On Kummer covers with many rational points over finite fields

Arnaldo Garcia\textsuperscript{a,*}, Alvaro Garzon\textsuperscript{b}

\textsuperscript{a}IMPA, Estrada Dona Castorina 110, 22.460-320, Rio de Janeiro, Brazil
\textsuperscript{b}Departamento de Matemática, Apartado Aereo 2188, Cali-Valle-Colombia

Received 21 August 2002; received in revised form 10 February 2003
Communicated by J. Walker

Abstract

We give a simple and effective method for the construction of algebraic curves over finite fields with many rational points. The curves constructed are Kummer covers or fibre products of Kummer covers of the projective line.

\copyright 2003 Elsevier B.V. All rights reserved.

MSC: 11G20; 14G15; 14H25

1. Introduction

Let \( C \) be a nonsingular, projective, geometrically irreducible curve defined over a finite field \( \mathbb{F}_q \) with \( q \) elements. Let \( \mathcal{C}(\mathbb{F}_q) \) denote the set of \( \mathbb{F}_q \)-rational points on \( \mathcal{C} \); i.e., points on \( \mathcal{C} \) having all coordinates in \( \mathbb{F}_q \). A celebrated theorem of A. Weil gives in particular the following upper bound:

\[
\#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + 2\sqrt{qg(\mathcal{C})},
\]

\cite{Weil1948}
where \( g(\mathcal{C}) \) stands for the genus of the curve \( \mathcal{C} \). If the cardinality \( q \) of the finite field is not a square, the upper bound above was improved by J.-P. Serre substituting \( 2\sqrt{q} \) by its integer part \( \lfloor 2\sqrt{q} \rfloor \). If the cardinality \( q \) is a square (say \( q = r^2 \)) then the curve \( \mathcal{C} \) is called maximal over \( \mathbb{F}_r \) if the cardinality \( \#\mathcal{C}(\mathbb{F}_r) \) attains Weil’s upper bound; i.e., \( \#\mathcal{C}(\mathbb{F}_r) = r^2 + 1 + 2rg(\mathcal{C}) \), see for example [1,2,4,8].

The interest in curves over finite fields with many rational points with respect to their genera (i.e., with \( \#\mathcal{C}(\mathbb{F}_q) \) close to known upper bounds; e.g., see the tables in [6]) was greatly renewed after Goppa’s construction of linear codes with good parameters from such curves. Other applications include: low-discrepancy sequences, stream ciphers, hash functions, finite geometries, etc… We refer to [9] for an extensive study on this subject and its connections with Ray Class Fields, Hilbert Class Fields, Drinfeld Modules, etc.

The aim here is to present an elementary and effective method for the construction of Kummer covers of the projective line over finite fields with many rational points. The key idea comes from [5] (see also [3]) and that is the construction of rational functions \( f(x)/r(x) \) in the rational function field \( \mathbb{F}_q(x) \) having the value 1 for many elements \( x = \beta \) in \( \mathbb{F}_q \).

The paper is organized as follows: in Section 2 we present our method for the construction of good curves \( \mathcal{C} \) and we explain how one computes the genus and the number of rational points; Section 3 is just to single out an important special case; in Section 4 and Section 5 we give several examples based on the two preceding sections, and in Section 6 we consider fibre products of two curves, both of them obtained by the method presented in Section 2.

Three things are worth mentioning:

(a) Many of the records on the tables (see [6]) that we match were obtained by totally different methods; so here we have a unified way to get those records.
(b) Our construction involves the choice of a divisor \( m \) of the cardinality \( (q-1) \) of the multiplicative group of the finite field \( \mathbb{F}_q \) in question, and we have almost always chosen \( m \) small enough so that the resulting genus \( g \) satisfies \( g \leq 50 \). This is done in order to compare with the tables in [6].
(c) We can always determine the exact number of rational points in the case \( m = q - 1 \); however if \( m \) is a proper divisor of \( (q-1) \) we sometimes used the computer program Mathematica to complete the determination of the rational points (see end of Section 2).

We have obtained two new records:

- A curve of genus 34 over \( \mathbb{F}_{16} \) with 183 rational points (see Example 6.1).
- A curve of genus 13 over \( \mathbb{F}_{81} \) with 243 rational points (see Example 5.1).

In the following tables we summarize the good pairs \((g, N)\) obtained in the examples of Sections 4, 5 and 6 here, where \( g = g(\mathcal{C}) \) and \( N = \#\mathcal{C}(\mathbb{F}_q) \). For the cases of characteristic \( p = 5 \), we have used a table of curves by V. Shabat that is not available on the web at present.
2. The method

Let \( f(x) \) and \( \ell(x) \) be two polynomials in \( \mathbb{F}_q[x] \) such that \( \deg f(x) \geq \deg \ell(x) \). Consider the euclidian division of \( f(x) \) by \( \ell(x) \); i.e.,

\[
f(x) = h(x)\ell(x) + r(x)
\]

for some polynomials \( h(x), r(x) \in \mathbb{F}_q[x] \) with \( \deg r(x) < \deg \ell(x) \). We will always assume that \( r(x) \neq 0 \) (i.e., we will always assume that \( f(x) \) is not a multiple of \( \ell(x) \)). The method for the construction is then to consider the nonsingular projective model \( \mathcal{C} \) of the curve given by the affine Kummer equation:

\[
y^m = f(x)/r(x), \quad \text{with } m \text{ a divisor of } (q - 1).
\]

As was shown in [7], the genus \( g(\mathcal{C}) \) can be derived from the multiplicities of the zeros and poles of the function \( f(x)/r(x) \in \mathbb{F}_q[x] \) (see [11, Proposition III.7.3]). If \( x = \alpha \in \mathbb{F}_q \) is a zero or a pole for \( f(x)/r(x) \) with multiplicity \( m_\alpha \), then we have \( d_\alpha \) points on the curve \( \mathcal{C} \) with first coordinate \( x = \alpha \), where

\[
d_\alpha = \gcd(m, m_\alpha).
\]

These \( d_\alpha \) points have ramification index \( e_\alpha := m/d_\alpha \) and they have different exponent equal to \( (e_\alpha - 1) \), by Dedekind’s Different Theorem. The same holds for the points
of $\mathcal{C}$ above the point at infinity; i.e., for $x = \infty$ one defines its multiplicity by $m_\infty = (\deg f(x) - \deg r(x))$ and, similarly,

$$d_\infty = gcd(m, m_\infty) \quad \text{and} \quad e_\infty = m/d_\infty. \quad (4)$$

It now follows from Hurwitz’s genus formula that:

$$2g(\mathcal{C}) = 2 + m \left( -2 + \sum_{x \in \mathbb{F}_q \cup \{\infty\}} (1 - d_x/m) \right). \quad (5)$$

The sum over $x \in \mathbb{F}_q \cup \{\infty\}$ in Formula (5) is a finite sum over only the zeros and poles of the rational function $f(x)/r(x)$.

