2^{*}(x))(x_{y_1}) = \sum_{i=1}^{m_1} \sum_{j=1}^{d_2} (Q_{\alpha_i,j} + Q_{\alpha_i^{-1},j}) - s_2m_1/(m_1, s_1) \sum_{i=1}^{m_1} Q_{0,i}$$

$$- \frac{m_1(2d_2 - s_2)}{(m_1, 2d_1 - s_1)} \sum_{i=1}^{m_1} Q_{\infty,i},$$

where $Q_{\alpha_i,j}$, $Q_{\alpha_i^{-1},j}$, $Q_{0,i}$, and $Q_{\infty,i}$ are the extensions in $K(x, y_1)$ of the places $P_{\alpha_i}$, $P_{\alpha_i^{-1}}$, $P_0$ and $P_{\infty}$ respectively. Thus the ramification indices in the extension $K(x, y_1, y_2)/K(x, y_1)$ are given by

$$e(R) = \begin{cases} 
    m_2(m_1, s_1), & \text{if } R \text{ is over } Q_{0,i}, \\
    m_2(m_1, 2d_1 - s_1), & \text{if } R \text{ is over } Q_{\infty,i}, \\
    m_2, & \text{if } R \text{ is over } Q_{\alpha_i,j} \text{ or } Q_{\alpha_i^{-1},j}, \\
    1, & \text{otherwise}.
\end{cases}$$

We conclude that Eqs. (12) define an absolutely irreducible curve. Its genus follows from the Riemann–Hurwitz formula applied to $K(x, y_1, y_2)/K(x, y_1)$.

Next, we provide a lower bound for the number of $\mathbb{F}_{q^2}$-rational points. From [15, Theorem 4], it follows that

- for $\alpha \in \mathbb{F}_{q^2}^*$ such that $f_1^{*}f_1^{*}f_2^{*}(\alpha) \neq 0$, the curve $X$ has $m_1m_2$ points with coordinate $x = \alpha$ if and only if $\frac{f_1^{*}(\alpha)f_1^{*}(\alpha)}{\alpha^{3}}$ is a $m_i$-th power in $\mathbb{F}_{q^2}$ for $i \in \{1, 2\}$,
- for $\alpha \in \mathbb{F}_{q^2}^*$ such that $f_1^{*}(\alpha) = 0$, the curve $X$ has $m_2$ points with coordinate $x = \alpha$ if and only if $\frac{f_1^{*}(\alpha)f_1^{*}(\alpha)}{\alpha^{3}}$ is a $m_2$-th power in $\mathbb{F}_{q^2}$,
- for $\alpha \in \mathbb{F}_{q^2}^*$ such that $f_2^{*}(\alpha) = 0$, the curve $X$ has $m_1$ points with coordinate $x = \alpha$ if and only if $\frac{f_1^{*}(\alpha)f_1^{*}(\alpha)}{\alpha^{3}}$ is a $m_1$-th power in $\mathbb{F}_{q^2}$.

From the proof of Theorem 4.1, for $i \in \{1, 2\}$, we have

$$\left(\frac{f_i^{*}(\alpha)f_i^{*}(\alpha)}{\alpha^{3}}\right)^{q^2 - 1} = 1 \iff \alpha \text{ is a root of } h_{1,1}h_{1,2}$$
where
\[h_{i,1}(x) = (f_i(x)f_i^*(x))^{q-1} - x^{s_i(q-1)} \quad \text{and} \quad h_{i,2}(x) = \sum_{j=0}^{q-1} (f_i(x)f_i^*(x))^{(q-1)/j} x^{s_i(q-1)}\left(\frac{q+1}{m_i} - 1 - j\right).
\]

From the proof of Theorem 4.1, we also have that if \(\beta \in \mathbb{F}_{q^2}\) satisfies \(\beta^{(q+1,2(d_1-s_1),2(d_2-s_2))} = 1\), then \(h_{i,1}(\beta) = 0\). Further, for \(i \in \{1,2\}\), if \(\beta \in \mathbb{F}_{q}^*\) and \(f_i(\beta)f_i^*(\beta) \neq 0\), then \(h_{i,1}(\beta) = 0\). Hence,
\[
\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m_1m_2[(q+1,2(d_1-s_1),2(d_2-s_2)) + q - 3 - 2N_{f_1f_2}(\mathbb{F}_{q^2}^*)]
+ 2m_2N_{f_1}(\mathbb{F}_{q}^*) + 2m_1N_{f_2}(\mathbb{F}_{q}^*).
\]

\(\Box\)

**Example 6.2** For polynomials \(f_1, f_2 \in \mathbb{F}_q[x]\) satisfying the conditions of Theorem 6.1 and the curve \(\mathcal{X}\) as defined in (12), we have the following table.

