On constructions of curves with many points over finite fields

1 Introduction

Let p be a prime number, $\mathbb{F}_q$ be the finite field with $q = p^n$ elements and let $\bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Given a polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ which is irreducible over $\bar{\mathbb{F}}_q$, the set

$$\mathcal{C}_f = \{(\alpha, \beta) \in \bar{\mathbb{F}}_q \times \bar{\mathbb{F}}_q \text{ such that } f(\alpha, \beta) = 0\}$$

is an affine plane algebraic curve (over the finite field $\mathbb{F}_q$) and the points $P = (\alpha, \beta) \in \mathcal{C}_f$ such that $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ are called rational points over $\mathbb{F}_q$.

Most of the curves that we are going to deal with here is represented as above (i.e, thru a polynomial in two variables over a finite field), but we will always be concerned with the projective non singular models of the curves.

For many years the question on how many rational points a curve of genus g over a finite field with q elements can have, has attracted the attention of mathematicians. In 1940 A. Weil proved the Riemann hypothesis for curves over finite fields. As an immediate corollary he obtained an upper bound for the number of rational points on a geometricaly irreducible nonsingular curve $\mathcal{C}$ of genus g over a finite field of cardinality q, namely

$$\#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q},$$

where $\mathcal{C}(\mathbb{F}_q)$ denotes the set of rational points of the curve $\mathcal{C}$.

This bound was proved for elliptic curves (i.e, $g=1$) by H. Hasse in 1933.However, the question of finding the maximun number $N_q(g)$ of rational points on an irreducible nonsingular curve of genus g over a finite field $\mathbb{F}_q$ did not attract the attention of the mathematicians until Goppa introduced geometric codes in 1980. (See [7]).

In 1981 Ihara shows in [8] that

$$N_q(g) \leq q+1+[(\sqrt{(8q+1)g^2+4(q^2-q)g}-g)/2],$$

where $[x]$ is the integer part of $x \in \mathbb{R}$. For $g > \frac{(q-\sqrt{q})}{2}$ the bound above is better than Weil's bound. In [11] Serre shows that Weil's bound may be sharpened to

$$N_q(g) \leq q+1+g[2\sqrt{q}].$$

In the same paper Serre introduced the idea of 'formule explicite' in analogy with number theory to obtain better upper bounds for $N_q(g)$. Oesterlé used methods of linear programming to implement this idea (see [12]).

The aim of this work is the construction of curves over finite fields with many rational points and the method is motivated by those used in [4] by van der Geer and van der Vlugt, and by Garcia and Quoos in [1]. We will describe them briefly.

In [4], given a polynomial $R(x) \in \mathbb{F}_q[x]$ with many roots in $\mathbb{F}_q$, they decompose $R(x)$ as

$$R(x) = R_1(x) + R_2(x), \text{ with } R_i(x) \in \mathbb{F}_q[x],$$

where $R_1(x)R_2(x)$ has many multiple roots. Then, they consider the curve $\mathcal{C}$ over $\mathbb{F}_q$ given by the Kummer equation

$$y^{q-1} = -\frac{R_1(x)}{R_2(x)}\,. \qquad (i)$$

In this case, if L (Resp L_i $i = 1, 2$) denotes the zero set of $R(x)$ (Resp $R_i(x)$ $i = 1, 2$) then $-\frac{R_1(\alpha)}{R_2(\alpha)} = 1$ for all $\alpha \in L - (L_1 \cap L_2)$. Therefore the curve defined by Equation (i) has at least $\lambda(q-1)$ rational points, where $\lambda = \#(L - (L_1 \cap L_2))$.

The reason for taking the product $R_1(x)R_2(x)$ with many multiples roots is to guarantee a low genus for the curve.

In [1], to each polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \geq q$, they associate a polynomial $\mathcal{R}(g(x))$ where the operator $\mathcal{R}$ is defined by the action on monomials as follows:

•$\mathcal{R}(x^j) = x^j$ if $j \leq q-1$.

•$\mathcal{R}(x^{q+j}) = \mathcal{R}(x^{1+j})$ for $j \geq 0$.

In this case the polynomial $f(x) = g(x) - \mathcal{R}(g(x))$ has all elements in $\mathbb{F}_q$ as roots, and then they consider the curve $\mathcal{C}$ over $\mathbb{F}_q$ defined by

$$y^r = \frac{g(x)}{\mathcal{R}(g(x))}\,, \text{ with } r \text{ a divisor of } q-1. \qquad (ii)$$

The number of $\mathbb{F}_q$-rational points on this curve satisfies the inequality $\#\mathcal{C}(\mathbb{F}_q) \geq r(q-c)$, where $c = \#\{\alpha \in \mathbb{F}_q$ such that $g(\alpha) = 0\}$.

Again here it is desirable to have $g(x)\mathcal{R}(g(x))$ with many multiples roots to get a curve of low genus.

Our method can be described as follows:

To each two polynomials $f(x)$ and $\ell(x)$ in $\mathbb{F}_q[x]$ such that $\deg(f(x)) \geq \deg(\ell(x))$, we associate a polynomial $\mathcal{R}_\ell(f(x))$ such that (Euclidean Algorithm)

$$f(x) = \ell(x)h(x) + \mathcal{R}_\ell(f(x)),$$

for some polynomial $h(x)$ and with $\deg(\mathcal{R}_\ell(f(x))) < \deg(\ell(x))$.

This means that the polynomial $\mathcal{R}_\ell(f(x))$ is the remainder of the Euclidean division of the polynomial $f(x)$ by $\ell(x)$. As in the above cases we will consider curves $\mathcal{C}$ over $\mathbb{F}_q$ defined by the affine equation

$$y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))}, \text{with } r \text{ a divisor of } q-1. \qquad (iii)$$

Observe that the number of $\mathbb{F}_q$-rational points on this curve satisfies the inequality $\#\mathcal{C}(\mathbb{F}_q) \geq \lambda r$, where $\lambda = \#\{\alpha \in \mathbb{F}_q \text{ such that } \ell(\alpha) = 0 \text{ and } f(\alpha) \neq 0\}$. Therefore we have to construct appropriate polynomials $f(x)$ and $\ell(x)$ to guarantee the existence of many rational points.