From Formula (5), we see that $g(\mathcal{C})$ is smaller as the rational function $f(x)/r(x)$ has fewer distinct zeros and poles. So it is desirable to have a product $f(x) \cdot r(x)$ with lots of multiple roots. Typically we take $f(x)$ as a power of a polynomial and we try to get a remainder $r(x)$ with many multiple roots.

Now we turn to the rational points over $\mathbb{F}_q$ of the curve $\mathcal{C}$ given by Eq. (2).

Roots of $h(x)/r(x)=0$: If $\beta \in \mathbb{F}_q$ satisfies $h(\beta) \cdot \ell(\beta)=0$ and $f(\beta) \neq 0$, then the value of $f(x)/r(x)$ at $x = \beta$ is equal to 1 (see Formula (1)). This guarantees that we have $m$ rational points on $\mathcal{C}$ with first coordinate $x = \beta$ as above. So in order to have many rational points over $\mathbb{F}_q$ we will always take $r(x)$ as a separable polynomial having all roots in the finite field $\mathbb{F}_q$.

Ramification points: If $x = x \in \mathbb{F}_q \cup \{\infty\}$ is a zero or a pole for the function $f(x)/r(x)$ with multiplicity $m_x$, then we have $d_x$ points on $\mathcal{C}$ with first coordinate $x = x$. If this zero or pole is rational (i.e., if $x = x \in \mathbb{F}_q \cup \{\infty\}$), then it may happen that the $d_x$ points with $x = x$ are again rational points over $\mathbb{F}_q$. Here is how one decides: We can assume that $x$ is a zero for $f(x)/r(x)$ (otherwise substitute $y$ by $1/y$) and hence we write

$$y^m = k(x) \cdot (x - \alpha)^{m_x} \quad \text{or} \quad \left(\frac{y^{m/d_x}}{(x - \alpha)^{m_x/d_x}}\right)^{d_x} = k(x),$$

where $k(x) \in \mathbb{F}_q(x)$ with $k(x) \neq 0$ and $k(x) \neq \infty$. Then the $d_x$ points are all rational over $\mathbb{F}_q$ if and only if $k(\alpha)$ is a $d_x$th power of an element of $\mathbb{F}_q$.

Case $m = q - 1$: In this case we see from Eq. (2) that a rational point on $\mathcal{C}$ which is neither a zero nor a pole for the rational function $f(x)/r(x)$ must have second coordinate satisfying $y \in \mathbb{F}_q^*$ and hence $y^{q - 1} = 1$. Hence in this case besides the possible rational ramification points, the other rational points on $\mathcal{C}$ must come from $x = \beta \in \mathbb{F}_q$ with $h(\beta) \cdot \ell(\beta) = 0$ and $f(\beta) \neq 0$.

Case $m < (q - 1)$: In this case it is in general harder to determine the exact number of rational points on $\mathcal{C}$ over $\mathbb{F}_q$. Besides the ones obtained as in the case $m = q - 1$, one also has to consider the following:

For $x = y \in \mathbb{F}_q$ which is not a zero or a pole for $f(x)/r(x)$, we consider the element $f(\gamma)/r(\gamma) \in \mathbb{F}_q^*$. This element $\tilde{\gamma} := f(\gamma)/r(\gamma) \in \mathbb{F}_q^*$ may satisfy

$$\tilde{\gamma} \neq 1 \quad \text{and} \quad \tilde{\gamma} \text{ is a } m \text{th power of an element of } \mathbb{F}_q. \quad (6)$$
For each \( \gamma \in \mathbb{F}_q \) as above with \( \tilde{\gamma} \) satisfying (6), we have \( m \) rational points on \( \mathcal{C} \) with first coordinate \( x= \gamma \). So in practice (when \( m \) is a proper divisor of \( (q-1) \)), after having a good candidate for a curve \( \mathcal{C} \) with many rational points with respect to its genus \( g(\mathcal{C}) \), we sometimes have carried out a computer search to determine the cardinality \( \mathcal{K} \) of the set of such elements

\[
\mathcal{K} := \# \{ \gamma \in \mathbb{F}_q \mid \gamma \text{ is not zero or pole for } f(x)/r(x), \tilde{\gamma} \neq 1 \text{ and } \tilde{\gamma} \text{ is } m\text{th power in } \mathbb{F}_q \}.
\]

(7)

This then gives rise to \( \mathcal{K}m \) “extra rational points” on the curve \( \mathcal{C} \).

3. An important special case of the method

Many of the curves \( \mathcal{C} \) with many rational points over \( \mathbb{F}_q \) with respect to the genus \( g(\mathcal{C}) \) that we will construct are obtained through this special case.

Let \( \ell(x) \in \mathbb{F}_q[x] \) be a separable polynomial having all roots in the finite field \( \mathbb{F}_q \). Let \( g(x) \in \mathbb{F}_q[x] \) be another polynomial which is relatively prime to the polynomial \( \ell(x) \). Then there are polynomials \( h(x) \) and \( v(x) \) in \( \mathbb{F}_q[x] \) such that:

\[
v(x)g(x) = h(x)\ell(x) + 1.
\]

(8)

We then consider the nonsingular projective model \( \mathcal{C} \) of the curve given by

\[
y^m = v(x)g(x), \quad \text{with } m \text{ a divisor of } (q-1).
\]

(9)

As in Section 2 we usually take \( g(x) \) highly inseparable (e.g., a power of a polynomial) and we try to get the polynomial \( v(x) \in \mathbb{F}_q[x] \) from Formula (8) also highly inseparable. As before this is done in order to get a low genus for the constructed curve \( \mathcal{C} \), since from Formula (5) we see that the genus depends essentially on the number of distinct roots of the polynomial \( f(x) := v(x)g(x) \).

One should think of the polynomial \( g(x) \in \mathbb{F}_q[x] \) as an auxiliary polynomial that is used to construct the polynomial \( f(x) := v(x)g(x) \) whose remainder in the division by \( \ell(x) \) satisfies \( r(x) = 1 \) (compare Formulas (8) and (1)).