| \(q\) | \(m_1\) | \(m_2\) | \(s_1\) | \(s_2\) | \(f_1\) | \(f_2\) | \(g\) | \#\(\mathcal{X}(\mathbb{F}_{q^2})\) | OLB |
|------|------|------|------|------|------|------|------|----------------|------|
| 19   | 2    | 4    | 4    | 4    | \(x^4 + 2\) | \(x^4 + 7\) | 33   | 1280          | 1248 |

Also, for a self-reciprocal polynomial \(f_1 \in \mathbb{F}_q[x]\), we have the following improvements in the manYPoints table in [23].

| \(q\) | \(m_1\) | \(m_2\) | \(s_1\) | \(s_2\) | \(f_1\) | \(f_2\) | \(g\) | \#\(\mathcal{X}(\mathbb{F}_{q^2})\) | OLB |
|------|------|------|------|------|------|------|------|----------------|------|
| 11   | 3    | 3    | 2    | 2    | \(x^2 + 1\) | \(x^2 + 7\) | 16   | 402           | 370  |
| 11   | 3    | 6    | 0    | 1    | \(x^2 + 1\) | \(x^2 + 10\) | 22   | 462           | 459  |
| 17   | 3    | 6    | 2    | 2    | \(x^2 + 1\) | \(x^2 + 3\)  | 37   | 1224          | 1179 |

| \(q\) | \(m_1\) | \(m_2\) | \(s_1\) | \(s_2\) | \(f_1\) | \(f_2\) | \(g\) | \#\(\mathcal{X}(\mathbb{F}_{q^2})\) | OLB |
|------|------|------|------|------|------|------|------|----------------|------|
| 5    | 3    | 6    | 2    | 5    | \(x^2 + 1\) | \(x^2 + 4\)  | 22   | 174           | 168  |

Analogously to Theorem 6.1, we have the following result corresponding to another type of fiber product.

**Theorem 6.3** Let \(i \in \{1,2\}\). Let \(m_i \geq 2\) be a divisor of \(q-1\), \(s_i\) be an integer \(0 \leq s_i < m_i\) and \(f_i\) be a separable polynomial in \(\mathbb{F}_q[x]\) of degree \(d_i\) satisfying \(f_i(0) \neq 0\) and \((f_i,f_i^*) = (f_1^*,f_2^*) = 1\). Then the curve \(\mathcal{X}\) defined by the affine equations
\[
\mathcal{X} : \begin{cases} y_2^{m_2} = \frac{x^2 f_2(x)}{f_2^*(x)} \\
y_1^{m_1} = \frac{x^1 f_1(x)}{f_1^*(x)} \end{cases}
\]

(13)
has genus
\[ g = m_1m_2(d_1 + d_2) - d_1m_2 - d_2m_1 + 1 - \kappa \]
where \( \kappa = (m_1m_2, s_1m_2, s_2m_1) \). Further, if \( \mathbb{F}_{q^2} \) is the full constant field of the function field \( \mathbb{F}_{q^2}(\mathcal{X}), [\mathbb{F}_{q^2}(\mathcal{X}), \mathbb{F}_{q^2}(x)] = m_1m_2 \) and \( (f_i, x^{d_i+1} - 1) = 1 \) for \( i \in \{1, 2\} \), then the number of \( \mathbb{F}_{q^2} \)-rational points \( \#\mathcal{X}(\mathbb{F}_{q^2}) \) of the curve \( \mathcal{X} \) satisfies
\[ \#\mathcal{X}(\mathbb{F}_{q^2}) \geq m_1m_2(q + 1). \]

**Example 6.4** For polynomials \( f_1, f_2 \in \mathbb{F}_q[x] \) satisfying the conditions of Theorem 6.3 and the curve \( \mathcal{X} \) as defined in (13), we have the following tables.

| New entry  | \( q \) | \( m_1 \) | \( m_2 \) | \( s_1 \) | \( s_2 \) | \( f_1 \) | \( f_2 \) | \( g \) | \( \#\mathcal{X}(\mathbb{F}_{q^2}) \) | OLB |
|------------|-------|-------|-------|-------|-------|-------|-------|-------|-----------------|-----|
| 13         | 3     | 3     | 0     | 2     |       | \( x^3 + 3x + 3 \) | \( x + 4 \) | 16    | 558             | 464 |
| 13         | 4     | 4     | 1     | 1     |       | \( x + 2 \)      | \( x + 6 \) | 21    | 568             | 556 |
| 17         | 4     | 4     | 1     | 1     |       | \( x + 3 \)      | \( x + 8 \) | 21    | 808             | 794 |

| New record | \( q \) | \( m_1 \) | \( m_2 \) | \( s_1 \) | \( s_2 \) | \( f_1 \) | \( f_2 \) | \( g \) | \( \#\mathcal{X}(\mathbb{F}_{q^2}) \) | OLB |
|------------|-------|-------|-------|-------|-------|-------|-------|-------|-----------------|-----|
| 13         | 2     | 4     | 0     | 2     |       | \( x^4 + 4 \) | \( x + 5 \) | 11    | 444             | 400 |
| 13         | 2     | 6     | 0     | 2     |       | \( x + 3 \) | \( x + 6 \) | 13    | 444             | 438 |

**Acknowledgements**
The authors would like to thank the anonymous reviewers for their valuable comments and helpful suggestions which improved both the quality and presentation of this paper.