Here one also tries to get a highly inseparable product $f(x)\mathcal{R}_\ell(f(x))$ to have a low genus curve.

Now, if one drops the assumption on the degree of the polynomial $\mathcal{R}_\ell(f(x))$ made above, then one sees that our method gives a generalization of the method in [4]. In fact if the polynomial $\ell(x)$ is written as

$$\ell(x) = f(x) + g(x), \qquad \text{with } f(x) \text{ and } g(x) \text{ polynomials},$$

then $f(x) = \ell(x) - g(x)$; i.e., one can choose $\mathcal{R}_\ell(f(x)) = -g(x)$. However we also observe that the examples of 'good curves' given in [4] satisfy

$$\deg(R_2(x)) < \deg(R(x)) = \deg(R_1(x)),$$

i.e., $R_1(x) = R(x) - R_2(x)$ and therefore $-R_2(x) = \mathcal{R}_R(R_1(x))$.

On the other hand, if one takes $\ell(x) = x^q - x$, then $\mathcal{R}_\ell(f(x)) = \mathcal{R}(f(x))$ and therefore the method used in [1] is a particular case of our method (i.e, it is the particular case of taking $\ell(x) = x^q - x$).

In this work the expression 'good curve $\mathcal{C}$ over $\mathbb{F}_q$' means that the number of rational points $\#\mathcal{C}(\mathbb{F}_q)$ satisfies $a = a_q(g) \leq \#\mathcal{C}(\mathbb{F}_q) \leq b_q(g) = b$, where as in [5] the meaning of the interval $[a_q(g), b_q(g)]$ is: we know that there exists a curve over $\mathbb{F}_q$ with genus g and with at least $a = b/\sqrt{2}$ rational points and the upper bound b is equal to the best upper bound known by Hasse-Weil, Serre, Ihara, Oesterlé or other means.

We have obtained here two new records and around ten new entries for the tables in [5] (some of them are really good new entries) and also several curves meeting or attaining the existing records on the tables. Two things are worth of mentioning:

i) Lots of the records on the tables that we match here were obtained by totally different methods, so here we have an unified way to get them.

ii) Our constructions always involve the choice of an integer r which divides the cardinality of the multiplicative group of the finite field in question, and we have always chosen r small enough so that the genus g is less than 50. This is done because of the existing tables (see [5]), but sometimes the choice of a bigger value for r would have led to even better curves but with genera well above 50. Unfortunately there are not tables involving such a bigger genera.

In section 2 we review the formulas for the genus in Kummer and Artin-Schreier extensions.

In section 3 we give the details of our method for the construction of good curves over finite fields.

In section 4 we construct polynomials $\ell(x)$ as a sum of certain polynomials $s_{m,j}(x) = s_j(x, x^q, \ldots, x^{q^{m-1}})$, where $s_j(x_1, \ldots, x_m)$ is the j-th elementary symmetric polynomial in m variables over $\mathbb{F}_q$ (see [2] for properties of these polynomials), and we give a characterization of the polynomial remainder $\mathcal{R}_\ell(s_{m,m}(x+1))$ (see Lemma 4.3). This is for constructions over $\mathbb{F}_{q^m}$ (see Theorem 4.1), and we illustrate it with examples in the case $m = 3$.

In section 5 we construct polynomials $\ell(x)$ as an appropriate products of irreducible polynomials. We give a characterization (see Lemma 5.2.1) for the remainder polynomial $\mathcal{R}_\ell(f(x))$ in the particular case when $\ell(x) = x^{q^2} - x$ and $f(x)$ is a suitable power of $(x^q - x)$. We also take other polynomials $f(x)$ and $\ell(x)$, and obtain several good examples of curves.

Section 7 is dedicated to construct examples of 'good curves' by considering the particular case when the polynomials $f(x)$ and $\ell(x)$ are chosen so that the remainder polynomial satisfies $\mathcal{R}_\ell(f(x)) = 1$.

In section 8 we construct curves with many rational points which are fiber products over the x-line of two curves $\mathcal{C}_1$ and $\mathcal{C}_2$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are given by equations of the type (iii). We give a result calculating the genus of these curves in the case when only total ramification occurs. (See Theorem 8.2).

Now we give below three tables (in characteristics $p = 2$, $p = 3$ and $p = 5$) summarizing the constructions of good curves over finite fields given in this work.

In these tables the numbers $\#\mathcal{C}(\mathbb{F}_q)$ below are the cardinalities of the sets of rational points on the curves constructed here using our method.

Table p=2.

q	g	$\#\mathcal{C}(\mathbb{F}_q)$	*old entry*	*Example*
8	9	45	45-46	4.1
8	15	57	57-68	6.2
8	25	86	86-97	6.1
8	57	168	—	8.4
16	2	31	33	5.2.5
16	2	33	33	5.2.4
16	4	45	45-46	5.2.1
16	6	65	65	5.2.5
16	12	83	83	5.2.4
16	19	117	129-134	8.2
16	20	127	127-140	5.2.5
16	34	183	161-213	8.2

q	g	$N(\mathbb{F}_q)$	*old entry*	*Example*
32	15	158	158-196	6.2
32	45	313	313-428	6.4
64	1	81	81	7.5
64	3	113	113	7.6
64	3	113	113	6.6
64	4	129	129	7.7
64	7	177	177	7.8
64	10	225	225	7.9
64	12	257	257	7.10
64	12	257	257	6.6
64	19	297	—	8.7
64	25	335	—	6.5
64	28	513	513	7.11
64	40	489	489-650	7.12

Table p=3.