4. Examples based on Section 2

Suppose that \( q = r^n \) with \( n \geq 2 \). An irreducible polynomial in \( \mathbb{F}_r[x] \) of degree \( n \) has all roots in \( \mathbb{F}_q \). A natural choice for the polynomial \( \ell(x) \) is then to take certain products of such irreducible polynomials.

Example 4.1. Let \( m \) be a divisor of \( (r^2 - 1) \) and \( d := \gcd(m, r - 1) \). Let \( w \in \mathbb{F}_{r^2} \) be such that \( w^d = -1 \). Then the curve \( \mathcal{C} \) given by

\[
y^{m/d} = w(x^r - x)^{(r-1)/d}
\]

is a maximal curve over \( \mathbb{F}_{r^2} \) with \( g(\mathcal{C}) = (r - 1) \cdot (m - d)/2d \).
The point here is to obtain by our method the equation for \( C \). We consider
\[
\ell(x) = \frac{x^2 - x}{x^2 - x} = (x' - x)^{-1} + 1,
\]
i.e., \( \ell(x) \) is the product of all irreducible polynomials in \( \mathbb{F}_r[x] \) of degree 2. Then taking \( f(x) = (x' - x)^{-1} \), we have \( f(x) = \ell(x) - 1 \); i.e., we get \( r(x) = -1 \). We are then led by our method to consider the equation \( y^m = -(x' - x)^{-1} \).

We then extract the \( d \)th root to obtain the defining equation.

As a variation of Example 4.1 we have the next example where we take the same polynomial \( \ell(x) \) but a different polynomial for \( f(x) \).

**Example 4.2** \((n = 2 \text{ and } r = 4)\). This is an example of a curve \( C \) over \( \mathbb{F}_{16} \) with \( g(C) = 4 \) and \(#C(\mathbb{F}_{16}) = 45 \). This is the best value known (see the table in [6]). This curve \( C \) over \( \mathbb{F}_{16} \) can be given by
\[
y^3 = \frac{(x^3 + x^2 + 1)^4}{x^3(x + 1)^3(x^3 + x + 1)}.
\]

Taking \( f(x) = (x^3 + x^2 + 1)^4 \) and \( \ell(x) = (x^{16} - x)/(x^4 - x) \), we have after some computation that \( r(x) = x^3(x + 1)^3(x^3 + x + 1) \). This shows that the equation for \( C \) is obtained by our method. That the genus is equal to 4 follows from the fact that we have exactly 6 ramified points and they are totally ramified (corresponding to the solutions of \((x^3 + x^2 + 1)(x^3 + x + 1) = 0\)). These points are not rational over \( \mathbb{F}_{16} \). Besides the 12 roots of \( \ell(x) = 0 \), one can check easily that \( x = 0, x = 1 \) and \( x = \infty \) also give rise to rational points of \( C \) over \( \mathbb{F}_{16} \). Hence \( #C(\mathbb{F}_{16}) \geq (12 + 3)3 = 45 \). The other possible rational points must have first coordinate satisfying \( x = \gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2 \). A direct computation shows
\[
\frac{(\gamma^3 + \gamma^2 + 1)^4}{\gamma^3(\gamma + 1)^3(\gamma^3 + \gamma + 1)} = \left( \frac{1}{\gamma} \right)^2,
\]
and this shows that the points on \( C \) with \( x = \gamma \) are not rational over \( \mathbb{F}_{16} \).

**Remark 1.** (a) Example 4.2 is an instance where \( m = 3 \) is a proper divisor of \((q - 1)\) and we have determined the exact number of rational points over \( \mathbb{F}_q \) without performing a computer search (i.e., we have shown that \( K = 0 \)).

(b) The curve \( C \) in Example 4.2 can also be given by the simpler equation
\[
z^3 = (x^3 + x^2 + 1)/(x^3 + x + 1).
\]
In fact take \( z = y(x + 1)/(x^3 + x^2 + 1) \). In several other examples to come, one can perform similar simplifications for the defining equations of the curves \( C \), but we have preferred not to perform them in order to make more evident that the equations are really obtained through the method in Section 2.
Example 4.3. Let $r$ be a power of an odd prime number and let $m$ be a divisor of $(r^2 - 1)$. The curve $C$ over $\mathbb{F}_{r^2}$ defined by the affine Kummer equation

$$y^m = x'(x' + 1)^t/(x' - 1),$$

with $t = (r - 1)/2$,

has genus satisfying

$$2g(C) = (m - 1)(r - 3) + 2(m - d),$$

where $d = \gcd(m, t)$, and moreover $\#C(\mathbb{F}_{r^2}) \geq m(r^2 - 1)/2 + (r - 1) + 2d$.

Taking $\ell(x) = (x^{(r+1)} + 1)$ and $f(x) = x'(x' + 1)^r$, we have

$$f(x) = \ell(x) + r(x)$$

with $r(x) = x^t - 1$.

This explains the equation for the curve. We omit further details.

Remark 2. Some of the curves in Example 4.3 are maximal curves over $\mathbb{F}_{r^2}$. For instance this is the case if we have: $(r, m) \in \{(3, 2), (9, 5), (5, 3)\}$.

In the next two examples we are going to construct four curves over $\mathbb{F}_{16}$ whose numbers of rational points attain the best known values (see the table in [6]).

Example 4.4. We will construct here two curves $C_1$ and $C_2$ over $\mathbb{F}_{16}$ satisfying:

- $g(C_1) = 2$ and $\#C_1(\mathbb{F}_{16}) = 33$; i.e., $C_1$ is maximal.
- $g(C_2) = 12$ and $\#C_2(\mathbb{F}_{16}) = 83$.

Consider the curve $C$ over $\mathbb{F}_{16}$ defined by

$$y^m = (x^3 + 1)^2/(x + 1),$$

with $m$ a divisor of $15 = r^2 - 1$.

The curve $C_1$ (resp. $C_2$) corresponds to the choice $m = 5$ (resp. $m = 15$).

Taking $\ell(x) = (x^3 - 1)/(x - 1)$ (i.e., the roots of $\ell(x)$ are exactly the primitive 5th roots of unity inside $\mathbb{F}_{16}^*$) and $f(x) = (x^3 + 1)^2$, one has $f(x) = (x^5 + x)\ell(x) + (x + 1)$. This explains the equation for the curve $C$ here. It is easy to see that

$$2g(C) = (m - 1) + (m - d),$$

with $d = \gcd(m, 5)$.

One can verify directly that $\#C(\mathbb{F}_{16}) = 5m + d + 3$.