**Data availability** Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

**Author details**
1Department of Mathematics, Birla Institute of Technology and Science-Pilani, Hyderabad Campus, Hyderabad, Telangana 500078, India, 1Instituto de Matemática, Universidade Federal do Rio de Janeiro, Cidade Universitária, Rio de Janeiro CEP: 21941-909, Brazil.

Received: 15 December 2022  Accepted: 3 July 2023  Published online: 30 July 2023

**References**
1. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. 24(3–4), 235–265 (1997). Computational Algebra and Number Theory (London, 1993)
2. Coulter, R.S.: The number of rational points of a class of Artin–Schreier curves. Finite Fields Appl. 8(4), 397–413 (2002)
3. Danisman, Y., Ozdemir, M.: On the genus spectrum of maximal curves over finite fields. J. Discret. Math. Sci. Cryptogr. 18(5), 513–529 (2015)
4. Garcia, A., Garzon, A.: On Kummer covers with many rational points over finite fields. J. Pure Appl. Algebra 185(1–3), 177–192 (2003)
5. Garcia, A., Quoos, L.: A construction of curves over finite fields. Acta Anth. 98(2), 181–195 (2001)
6. Garcia, A., Stichtenoth, H., Xing, C.-P.: On subfields of the Hermitian function field. Compos. Math. 120(2), 137–170 (2000)
7. Goppa, V.D.: Codes that are associated with divisors. Problemy Peredachi Informatsii 13(1), 33–39 (1977)
8. Goppa, V.D.: Codes on algebraic curves. Sov. Math. Dokl. 24(1), 170–172 (1981)
9. Howe, E.W.: Curves of medium genus with many points. Finite Fields Appl. 47, 145–160 (2017)
10. Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28(3), 721–724 (1982), 1981
11. Kawakita, M.Q.: Kummer curves and their fibre products with many rational points. Appl. Algebra Eng. Commun. Comput. 14(1), 55–64 (2003)
12. Kawakita, M.Q.: Certain sextics with many rational points. Adv. Math. Commun. 11(2), 289–292 (2017)
13. Moisio, M.: On the number of rational points on some families of Fermat curves over finite fields. Finite Fields Appl. 13(3), 546–562 (2007)
14. Oliveira, D., Martínez, F.E.: Artin–Schreier curves given by \( \mathbb{F}_q \)-linearized polynomials. ArXiv Preprint (2020). arXiv:2012.01534
15. Özbudak, F., Temür, B.G.: Finite number of fibre products of Kummer covers and curves with many points over finite fields. Des. Codes Cryptogr. 70(3), 385–404 (2014)
16. Özbudak, F., Temür, B.G., Yayla, O.: Further results on fibre products of Kummer covers and curves with many points over finite fields. Adv. Math. Commun. 10(1), 151–162 (2016)
17. Rojas-León, A.: On the number of rational points on curves over finite fields with many automorphisms. Finite Fields Appl. 19, 1–15 (2013)
18. Rökaeus, K.: New curves with many points over small finite fields. Finite Fields Appl. 21, 58–66 (2013)
19. Stichtenoth, H.: Algebraic Function Fields and Codes. Graduate Texts in Mathematics, vol. 254, 2nd edn. Springer, Berlin (2009)
20. van der Geer, G.: Hunting for curves with many points. In: Coding and Cryptology, vol. 5557. Lecture Notes in Computer Science, pp. 82–96. Springer, Berlin (2009)
21. van der Geer, G., van der Vlugt, M.: How to construct curves over finite fields with many points. In: Arithmetic Geometry (Corvona, 1994). Symposium on Mathematics, vol. XXXVII, pp. 169–189. Cambridge University Press, Cambridge (1997)
22. van der Geer, G., van der Vlugt, M.: Kummer covers with many points. Finite Fields Appl. 6(4), 327–341 (2000)
23. van der Geer, G., Howe, E. W., Lauter, K. E., Ritzenthaler, C.: Tables of curves with many points. (2009). http://www.manypoints.org. Accessed 8 Oct 2021
24. Xing, C., Yeo, S.L.: Algebraic curves with many points over the binary field. J. Algebra 311(2), 775–780 (2007)

Publisher’s Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightholder(s), author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.