q	g	$N(\mathbb{F}_q)$	*old entry*	*Example*
27	1	38	38	4.2
27	2	48	48	5.3.1
27	11	96	96-136	8.6
27	18	148	—	7.2
27	30	196	—	7.3
27	37	236	—	5.3.3
27	44	293	—	7.4
27	48	316	325-402	5.3.1
27	49	314	314-409	4.2
81	11	218	—	7.13
81	13	243	224-315	7.14
81	14	278	—	7.15
81	25	392	—	7.16
81	153	1616	—	Prop 5.2.1
81	313	3216	—	Prop 5.2.1

Table p=5.

q	g	$N(\mathbb{F}_q)$	*old entry*	*Example*
5	1	10	10	5.1.2
5	3	16	16	5.1.1
5	7	22	22-27	5.1.3
25	3	52	52-56	5.2.3
25	5	56	—	Prop 5.2.1
25	7	76	—	5.2.2
25	7	84	—	7.1
25	13	104	—	Prop 5.2.1
25	19	132	—	5.2.3
25	21	152	—	Prop 5.2.1
25	43	252	—	Prop 5.2.3
25	43	252	—	8.3
25	45	296	—	Prop 5.2.1
125	2	151	—	4.3
125	7	221	—	4.3
125	9	252	—	5.3.2

We end up this introduction by saying that although the curves constructed here are obtained thru our method, the exact amount of rational points on them requires quite often a computer search. We acknowledge that we have used Mathematica 4.0 to perform some of the computations needed in this work.

2 Preliminaries

In this section we reproduce some results that we will use along this work, to calculate the genus of a curve $\mathcal{C}'$ that covers another curve $\mathcal{C}$ (i.e., there exist a surjective map $\mathcal{C}' \to \mathcal{C}$). Typically the curve $\mathcal{C}$ will be the projective line and the cover will be cyclic. We present those results in the language of function fields (i.e., F' (resp F) is the field of rational functions of $\mathcal{C}'$ (resp of $\mathcal{C}$)), for the proof of these results we give as reference [13] Chapter III.

Definition 2.1 *Let F'/F be a finite separable extension of function fields. Then the different of F'/F, denoted by $\mathcal{D}(F'/F)$, is the divisor of F' given by*

$$\mathcal{D}(F'/F) = \sum_{P\in\mathbb{P}(F)} \sum_{P'|P} d(P'/P)P'.$$

where $d(P'/P)$ is the different exponent of the place P' lying over $P \in \mathbb{P}(F)$. We denote by $\nu_{P'}$ the corresponding valuation. The degree of $\mathcal{D}(F'/F)$ will be denoted by $deg(\mathcal{D}(F'/F))$.

Proposition 2.1 (Hurwitz Genus Formula) *Let F/K be an algebraic function field of genus g and F'/F be a finite separable extension. Let K' denote the constant field of F' and let g' be the genus of F'/K'. Then we have*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + deg((\mathcal{D}(F'/F)).$$

The determination of the different exponent in the next two propositions is due to H. Hasse (see [6]).

Proposition 2.2 (Kummer Extensions) *Let F/K be an algebraic function field and suppose that the constant field K contains a primitive r-th root of unity (with $r > 1$). Suppose that $u \in F$ is an element satisfying*

$$u \neq w^d \quad \textit{for all } w \in F \qquad \textit{and all divisors } d > 1, \ \textit{of } r.$$

Let

$$F' = F(y) \qquad \textit{with} \quad y^r = u.$$

An extension such as F' is said to be a Kummer extension of F. We have

(a) *The polynomial $\Phi(T) = T^r - u$ is the minimal polynomial of y over F (in particular, it is irreducible over F). The extension F'/F is Galois of degree r; its Galois group is cyclic, and all automorphism of F'/F are given by $\sigma(y) = \zeta y$, where $\zeta \in K$ is a r-th root of unity.*

(b) *Let $P \in \mathbb{P}(F)$ and let $P' \in \mathbb{P}(F')$ be an extension of P. Then*

$$e(P'|P) = \frac{r}{m_P} \qquad \textit{and} \qquad d(P'|P) = \frac{r}{m_P} - 1,$$

where

$$m_P := gcd(r, \nu_P(u)) > 0$$

is the greatest common divisor of r and $\nu_P(u)$.

(c) *If K' denotes the constant field of F' and g (resp g') is the genus of F/K (resp F'/K'), then*

$$g' = 1 + \frac{r}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}(F)} \left(1 - \frac{m_P}{r} \right) degP \right).$$

Corollary 2.1 *Let F/K be a function field and let $F' = F(y)$ with $y^r = u \in F$, where $r \not\equiv 0$ mod char K and suppose that the constant field K contains a primitive r-th root of unity. Assume that there exists a place $Q \in \mathbb{P}(F)$*

such that $gcd(\nu_Q(u), r) = 1$. *Then* K *is the constant field of* F', *the extension* F'/F *is cyclic of degree* r *and*

$$g' = 1 + r(g-1) + \frac{1}{2} \sum_{P \in \mathbb{P}(F)} (r - m_P) degP.$$

Proposition 2.3 (Artin-Schreirer extensions) *Let* F/K *be an algebraic function field of characteristic* $p > 0$. *Suppose that* $u \in F$ *is an element which satisfies the following condition:*

$$u \neq w^p - w \qquad \text{for all} \qquad w \in F.$$

Let

$$F' = F(y) \quad \text{with} \quad y^p - y = u.$$

Such an extension is called an Artin-Schreirer extension of F. *For* $P \in \mathbb{P}(F)$ *we define the integer* m_P *by*

$$m_P := \begin{cases} m & \text{if there exists an element } z \in F \text{ satisfying} \\ & \nu_P(u - (z^p - z)) = -m < 0 \text{ and } m \not\equiv 0 \bmod p, \\ -1 & \text{if } \nu_P(u - (z^p - z)) \geq 0 \text{ for some } z \in F. \end{cases}$$

We then have:

(a) F'/F *is a cyclic Galois extension of degree* p. *The automorphisms of* F'/F *are given by* $\sigma(y) = y + \zeta$, *with* $\zeta \in \mathbb{F}_p$.