Example 4.5. We will now construct two curves $C_1$ and $C_2$ over $\mathbb{F}_{16}$ satisfying:

- $g(C_1) = 6$ and $\#C_1(\mathbb{F}_{16}) = 65$; i.e., $C_1$ is maximal.
- $g(C_2) = 20$ and $\#C_2(\mathbb{F}_{16}) = 127$.

Consider the curve $C$ over $\mathbb{F}_{16}$ given by

$$y^m = (x^2 + x + 1)^4/x^6(x + 1),$$

where $m$ is a divisor of $15$.

The curve $C_1$ (resp. $C_2$) corresponds to the choice $m = 5$ (resp. $m = 15$).

Taking $\ell(x) = (x^4 + x + 1)(x^5 - 1)/(x - 1)$ and $f(x) = (x^2 + x + 1)^4$, we get

$$f(x) = \ell(x) + r(x)$$

with $r(x) = x^6(x + 1)$.
This explains the equation for the curve \( C \) here. One can show that

- \[ 2g(C) = 2(m - 1) + (m - d), \text{ with } d = \gcd(m, 3). \]
- \[ \#C(F_{16}) = \begin{cases} 12m + d + 4 & \text{if } m = 5 \\ 8m + d + 4 & \text{if } m \neq 5. \end{cases} \]

It follows from [10] that the curve \( C_1 \) above admits the simpler model \( z^4 + z = w^5 \).

Before considering curves over finite fields \( F_q \) with \( q = r^n \) and \( n \geq 3 \) we will give two more examples leading to good curves over \( F_{25} \). In these two examples we will use the following irreducible polynomials of degree 2 over \( F_5 \):

- \( \ell_1(x) = x^2 + 2 \), \( \ell_2(x) = x^2 - 2 \), \( \ell_3(x) = x^2 - x + 1 \),
- \( \ell_4(x) = x^2 + 2x - 2 \), \( \ell_5(x) = x^2 + 2x - 1 \), \( \ell_6(x) = x^2 - 2x - 2 \).

**Example 4.6.** The curve \( C \) over \( F_{25} \) given by \( y^8 = x(x - 1)^3(x + 2) \) has \( g(C) = 7 \) and \( \#C(F_{25}) = 84 \).

As in Example 4.1, the point here is to obtain the equation defining the curve \( C \) using our method. For that we consider

\[ \ell(x) = \ell_1(x)\ell_2(x)\ell_4(x)\ell_6(x) \quad \text{and} \quad f(x) = x^3(x + 2)^3(x - 1)^9. \]

We then have \( f(x) = h(x)\ell(x) + 1 \), with \( h(x) = (x + 1)(x - 2)^2(x^4 + 2x^2 - 2) \). We are then led to consider the equation \( y^{24} = x^3(x + 2)^3(x - 1)^9 \). Taking the third root of the equation above we get the equation for the curve.

**Example 4.7.** We are going to construct curves \( C_1 \), \( C_2 \) and \( C_3 \) over \( F_{25} \) with:

- \( g(C_1) = 3 \) and \( \#C_1(F_{25}) = 52 \).
- \( g(C_2) = 19 \) and \( \#C_2(F_{25}) = 132 \).
- \( g(C_3) = 43 \) and \( \#C_3(F_{25}) = 252 \).

Consider the curve \( C \) over \( F_{25} \) defined by

\[ y^m = \frac{x^5(x + 1)^5}{(x - 2)(x^2 + 2x - 2)^4}, \text{ with } m \text{ a divisor of } 24. \]

The curve \( C_1 \) (resp. \( C_2 \), \( C_3 \)) corresponds to \( m = 4 \) (resp. \( m = 12 \), \( m = 24 \)).

This equation for the curve comes from \( \ell(x) = \ell_1(x)\ell_2(x)\ell_3(x)\ell_5(x)\ell_6(x) \) and \( f(x) = (x^2 + x)^5 \). This curve \( C \) satisfies

\[ g(C) = (m - 1) + (m - d), \text{ with } d = \gcd(m, 4), \text{ and } \#C(F_{25}) \geq 10m + 2d + 4. \]

The 2d rational points appearing in the inequality for \( \#C(F_{25}) \) above are the ones with first coordinate satisfying \( x^2 + 2x - 2 = 0 \). We explain why they are rational points, but
we are not going to give similar details in other examples. Since \( d \) is a divisor of 4 we can write the equation of \( C \) as below

\[
\left( \frac{y^{m/d}(x^2 + 2x - 2)^{d/d}}{x^{d/d}(x + 1)^{d/d}} \right)^d = \frac{x^2 + x}{x - 2}.
\]

Let \( x \in \mathbb{F}_{25} \) be such that \( x^2 + 2x - 2 = 0 \), then \( x^2 + x = -(x - 2) \) and hence \( (x^2 + x)/(x - 2) = -1 \). The rationality of the points with \( x = x \) now follows since \( (-1) \) is a \( d \)th power in \( \mathbb{F}_{25}^\ast \); in fact, \( d \) divides 4 and hence \( 2d \) divides 24.

It is easy to verify directly that \( (10m + 2d + 4) \) is the exact number of rational points in the cases \( m = 12 \) and \( m = 24 \). Through a computer search one sees that the same holds also for \( m = 4 \).

Now we will give some examples of good curves over \( \mathbb{F}_q \) with \( q = r^m \) and \( n \geq 3 \).

**Example 4.8.** Let \( r \) be a power of a prime number \( p \) and let \( m \) be a divisor of \( (r^3 - 1) \). The curve \( C \) over \( \mathbb{F}_{r^3} \) defined by the affine equation

\[
y^m = \frac{(x^r - x)^{r^2 - 1}}{(x^r - x)^{r^2 - 1} + 1}
\]

has the following properties (with \( d := \gcd(m, r - 1) \)):

- \( 2g(C) = (r + 1) \cdot [(r - 2)(m - 1) + (m - d)] \)
- \( \#C(\mathbb{F}_{r^3}) = \begin{cases} m(r^3 - r) + d(r + 1) & \text{if } p(r - 1)/d \text{ is even} \\ m(r^3 - r) & \text{if } p(r - 1)/d \text{ is odd.} \end{cases} \)

Taking \( \ell(x) = (x^r - x)/(x^r - x) \), the equation above comes from

\[
f(x) = (x^r - x)^{r^2 - 1} = \ell(x) - [(x^r - x)^{r^2 - 1} + 1].
\]

**Example 4.9.** Let \( r \neq 2 \) be a power of a prime number \( p \) and let \( m \) be a divisor of \( (r^3 - 1) \). The curve \( C \) over \( \mathbb{F}_{r^3} \) defined by the Kummer equation

\[
y^m = -\frac{x^r(x^{r - 1} + 1)^r}{x - 1}
\]

has the following properties (with \( d := \gcd(m, r - 1) \)):

- \( 2g(C) = \begin{cases} (m - 1)(r - 3) + 2(m - d) & \text{if } p = 2 \\ (m - 1)(r - 1) + (m - d) & \text{if } p \neq 2. \end{cases} \)
- \( \#C(\mathbb{F}_{r^3}) = \begin{cases} mr^2 + d + 2 & \text{if } p \neq 2 \text{ and } (r - 1)/d \text{ even} \\ mr^2 + 2 & \text{if } p \neq 2 \text{ and } (r - 1)/d \text{ odd.} \end{cases} \)

Here one takes \( \ell(x) = x^r + x^r + x - 1 \) and \( f(x) = x^r + x^r \).
Remark 3. As an application of Example 4.9 we get a curve \( C \) over \( \mathbb{F}_{27} \) with genus 37 and with 236 rational points; this is a new entry for the table in [6].

Example 4.10. The equation below gives a curve \( C \) with \( g(C) = 25 \) and \( \#C(\mathbb{F}_{64}) = 335 \):

\[
y^9 = \frac{(x + 1)^{30}}{x^4(x^2 + x + 1)^3(x^4 + x^3 + x^2 + x + 1)^4}.
\]

This example provides a new entry in the table in [6]. In this construction we will take the polynomial \( \ell(x) \) as a product of 5 irreducible polynomials in \( \mathbb{F}_2[x] \), each one having degree equal to 6. Take then

\[
\ell_1(x) = x^6 + x + 1, \quad \ell_2(x) = x^6 + x^3 + 1, \quad \ell_3(x) = x^6 + x^5 + 1,
\]

\[
\ell_4(x) = x^6 + x^4 + x^2 + x + 1, \quad \ell_5(x) = x^6 + x^5 + x^4 + x^2 + 1.
\]

Taking \( \ell(x) = \prod_{i=1}^{5} \ell_i(x) \) and \( f(x) = (x + 1)^{30} \), we get the equation. The genus computation is routine and for the number of rational points one performs a computer search to show that \( K = 6 \) (see Formula (7) in Section 2).

The next remark shows that our method can be applied to prime fields.

Remark 4. (a) Let \( q = 5 \), \( \ell(x) = x^2 + x \) and \( f(x) = x^3 - x^2 + x - 1 \). We then consider the curve \( C \) over \( \mathbb{F}_5 \) given by \( y^4 = 2(x - 1)(x + 2) \). This curve \( C \) satisfies \( g(C) = 1 \) and \( \#C(\mathbb{F}_5) = 10 \); i.e., it attains Serre’s bound.

(b) Let \( q = 5 \), \( \ell(x) = x^5 - x \) and \( f(x) = (x^2 + x + 1)^3 \). We then have

\[
f(x) = (x + 3)\ell(x) + r(x), \quad \text{with} \quad r(x) = x^4 + 2x^3 + 2x^2 + x + 1.
\]

We then consider the curve \( C \) over \( \mathbb{F}_5 \) given by \( y^4 = (x^2 + x + 1)^3/r(x) \). This curve \( C \) satisfies \( g(C) = 7 \) and \( \#C(\mathbb{F}_5) = 22 \); this is the best known value.

5. Examples based on Section 3

In the preceding section we have given only two new entries for the table in [6] (see Remark 3 and Example 4.10) and six new entries \( p = 5 \) (see Example 4.3 with \( m = 8 \), \( m = 12 \) or \( m = 24 \), Examples 4.6 and 4.7). All the other examples were either maximal curves or curves attaining the existing record. That is not so bad since it represents a unified way to reach those records. In this section our performance will be better, especially in characteristic \( p = 3 \). On the other hand we will have to perform here several computer searches to determine the quantity \( K \) (see Formula (7) in Section 2). In the next four examples we construct curves over \( \mathbb{F}_{81} \) taking the polynomial \( \ell(x) \) as a product of two irreducible polynomials in \( \mathbb{F}_3[x] \) of degree 4. All these examples give new entries in [6]. We use the following polynomials:

\[
\ell_1(x) = x^4 + x^3 + x^2 + 1, \quad \ell_2(x) = x^4 + x^2 - x + 1, \quad \ell_3(x) = x^4 + x - 1,
\]

\[
\ell_4(x) = x^4 + x^2 + x + 1, \quad \ell_5(x) = x^4 - x^3 + x + 1, \quad \ell_6(x) = x^4 - x^3 - 1.
\]
Example 5.1. The curve $\mathcal{C}$ over $\mathbb{F}_{81}$ given by
\[ y^{10} = (x - 1)^4(x + 1)^3(x^3 - x^2 + x + 1) \]
has $g(\mathcal{C}) = 13$ and $\#\mathcal{C}(\mathbb{F}_{81}) = 243$. The former best value was 224.

To see that the equation comes from Section 3, one takes $\ell(x) = \ell_1(x)\ell_2(x)$ and $g(x) = (x - 1)^3$. We have $v(x)g(x) = h(x)\ell(x) + 1$, with $h(x) = x^2$ and $v(x) = (x - 1)(x + 1)^3(x^3 - x^2 + x + 1)$. This explains the equation for the curve. The genus computation is routine.

The nine roots of $h(x) \cdot \ell(x) = 0$ give rise to 90 rational points. Surprisingly enough a computer search gives $\mathcal{K} = 14$ (see the notation of Case $m < q - 1$ in Section 2). The point $x = \infty$ has 10 points above it and they are rational points (notice that the equation defining $\mathcal{C}$ has degree 10 on both sides). The unique point above $x = -1$ and the two points above $x = 1$ are also rational. This then gives
\[ \#\mathcal{C}(\mathbb{F}_{81}) = 9 \times 10 + 14 \times 10 + 10 + 1 + 2 = 243. \]

Example 5.2. The curve $\mathcal{C}$ given by the equation $y^{10} = x^5(x - 1)^4(x^2 + x - 1)$ has $g(\mathcal{C}) = 11$ and $\#\mathcal{C}(\mathbb{F}_{81}) = 220$.