(b) P *is unramified in* F'/F *if and only if* $m_P = -1$.

(c) P *is totally ramified in* F'/F *if and only if* $m_P > 0$. *Denote by* P' *the unique place of* F' *lying over* P. *Then the different exponent* $d(P'|P)$ *is given by*

$$d(P'|P) = (p-1)(m_P + 1).$$

(d) If at least one place $Q \in \mathbb{P}(F)$ *satisfies* $m_Q > 0$, *then* K *is algebraically closed in* F', *and*

$$g' = p.g + \frac{p-1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1).degP\right),$$

where g' *(resp.* g*) is the genus of* F'/K *(resp.* F/K*).*

3 Certain Kummer coverings

Let p be a prime number, $\mathbb{F}_q$ be a finite field with $q = p^n$ elements and let $\bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. The purpose of this section is to introduce polynomials $\mathcal{R}_\ell(f(x))$ associated to the polynomials $\ell(x)$ and $f(x) \in \mathbb{F}_q[x]$. Then we will construct curves $\mathcal{C}$ over $\mathbb{F}_q$ with many rational points which are Kummer covers of the projective line $\mathbf{P}^1(\bar{\mathbb{F}}_q)$ of the type

$$y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))} \tag{1}$$

where r is a divisor of $q-1$.

Notation: Given $f(x)$ and $\ell(x)$ polynomials, we will denote by $\mathcal{R}_\ell(f(x))$ any polynomial $t(x)$ such that:

$$f(x) = \ell(x)h(x) + t(x), \qquad \text{for some polynomial } h(x). \tag{$*$}$$

This way, we have (essentially)

$$\ell(x) = 0 \qquad \Rightarrow \frac{f(x)}{t(x)} = 1.$$

This property leads us to hope that some curves of the type in the Equation (1) have many rational points over $\mathbb{F}_q$ when the polynomial $\ell(x)$ has many roots in $\mathbb{F}_q$

Although the expression given for $f(x)$ and the curve construction in (1) do not require that $t(x)$ is the remainder of the Euclidean division of $f(x)$ by $\ell(x)$, we will suppose in this work that this is the case, i.e., we will suppose that

$$f(x) = \ell(x)h(x) + \mathcal{R}_\ell(f(x)), \text{ with } \deg\mathcal{R}_\ell(f(x)) < \deg\ell(x). \tag{$*$}$$

The really important thing here, is that the number of distinct roots in the product $f(x)\mathcal{R}_\ell(f(x))$ should be small in order that the curve given by (1) has low genus (see Proposition 3.1). So in general the inseparability of this product is desirable.

Observe that in general it is difficult to give a criterion that assures the inseparability of the polynomial $\mathcal{R}_\ell(f(x))$, this will be possible only in some particular cases. For example, when $\ell(x) = x^q - x$, which is the particular case treated in [1], we have that it is enough to know the behavior of $\mathcal{R}_\ell(\cdot)$ in each monomial of $f(x)$ to determine $\mathcal{R}_\ell(f(x))$. For this, observe that

$$\text{if } m \equiv n \bmod (q-1) \text{ and } 1 \leqslant n \leqslant q-1, \text{ then } \mathcal{R}_\ell(x^m) = x^n.$$

Then we have that

i) $\mathcal{R}_\ell(x^j) = x^j, \quad \forall j \leqslant q-1.$

ii) $\mathcal{R}_\ell(x^{q+j}) = \mathcal{R}_\ell(x^{1+j}), \quad \forall j \geqslant 0.$

Remark 3.1 The following properties of the polynomial $\mathcal{R}_\ell(f(x))$ are easy consequences of the definition:

a) If $\ell_1(x) \mid \ell_2(x)$ and $\deg(\mathcal{R}_{\ell_2}(f(x))) < \deg(\ell_1(x))$, then $\mathcal{R}_{\ell_1}(f(x)) = \mathcal{R}_{\ell_2}(f(x))$.

b) Let $\mathcal{V}_\ell = \{\alpha \in \bar{\mathbb{F}}_q; \ell(\alpha) = 0\}$, and $f(x) \in \mathbb{F}_q[x]$. The polynomial $\mathcal{R}_\ell(f(x))$ satisfies:

   i) $\forall \alpha \in \mathcal{V}_\ell, \quad f(\alpha) = 0$ if and only if $\mathcal{R}_\ell(f(x))(\alpha) = 0$.

   ii) $\forall \alpha \in \mathcal{V}_\ell$ such that $f(\alpha) \neq 0, \quad \dfrac{f(x)}{\mathcal{R}_\ell(f(x))}(\alpha) = 1.$

   iii) If we write $f(x)^r = \ell(x)h(x) + \mathcal{R}_\ell(f(x)^r)$, then $\forall \alpha \in \mathcal{V}_\ell \cap \mathbb{F}_q$ such that $f(\alpha) \neq 0$, we have $f(\alpha)^r = \mathcal{R}_\ell(f(x)^r)(\alpha)$. Therefore, $\mathcal{R}_\ell(f(x)^r)(\alpha)$ and $\dfrac{\mathcal{R}_\ell(f(x)^{r+k})}{\mathcal{R}_\ell(f(x)^k)}(\alpha)$ are r-th powers in $\mathbb{F}_q$.