Here one takes $\ell(x) = \ell_3(x)\ell_4(x)$ and $g(x) = x(x - 1)^4$. Then
\[ v(x)g(x) = h(x)\ell(x) + 1, \]
with $h(x) = (x + 1)^3$ and $v(x) = x^4(x^2 + x - 1)$. Besides the nine distinct roots of $h(x)\ell(x) = 0$, one has here $\mathcal{K} = 12$. Also one has 10 rational ramification points and then $\#\mathcal{C}(\mathbb{F}_{81}) = 9 \times 10 + 12 \times 10 + 10 = 220$.

Example 5.3. The curve $\mathcal{C}$ defined by $y^{10} = -x^3(x - 1)^6(x^3 + x^2 + x - 1)^2$ has genus $g(\mathcal{C}) = 14$ and $\#\mathcal{C}(\mathbb{F}_{81}) = 278$.

Here one takes $\ell(x) = \ell_1(x)\ell_5(x)$ and $g(x) = x^3(x - 1)^5$; then
\[ v(x)g(x) = h(x)\ell(x) + 1 \]
with $h(x) = -(x + 1)(x^2 + 1)(x^5 - 1)/(x - 1))$ and $v(x) = -(x - 1)(x^3 + x^2 + x - 1)^2$. There are 15 distinct roots of $h(x) \cdot \ell(x) = 0$ and one computes that $\mathcal{K} = 12$. Adding the 8 rational points that are ramified, we finish.

Example 5.4. The curve $\mathcal{C}$ over $\mathbb{F}_{81}$ given by $y^{20} = -x^4(x - 1)^9(x^2 - x - 1)$ satisfies $g(\mathcal{C}) = 25$ and $\#\mathcal{C}(\mathbb{F}_{81}) = 392$.

Here we take $\ell(x) = \ell_1(x)\ell_6(x)$ and $g(x) = x(x - 1)^7$. We omit details.

Continuing with $p = 3$, we will give now three examples of curves over $\mathbb{F}_{27}$ and they all give new entries for the table in [6]. Here the polynomial $\ell(x)$ will be a product
of irreducible polynomials of degree 3 in \( \mathbb{F}_3[x] \). We will use:

\[
\ell_1(x) = x^3 - x^2 - x - 1, \quad \ell_2(x) = x^3 - x^2 + x + 1, \\
\ell_3(x) = x^3 + x^2 + x - 1, \quad \ell_4(x) = x^3 + x^2 - x + 1, \\
\ell_5(x) = x^3 - x^2 + 1, \quad \ell_6(x) = x^3 - x + 1, \quad \ell_7(x) = x^3 - x - 1.
\]

We will just give in each of the three examples below the pair of polynomials \( \ell(x) \) and \( g(x) \in \mathbb{F}_{27}[x] \) used to get the equation of the curve.

**Example 5.5.** Taking \( \ell(x) = \ell_1(x)\ell_2(x) \) and \( g(x) = (x - 1)^6 \), we get the curve \( \mathcal{C} \) over \( \mathbb{F}_{27} \) given by the equation \( y^{13} = -(x - 1)^7(x^3 + x^2 - 1) \). We have that \( g(\mathcal{C}) = 18 \) and \( \#\mathcal{C}(\mathbb{F}_{27}) = 148 \).

**Example 5.6.** Taking \( \ell(x) = \ell_1(x)\ell_3(x)\ell_4(x)\ell_5(x) \) and \( g(x) = (x^2 + x - 1)^3 \), we get the curve \( \mathcal{C} \) defined by \( y^{13} = (x^2 + x - 1)^4(x^4 - x^3 - x^2 + x - 1) \). This curve has \( g(\mathcal{C}) = 30 \) and \( \#\mathcal{C}(\mathbb{F}_{27}) = 196 \).

**Example 5.7.** Taking \( \ell(x) = \ell_5(x)\ell_6(x)\ell_7(x) \) and \( g(x) = x^4(x + 1) \), we get the curve \( \mathcal{C} \) given by the affine equation \( y^{26} = x^7(x + 1)^3(x^3 + x^2 + x - 1) \). This curve has \( g(\mathcal{C}) = 44 \) and \( \#\mathcal{C}(\mathbb{F}_{27}) = 278 \).

Now we move to \( p = 2 \). We are going to give 6 maximal curves over \( \mathbb{F}_{64} \) having genus \( g = 3, 4, 7, 10, 12 \) and 28. As before we will just give the pair of polynomials \( \ell(x) \) and \( g(x) \) used to get the equation of the curve. We will need in this construction the following 10 irreducible polynomials in \( \mathbb{F}_2[x] \):

\[
\ell_1(x) = x^6 + x^5 + x^3 + x^2 + 1, \quad \ell_2(x) = x^6 + x^5 + x^2 + x + 1, \\
\ell_3(x) = x^6 + x^4 + x^3 + x + 1, \quad \ell_4(x) = x^3 + x^2 + 1, \quad \ell_5(x) = x^3 + x + 1, \\
\ell_6(x) = x^6 + x + 1, \quad \ell_7(x) = x^6 + x^5 + x^4 + x + 1, \quad \ell_8(x) = x^6 + x^3 + 1, \\
\ell_9(x) = x^6 + x^5 + x^4 + x^2 + 1, \quad \ell_{10}(x) = x^6 + x^4 + x^2 + x + 1.
\]

**Example 5.8.** Taking \( \ell(x) = \ell_1(x)\ell_2(x)\ell_3(x) \) and \( g(x) = x^9(x + 1)^{10} \), we obtain the equation \( y^9 = x^9(x + 1)^{15}(x^3 + x + 1)^3 \). Taking the third root of this equation, we get the curve \( \mathcal{C} \) given by \( y^3 = x^3(x + 1)^5(x^3 + x + 1) \). It is a maximal curve over \( \mathbb{F}_{64} \) with \( g(\mathcal{C}) = 3 \).

**Example 5.9.** Taking \( \ell(x) = \ell_1(x)\ell_4(x)\ell_5(x) \) and \( g(x) = (x^2 + x + 1)^9 \), we get the curve \( \mathcal{C} \) given by the affine equation \( y^9 = (x^2 + x + 1)^{14} \), which is a maximal curve over \( \mathbb{F}_{64} \) with \( g(\mathcal{C}) = 4 \).