Proposition 3.1 *The curve $\mathcal{C}$ over the finite field $\mathbb{F}_q$ given by the Kummer equation*

$$y^r = u(x) := \frac{f(x)}{\mathcal{R}_\ell(f(x))},$$

where r divides $q-1$ and the rational function $u(x)$ is not the $d-th$ power of an element $v(x) \in \bar{\mathbb{F}}_q(x)$ for any divisor d of r with $d > 1$, has the following properties:

i) If $(u) = \sum_{i=1}^{n} d_i P_i$ is the divisor of u with distinct $P_i \in \mathbf{P}^1(\bar{\mathbb{F}}_q)$ and there exists i such that $gcd(r, \mid d_i \mid) = 1$, then the genus $g(\mathcal{C})$ of $\mathcal{C}$ is given by

$$2g(\mathcal{C}) - 2 = r(n-2) - \sum_{i=1}^{n} gcd(r, \mid d_i \mid).$$

ii) The set of $\mathbb{F}_q$-rational points satisfies $\#\mathcal{C}(\mathbb{F}_q) \geq r\lambda$ where

$$\lambda = \#\{\alpha \in \mathcal{V}_\ell \cap \mathbb{F}_q ; f(\alpha) \neq 0\}$$

Proof: The formula for the genus follows from Propositions 2.1 and 2.2.

By Remark 2.2, for each point $\alpha \in \mathcal{V}_\ell \cap \mathbb{F}_q$ with $f(\alpha) \neq 0$, we have that $u(\alpha) = 1$, and hence, there lie r points on $\mathcal{C}$ with α as first coordinate and these points are rational . Therefore the set of $\mathbb{F}_q$-rational points satisfies $\#\mathcal{C}(\mathbb{F}_q) \geq r\lambda$ where $\lambda = \#\{\alpha \in \mathcal{V}_\ell \cap \mathbb{F}_q ; f(\alpha) \neq 0\}$. □

Remark 3.2 i) In some cases the polynomials $f(x)$ or $\mathcal{R}_\ell(f(x))$ have r-th powers as factors. If this occur, the equation defining the curve $\mathcal{C}$ can be rewriten after eliminating such powers. However we prefer not to make this transformation, since if we do it then in the equation defining the curve $\mathcal{C}$ it is not evident the relation between the polynomials $\ell(x)$, $f(x)$ and $\mathcal{R}_\ell(f(x))$.

We will then write inside brackets the transformed equation obtained after eliminating these r-th powers.

ii) Observe that in the proof of Proposition 3.1 we only counted the rational points coming from the roots of the polynomial $\ell(x)$ in $\mathbb{F}_q$. We can obtain other rational points coming from the ramification points and also from the rational solutions of the equation

$$T^r = u(x) \tag{2}$$

outside of $\mathcal{V}_\ell$; i.e., with the first coordinate distinct from the roots of the polynomial $\ell(x)$. We will denote the number of these first coordinates by κ.

Observe that the solutions $x = \alpha$ of Equation (2) such that $\ell(\alpha)h(\alpha) \neq 0$ with $h(x)$ as in Equation $(*)$ above, correspond to the elements $\alpha \in \mathbb{F}_q$ such that $u(\alpha)$ is a r-th power in $\mathbb{F}_q$ distinct from 1.

We always have that

$$\kappa \geq \#\{\alpha \in \mathcal{V}_h \cap \mathbb{F}_q \text{ such that } f(\alpha)\ell(\alpha) \neq 0\},$$

where as before $f(x) = \ell(x)h(x) + \mathcal{R}_\ell(f(x))$, and we have equality above if $r = q-1$. Of course each first coordinate $x = \alpha$ gives rise to exactly r rational points over $\mathbb{F}_q$ having that first coordinate.

To analyze the ramification points of $\mathcal{C}$ we will proceed as follows: Let $\alpha \in \mathbb{F}_q$ be a root or pole of $u(x)$ and let m be its multiplicity. We can write the equation defining $\mathcal{C}$ as

$$y^r = (x-\alpha)^m \phi(x),$$

with $\phi(x) \in \mathbb{F}_q(x)$ and $\phi(\alpha) \neq 0$. If $d = \gcd(r, |m|)$ then we have

$$\left(\frac{y^{\frac{r}{d}}}{(x-\alpha)^{\frac{m}{d}}}\right)^d = \phi(x).$$

Then, the d points corresponding to $x = \alpha$ are rational if and only if $\phi(\alpha)$ is a d-th power in $\mathbb{F}_q$

iii) By Remark 2.2, *ii*) if the curve $\mathcal{C}$ in Proposition 2.1 is defined by equations of the type

$$y^r = \mathcal{R}_\ell(f(x)^r) \quad \text{or} \quad y^r = \frac{\mathcal{R}_\ell(f(x)^{r+k})}{\mathcal{R}_\ell(f(x)^k)},$$

we obtain similar lower bounds for the number of $\mathbb{F}_q$-rational points.

In accordance with the previous proposition, it will be convenient to consider polynomials $\ell(x)$ with many roots in $\mathbb{F}_q$. This property will allow us to obtain a substantial number of rational points. In the next sections, we will construct some of those polynomials $\ell(x)$ and $f(x)$ leading to curves with many points.

We end this section with the following proposition which justifies the assumption made above in Equation $(*)$ i.e.,

$$\deg \mathcal{R}_\ell(f(x)) < \deg \ell(x).$$

Proposition 3.2 *Let $\mathcal{C}$ be a curve over the finite field $\mathbb{F}_q$ given by the Kummer equation*

$$y^r = \mu(x) := \frac{a(x)}{b(x)}, \text{ with } r \text{ a divisor of } q-1,$$

and assume that the rational function $\mu(x)$ is not the $d-th$ power of an element of $\bar{\mathbb{F}}_q(x)$ for any divisor d of r with $d > 1$. Then there exists an absolutely irreducible curve $\tilde{\mathcal{C}}$ over $\mathbb{F}_q$ defined by an equation of type (1), for some polynomials $f(x)$ and $\ell(x)$ in $\mathbb{F}_q[x]$, such that the curve $\tilde{\mathcal{C}}$ is isomorphic to $\mathcal{C}$.

Proof: First of all we can suppose that $\deg(a(x)) \geq \deg(b(x))$. In fact just notice that the equation for $y_1 = y^{-1}$ is

$$y_1^r = \frac{b(x)}{a(x)}.$$

If $\deg(a(x)) > \deg(b(x))$ then the polynomials $f(x) := a(x)$ and $\ell(x) := a(x) - b(x)$ satisfy $a(x) = \ell(x) + b(x)$ with $\deg(b(x)) < \deg(\ell(x))$.