**Example 5.10.** Taking \( \ell(x) = \ell_6(x)\ell_7(x) \) and \( g(x) = (x^3 + x)^6 \), we get the curve \( \mathcal{C} \) given by the affine equation \( y^9 = x^{10}(x + 1)^{15}(x^2 + x + 1) \), which is a maximal curve over \( \mathbb{F}_{64} \) with \( g(\mathcal{C}) = 7 \).
Example 5.11. Taking \( \ell(x) = \ell_3(x)\ell_6(x) \) and \( g(x) = (x^4 + x)^6 \), we get the curve \( \mathcal{C} \) defined by the affine equation \( y^3 = x^4(x + 1)^6(x^2 + x + 1)^6 \), which is a maximal curve over \( \mathbb{F}_{64} \) with \( g(\mathcal{C}) = 10 \).

Let \( r \) be a power of \( p = 2 \). The largest genus \( g_1 \) for a maximal curve over \( \mathbb{F}_r \) is \( g_1 = r(r - 1)/2 \) and the second largest genus \( g_2 \) is given by \( g_2 = r(r - 2)/4 \). When \( r = 8 \) one gets \( g_2 = 12 \) and \( g_1 = 28 \).

Example 5.12. Taking \( \ell(x) = \ell_1(x)\ell_4(x)\ell_9(x) \) and \( g(x) = (x + 1)^{10} \), we get the curve \( \mathcal{C}_2 \) given by the equation \( y^9 = x^3(x + 1)^{10}(x^3 + x + 1) \), which is a maximal curve over \( \mathbb{F}_{64} \) with \( g(\mathcal{C}_2) = g_2 = 12 \).

Example 5.13. Taking \( \ell(x) = \ell_7(x)\ell_9(x)\ell_{10}(x) \) and \( g(x) = (x + 1)^{10} \), we get the curve \( \mathcal{C}_1 \) given by the equation \( y^9 = x(x + 1)^{18}(x^2 + x + 1)(x^6 + x^4 + x^3 + x + 1) \), which is a maximal curve over \( \mathbb{F}_{64} \) with \( g(\mathcal{C}_1) = g_1 = 28 \).

6. Fibre products and examples

Let \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \) be two curves over \( \mathbb{F}_q \) whose equations are obtained through our method; i.e., for \( i = 1, 2 \) we have polynomials \( \ell_i(x), f_i(x) \in \mathbb{F}_q[x] \) and the curve \( \mathcal{C}_i \) is then given by an equation

\[
y^m_i = \frac{f_i(x)}{r_i(x)}, \quad \text{with } m_i \text{ a divisor of } (q - 1),
\]

where \( r_i(x) \) is the remainder in the division of \( f_i(x) \) by \( \ell_i(x) \). We will consider in this section the fibre product \( \mathcal{C} \) of the curve \( \mathcal{C}_1 \) with the curve \( \mathcal{C}_2 \) (in the language of function fields we are then considering the compositum of the function fields corresponding to \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \)). In order to get a nice genus formula for the product curve \( \mathcal{C} \), we will assume that all ramification points on \( \mathcal{C}_i \) \( (i = 1, 2) \) are totally ramified; i.e. each multiplicity of a zero or a pole of \( f_i(x)/r_i(x) \) is relatively prime to \( m_i \) or a multiple of \( m_i \). In the latter case of multiplicities \( \equiv 0 \mod m_i \), the points are unramified. We denote the set of totally ramified points on \( \mathcal{C}_i \) by \( T_i \); i.e.,

\[
T_i = \{ z \in \overline{\mathbb{F}_q} \cup \{ \infty \} | z \text{ is a zero or a pole for } f_i(x)/r_i(x) \text{ with multiplicity } \not\equiv 0 \mod m_i \}.
\]

Also we set \( t_i = \# T_i \) and \( g_i = g(\mathcal{C}_i) \), for \( i = 1, 2 \). Because of the assumption that the points are totally ramified we have

\[
2g_i = (m_i - 1)(t_i - 2). \tag{10}
\]

We will assume that \( \mathcal{C} \) is a degree \( m_1 \cdot m_2 \) cover of the projective \( x \)-line (e.g., this is the case if \( T_1 \neq T_2 \)). Applying Abhyankar’s lemma (see [11, Proposition III.8.9]) and Hurwitz’s genus formula, we get the formula for the genus \( g(\mathcal{C}) \) of the product curve (where \( t = \#(T_1 \cap T_2) \) and \( \delta = gcd(m_1, m_2) \)):

\[
g(\mathcal{C}) = (m_1 - 1)(m_2 - 1) + m_1 g_2 + m_2 g_1 - \frac{t}{2}(m_1 m_2 - m_1 - m_2 + \delta). \tag{11}
\]
Remark 5. In the above situation Castelnuovo’s inequality says that (see [11, Theorem III.10.3])
\[ g(C) \leq (m_1 - 1)(m_2 - 1) + m_1 g_2 + m_2 g_1. \]
Formula (11) above then gives the correction term in our particular situation.

Let \( \ell(x) \in \mathbb{F}_q[x] \) be the greatest common divisor of \( \ell_1(x) \) and \( \ell_2(x) \), and let
\[ \lambda = \# \{ \beta \in \mathbb{F}_q \mid \ell(\beta) = 0 \text{ and } f_1(\beta)f_2(\beta) \neq 0 \}. \]
We then have the following inequality
\[ \#C(\mathbb{F}_q) \geq \lambda m_1 m_2. \]
In order to guarantee that the curve \( C \) has many rational points, one usually takes the polynomials \( \ell_1(x) \) and \( \ell_2(x) \) with many common roots.

In the next five examples we will construct good curves \( C \) that are obtained as fibre products as above. We start with a new record:

Example 6.1. Let \( C \) be the curve over \( \mathbb{F}_{16} \) which is the fibre product of the curves \( C_1 \) and \( C_2 \) given by
\[ y_1^5 = (x^4 + x)^3 \quad \text{and} \quad y_2^3 = \frac{(x^2 + x + 1)(x^3 + x + 1)^2}{x(x + 1)(x^3 + x^2 + 1)^3}. \]
We have \( g(C) = 34 \) and \( \#C(\mathbb{F}_{16}) = 183 \); the former best value was 161.
In this case \( \ell_1(x) = \ell_2(x) = (x^{15} - 1)/(x^3 - 1) \); i.e., the roots of \( \ell(x) \) are the elements of \( \mathbb{F}_{16} \) outside \( \mathbb{F}_4 \). The curves \( C_1 \) and \( C_2 \) are obtained by taking
\[ f_1(x) = (x^4 + x)^3 \quad \text{and} \quad f_2(x) = (x^2 + x + 1)(x^3 + x + 1)^2. \]
One can check easily that \( \lambda = 12 = \deg \ell(x) \) (see Formula (12)), and hence
\[ \#C(\mathbb{F}_{16}) \geq 12 \cdot 5 \cdot 3 = 180. \]
We have three more rational points on \( C \) corresponding to \( x = 0, x = 1 \) and \( x = \infty \).

The determination of the genus \( g(C) \) is a direct application of Formulas (10) and (11), since we have here \( t_1 = 5, t_2 = 6 \) and \( t = 3 \).

We now construct a curve \( C \) over \( \mathbb{F}_8 \) with \( g(C) = 57 \) and \( \#C(\mathbb{F}_8) = 168 \). One cannot find genus 57 curves on the tables, but if one compares with the table in [6] one sees that 168 is certainly a very good entry for such a genus.

Example 6.2. Let \( C \) be the curve over \( \mathbb{F}_8 \) which is the fibre product of the curves \( C_1 \) and \( C_2 \) given by
\[ y_1^7 = x(x + 1)^2 \quad \text{and} \quad y_2^7 = (x^2 + x + 1)^2/(x + 1). \]
This curve \( C \) satisfies \( g(C) = 57 \) and \( \#C(\mathbb{F}_8) = 168 \).

Here one takes \( \ell_1(x) = \ell_2(x) = x^3 + x + 1, f_1(x) = x^3 + x^2 \) and \( f_2(x) = (x^2 + x + 1)^2 \).
It is easy to see that \( \lambda = 3 \) and then from Formula (13) we have
\[ \#C(\mathbb{F}_8) \geq 3 \cdot 7 \cdot 7 = 147. \]
We think of \( C \) as a degree 7 cover of \( C_1 \) and it is easy to see that the unique point on \( C_1 \) with \( x = 0 \) has 7 rational preimages in the curve \( C \). The same holds for the unique point on \( C_1 \) with \( x = 1 \) or with \( x = \infty \). Also the points with \( x^3 + x^2 + 1 = 0 \) are not rational and then \( \#C(F_8) = 147 + 3 \times 7 = 168 \).

We give the details that the 7 points on \( C \) with \( x = 1 \) are rational points. In fact we have that 
\[
 u := \frac{x + 1}{y^2} \text{ is a local parameter at the unique point on } \ C \text{ with } x = 1.
\]

We write the equation for the cover \( C \to C_1 \) in the form
\[
 (uy^2)^7 = (x^2 + x + 1)^2/x^3.
\]

The value of the right hand side above is one at \( x = 1 \), and this shows the rationality of the points. The genus follows from Formulas (10) and (11).

**Example 6.3.** Let \( C \) be the curve over \( F_{64} \) which is the fibre product of the curves \( C_1 \) and \( C_2 \) given by
\[
 y_1^3 = \frac{(x + 1)^4}{(x^3 + x + 1)} \quad \text{and} \quad y_2^3 = (x^8 + x)^7.
\]

This curve has \( g(C) = 19 \) and \( \#C(F_{64}) = 297 \); this gives a new entry in [6].

The equation for the curve \( C_1 \) is just another way of representing the maximal curve in Example 5.8 and the curve \( C_2 \) is the curve in Example 4.1 with \( r = 8 \) and \( m = 3 \). Here one takes
\[
 \ell_1(x) = (x^6 + x^4 + x^3 + x + 1)(x^6 + x^5 + x^2 + x + 1)
\]
\[
 \times (x^6 + x^5 + x^3 + x^2 + 1)(x^6 + x^5 + x^4 + x + 1), \quad \ell_2(x) = (x^{64} - x)/(x^8 - x), \quad f_1(x) = (x + 1)^{30} \quad \text{and} \quad f_2(x) = (x^8 + x)^7.
\]

The genus is again straightforward but the determination of the number of rational points requires a computer search. We omit the details.

**Example 6.4.** Let \( C \) be the fibre product of \( C_1 \) and \( C_2 \) over \( F_{27} \), where
\[
 y_1^2 = \frac{x^8(x^2 + 1)^9}{x^8 + 1} \quad \text{and} \quad y_2^2 = \frac{x^8(x^2 - 1)^8}{(x^4 + 1)(x^2 + 1)}.
\]

This curve \( C \) has \( g(C) = 11 \) and \( \#C(F_{27}) = 96 \); this is the best value known.

Here we take \( \ell_1(x) = x^{26} - 1, \ell_2(x) = (x^{26} - 1)/(x^2 - 1), \ f_1(x) = (x^3 + x)^9 \) and \( f_2(x) = (x^3 - x^2)^8 \). We then get
\[
 gcd(\ell_1(x), \ell_2(x)) = \ell_2(x) \quad \text{and hence} \quad \#C(F_{27}) \geq 24 \times 2 \times 2 = 96.
\]

The determination of the genus is routine and we leave to the reader the checking that there are no further rational points.
Example 6.5. Here we give two new entries over $\mathbb{F}_{25}$. They are:

- A curve $\tilde{C}_1$ with $g(\tilde{C}_1) = 19$ and $\#\tilde{C}_1(\mathbb{F}_{25}) = 132$.
- A curve $\tilde{C}_2$ with $g(\tilde{C}_2) = 43$ and $\#\tilde{C}_2(\mathbb{F}_{25}) = 252$.

The curve $\tilde{C}_1$ (resp. $\tilde{C}_2$) is the fibre product of the curve in Example 4.1 with $r = 5$ and $m = 6$ (resp. $m = 24$) with the curve given by the following equation:

$$y_2^2 = -\frac{x^4(x^4 - a)^5}{a^5x^4 - 1}, \quad \text{with } a \in \mathbb{F}_{25} \quad \text{and} \quad a^6 = -1.$$  

We finish this paper with the following example. The goal here is just to illustrate that fibre products of Kummer covers with Artin-Schreier covers should also be considered when trying to get good curves over finite fields.

Example 6.6. Consider the curve $\mathcal{C}$ over $\mathbb{F}_8$ which is the fibre product of

$$y_1^3 = \frac{x^3(x + 1)^3}{x^2 + x + 1} \quad \text{and} \quad y_2^2 + y_2 = \frac{\ell(x)}{x^2 + x + 1},$$

where $\ell(x) = (x^8 - x)/(x^2 - x)$. We have $g(\mathcal{C}) = 25$ and $\#\mathcal{C}(\mathbb{F}_8) = 86$.

This is the best value known (see [6]). Notice that the curve $\mathcal{C}_1$ is obtained by considering the division of $f(x) = x^3(x + 1)^3$ by $\ell(x)$. We omit the details.

References