If $\deg(a(x)) = \deg(b(x))$ then, let θ be an element of the set

$$\Gamma = \{\alpha \in \mathbb{F}_q \text{ such that } \mu(\alpha) \text{ is an } r\text{-th power in } \mathbb{F}_q^*\},$$

and consider the curve $\tilde{\mathcal{C}}$ defined by the equation

$$z^r = \frac{(x-\theta)^r a(x)}{b(x)}.$$

In this case we have that $\deg((x-\theta)^r a(x)) > \deg(b(x))$ and hence we are in the above case. Now, the application

$$\begin{array}{rccc} \pi : & \mathcal{C} & \longrightarrow & \tilde{\mathcal{C}} \\ & (x,y) & \mapsto & (x,(x-\theta)y) \end{array}$$

gives the desired isomorphism. $\square$

4 Certain symmetric polynomials and Kummer curves

In this section we introduce the polynomials $s_{m,j}(x)$ (see [2]) and we use them to construct curves over the finite field $\mathbb{F}_{q^m}$ with many rational points, using the method of section 2.

For integers $m \geq 1$ and $j = 1, \dots m$ we define (See [2])) a polynomial $s_{m,j}(x) \in \mathbb{F}_q[x]$ as follows

$$s_{m,j}(x) := s_j(x, x^q, \dots, x^{q^{m-1}}),$$

where $s_j(x_1, \dots, x_m)$ is the j-th elementary symmetric polynomial in m variables over $\mathbb{F}_q$. We agree to define $s_{m,0}(x) := 1$ and $s_{m,j}(x) := 0$ for $j > m$ and for $j < 0$.

Lemma 4.1 *For all $j \in \mathbb{Z}$ and $m \geq 2$ the following holds*

i) $s_{m,j}(x) = s_{m-1,j}(x)^q + x s_{m-1,j-1}(x)^q.$

ii) $s_{m,j}(x) = x^{q^{m-1}} s_{m-1,j-1}(x) + s_{m-1,j}(x).$

iii) $s_{m,j}(x)^q - s_{m,j}(x) = (x^{q^m} - x) s_{m-1,j-1}(x)^q.$

Proof: Let $\Lambda_{m,j}$ be a subset of $\mathbb{N}^j$ consisting of $\alpha := (\alpha_1, ...\alpha_j)$ with $0 \leq \alpha_i \leq m-1$ and $\alpha_1 < \alpha_2 < ... < \alpha_j$.

Let $\Lambda^*_{m,j} = \{\alpha \in \Lambda_{m,j} \; ; \; \alpha_1 > 0\}$.

We have clearly a bijection

$$\begin{array}{ccc} \Lambda_{m,j} & \longleftrightarrow & \{\text{Monomials of } s_{m,j}(x)\} \\ \alpha & \mapsto & x^{q^{\alpha_1}} x^{q^{\alpha_2}} ... x^{q^{\alpha_j}} \end{array}$$

The polynomial $s_{m,j}(x)$ is the sum of $\binom{m}{j}$ monomials corresponding to the distinct elements of $\Lambda_{m,j}$.

Now, looking at $\alpha \in \Lambda_{m,j}$ with $\alpha_1 = 0$, we see that $s_{m,j}(x)$ contains all monomials of the form $xg(x)$ where $g(x) = x^{q^{\beta_1}} ... x^{q^{\beta_{j-1}}}$ with $\beta = (\beta_1, .., \beta_{j-1}) \in \Lambda^*_{m,j-1}$. Hence $g(x) = (x^{q^{\beta_1 - 1}} ... x^{q^{\beta_{j-1} - 1}})^q$ with $\beta - 1 := (\beta_1 - 1, ..., \beta_{j-1} - 1) \in \Lambda_{m-1,j-1}$.

The remaining monomials of $s_{m,j}(x)$ are of the form $x^{q^{\alpha_1}} \ldots x^{q^{\alpha_j}}$ where $\alpha = (\alpha_1, \ldots \alpha_j) \in \Lambda^*_{m,j}$ i.e., they are of the form $(x^{q^{\alpha_1 - 1}} \ldots x^{q^{\alpha_j}})^q$ with $\alpha - 1 = (\alpha_1 - 1, \ldots \alpha_j - 1) \in \Lambda_{m-1,j}$. This proves item i).

The second item is proven in a similar way. Now by item ii) we have

$$s_{m,j}(x)^q = x^{q^m} s_{m-1,j-1}(x)^q + s_{m-1,j}(x)^q,$$

and combining this equality with i) we obtain iii). $\square$

Remark 4.1 The item *iii)* in Lemma 4.1 gives two interesting facts: firstly the polynomial function $s_{m,j}$ sends $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ for $j = 0, \ldots, m$ (moreover, it is not hard to see that the polynomial function $s_{m,j}$ is either constant or surjective); secondly, the roots of the polynomial $s_{m,j}(x)$ belong to $\bigcup_{1 \leq t \leq m} \mathbb{F}_{q^t}$. (See [2],Th 3.2).

Lemma 4.2 *The polynomial $\tau_m(x) := \sum_{j=0}^{m-1} s_{m,j}(x)$ is separable, it has deg(τ_m) $= t_m := q^{m-1} + \ldots + q$ and its roots belong to $\mathbb{F}_{q^m}$*

Proof: First, observe that $\tau_m(x) = \sum_{j=0}^{m} s_{m,j}(x) - s_{m,m}(x)$. By Lemma 4.1, item i) we have

$$\begin{aligned}
\textstyle\sum_{j=0}^{m} s_{m,j}(x) &= \left(\sum_{j=0}^{m-1} s_{m-1,j}(x)\right)^q + x\left(\sum_{j=1}^{m} s_{m-1,j-1}(x)\right)^q \\
&= \left(\sum_{j=0}^{m-1} s_{m-1,j}(x)\right)^q + x\left(\sum_{j=0}^{m-1} s_{m-1,j}(x)\right)^q \\
&= (x+1)\left(\sum_{j=0}^{m-1} s_{m-1,j}(x)\right)^q .
\end{aligned}$$

Also, $s_{m,m}(x) = x s_{m-1,m-1}(x)^q$ and therefore

$$\tau_m(x) = x\tau_{m-1}(x)^q + \sum_{j=0}^{m-1} s_{m-1,j}(x)^q.$$

It follows that $\tau'_m(x) = \tau_{m-1}(x)^q$ and hence

$$\begin{aligned}
\gcd(\tau_m(x), \tau'_m(x)) &= \gcd(\sum_{j=0}^{m-1} s_{m-1,j}(x)^q \ , \ \sum_{j=0}^{m-1} s_{m-1,j}(x)^q - s_{m-1,m-1}(x)^q) \\
&= \gcd(\sum_{j=0}^{m-1} s_{m-1,j}(x)^q \ , \ s_{m-1,m-1}(x)^q) \\
&= 1.
\end{aligned}$$

Now, it is clear that the degree of $\tau_m(x)$ is the degree of $s_{m,m-1}(x)$ which is t_m. The last assertion that the roots of $\tau_m(x)$ belong to $\mathbb{F}_{q^m}$ follows from the separability (see [2], Theorem 3.6). $\square$

Now we are going to use the polynomials $\tau_m(x)$ to construct curves with many rational points. For this we need the next result:

Lemma 4.3 *If $\ell(x) = \tau_m(x)$ and $f(x) = s_{m,m}(x+1)$, then*

$$\mathcal{R}_\ell(f(x)) = -x(x+1)\tau_{m-1}(x)^q = -(xs_{m,m}(x+1) - (x+1)s_{m,m}(x)).$$

Proof: The equality

$$x(x+1)\tau_{m-1}(x)^q = xs_{m,m}(x+1) - (x+1)s_{m,m}(x)$$

follows easily form the equality

$$\tau_{m-1}(x) = s_{m-1,m-1}(x+1) - s_{m-1,m-1}(x)$$

Now we compute the polynomial $\mathcal{R}_\ell(f(x))$.

From the proof of the Lemma 4.2 we have

$$\tau_m(x) - x\tau_{m-1}(x)^q = \sum_{j=0}^{m-1} s_{m-1,j}(x)^q.$$

Also, it is easy to prove (by induction) that

$$(x+1)^{q^{m-1}+\ldots+q+1} = \sum_{j=0}^{m} s_{m,j}(x).$$

On the other hand, again by the proof of the Lemma 4.2,

$$\sum_{j=0}^{m} s_{m,j}(x) \quad = \quad (x+1)\sum_{j=0}^{m-1} s_{m-1,j}(x)^q.$$

Therefore

$$\begin{aligned} s_{m,m}(x+1) = (x+1)^{q^{m-1}+\ldots+q+1} &= \sum_{j=0}^{m} s_{m,j}(x) \\ &= (x+1)(\tau_m(x) - x\tau_{m-1}(x)^q) \\ &= (x+1)\tau_m(x) - x(x+1)\tau_{m-1}(x)^q. \end{aligned}$$

□

The important features of taking $\ell(x)$ and $f(x)$ as in the Lemma 4.3 are:

i) The polynomial $\ell(x)$ is separable and its roots belong to $\mathbb{F}_{q^m}$.

ii) Both polynomials $f(x)$ and $\mathcal{R}_\ell(f(x))$ are highly inseparable.

We now give a result that explores those two features:

Theorem 4.1 *Let $m \geq 2$, $\ell(x) = \tau_m(x)$ and $f(x) = s_{m,m}(x+1)$. The non-singular complete geometrically irreducible curve $\mathcal{C}$ over $\mathbb{F}_{q^m}$ defined by the Kummer equation*

$$y^r = -\frac{s_{m,m}(x+1)}{x(x+1)\tau_{m-1}(x)^q} = -\frac{s_{m,m}(x+1)}{xs_{m,m}(x+1) - (x+1)s_{m,m}(x)},$$

with r a divisor of $q^m - 1$, has genus given by

$$g(\mathcal{C}) = \frac{(t_{m-1}+1)(r-1)-(u+v)+2}{2}$$

where t_{m-1} is defined as in the Lemma 4.2, $u = gcd(t_{m-1}+1, r)$ and $v = gcd(q-1, r)$ and the set of $\mathbb{F}_{q^m}$-rational points on $\mathcal{C}$ satisfies $\#\mathcal{C}(\mathbb{F}_{q^m}) \geq rt_m + 1$.

Proof: The point corresponding to $x = 0$ is totally ramified, and this guarantees that the curve is indeed geometrically irreducible (See [13]).

The points on $\mathcal{C}$ corresponding to $x = -1$ and $x = \infty$ have ramification indices $e = \frac{r}{u}$ and $e = \frac{r}{v}$, respectively.

To see this assertion for the points with $x = -1$, one can prove by induction that $\tau_m(-1) = (-1)^{m+1}$.

Notice also that $\gcd(t_m, r) = \gcd(t_{m-1}+1, r)$. Moreover we have u points on $\mathcal{C}$ with $x = -1$ and v points with $x = \infty$.

Besides $x = 0$, since $\tau_{m-1}(x)$ is separable, we have $t_{m-1} = \deg(\tau_{m-1})$ other points that are totally ramified, and hence the genus formula follows from Proposition 3.1.

The estimate for number of rational points over $\mathbb{F}_{q^m}$ also follows from Proposition 3.1, since $\tau_m(-1) \neq 0$. □

Remark 4.2 To compute the exact number of rational points of the curve in the above Theorem, we have to analyze the ramification points of $\mathcal{C}$ and also compute the rational solutions of the Equation (2) in Remark 3.2.

For the ramification points with $x \neq 0$, we have those satisfying $\tau_{m-1}(x) = 0$. By Lemma 4.2 we have that the roots of $\tau_{m-1}(x) = 0$ with $x \in \mathbb{F}_{q^m}$ must lie in $\mathbb{F}_q$ (i.e., $x \in \mathbb{F}_q$).

i) If $\alpha \in \mathbb{F}_q^*$ is a pole of

$$\frac{s_{m,m}(x+1)}{x(x+1)\tau_{m-1}(x)^q} = -\frac{s_{m,m}(x+1)}{x s_{m,m}(x+1) - (x+1)s_{m,m}(x)}$$

then α satisfies the equation:

$$\left(1 + \frac{1}{\alpha}\right)^{m-1} = 1.$$

The above equation for α has $d-1$ solutions in $\mathbb{F}_q$with $d := gcd(m-1, q-1)$ and therefore we have $d-1$ extra rational points coming from $\tau_{m-1}(x) = 0$.

ii) Let P_{-1} denote a point with first coordinate $x = -1$. Then by Remark 3.2 the point P_{-1} is rational, if and only if $\tau_{m-1}(-1) = (-1)^m$ is an u-th power in $\mathbb{F}_{q^m}$; i.e., if and only if

$$\begin{cases} m \text{is even or} \\ p = 2 \text{ or} \\ m \text{is odd, } p \neq 2 \text{ and } \frac{q^m-1}{u} \text{is even.} \end{cases}$$

In these cases we have u rational points with $x = -1$.

iii) Denoting by P_∞ a point with $x = \infty$, we have that P_∞ is rational point if and only if $p = 2$ or $\frac{q^m-1}{v}$ is even, in this case we have v rational points with $x = \infty$.

The following examples are applications of Theorem 4.1 in the case $m = 3$.

Example 4.1 Let $q = 2$. Then $\ell(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and we have the curve $\mathcal{C}$ over $\mathbb{F}_8$ defined by the equation

$$y^7 = \frac{(x+1)^6}{x(x^2+x+1)^2}.$$

This curve has genus $g(\mathcal{C}) = 9$.

By inspection we see that the Equation (2) has no solution in $\mathbb{F}_8\backslash\mathcal{V}_\ell$ and since $p=2$, by Remark 3.2 the points corresponding to $x=0$, $x=1$ and $x=\infty$ are rational; therefore the number of $\mathbb{F}_8$-rational points is $\mathcal{C}(\mathbb{F}_8)=7\times 6+3=45$. One does not know any curve over $\mathbb{F}_8$ of genus 9 having more than 45 rational points. (See table in [5]). $\square$

Example 4.2 For $q=3$, we have that $\ell(x)=x^{12}+x^{10}+x^9+x^4+x^3+x+1$. Consider the curve $\mathcal{C}$ over $\mathbb{F}_{27}$ given by the equation

$$y^r=-\frac{(x+1)^{12}}{x(x^3+x+1)^3}\,,\qquad \text{with } r \text{ a divisor of } 26.$$

For $r=2$ we obtain a curve $\mathcal{C}$ with genus $g(\mathcal{C})=1$. For the rational points, by Remark 3.2 we obtain one rational point corresponding to $x=1$ (since in this case $d=2$). On the other hand, the points corresponding to $x=-1$ and $x=\infty$ are not rational over $\mathbb{F}_{27}$ since (-1) is not a square in the finite field with 27 elements. (See Remark 3.2 *ii*) and *iii*)). Therefore $\#\mathcal{C}(\mathbb{F}_{27})=2\times(12+6)+1+1=38$; this curve attains the Serre's bound.

For $r=26$, the curve has genus $g(\mathcal{C})=49$. Equation (2) does not have solution outside of $\mathcal{V}_\ell$ (See Remark 2.3). The points corresponding to $x=-1$ and $x=\infty$ are not rational; then we have $\#\mathcal{C}(\mathbb{F}_{27})=26\times 12+1+1=314$. Ones does not know any curve over $\mathbb{F}_{27}$ of genus 49 having more than 314 rational points. (See table in [5]). $\square$

Example 4.3 In this example we will construct two curves $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_{125}$ with genus $g(\mathcal{C}_1)=2$ and $g(\mathcal{C}_2)=7$ respectively, the number of rational points of these curves provides a new entries in table (see[14]).

For $q=5$, we have $\ell(x)=x^{30}+x^{26}+x^{25}+x^6+x^5+x+1$; we then consider the curve $\mathcal{C}$ over $\mathbb{F}_{125}$ defined by the equation

$$y^r=-\frac{(x+1)^{30}}{x(x^5+x+1)^5}\,,\qquad \text{with } r \text{ a divisor of } 124.$$

For $r = 2$ the genus is $g(\mathcal{C}) = 2$. The Equation (2) in Remark 3.2 has $\kappa = 43$ solutions outside of $\mathcal{V}_\ell$, furthermore $u = 2$, $d = 2$ and $v = 2$, therefore by Remark 3.2 *ii)* and *iii)* the points corresponding to $x = 0$, $x = -1$ and $x = \infty$ are rational; this implies $\#\mathcal{C}(\mathbb{F}_{125}) = 2 \times (30 + 43) + 5 = 151$.

For $r = 4$ we obtain, $g(\mathcal{C}) = 7$, the Equation (3.2) has $\kappa = 24$ solutions, $u = 2$, $d = 2$ and $v = 4$, therefore $\#\mathcal{C}(\mathbb{F}_{125}) = 4 \times (30 + 24) + 5 = 221$. $\square$

Particularly interesting in Theorem 4.1 is the case $m = 2$, more precisely we have the following result

Theorem 4.2 *Let $m = 2$ in Theorem 4.1. The non singular complete geometrically irreducible curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ given by the Kummer equation*

$$y^r = -\frac{(x+1)^q}{x}, \qquad \text{with } r \text{ a divisor of } q^2 - 1,$$

has genus $g(\mathcal{C}) = \frac{r-v}{2}$, and $\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + q(r-v) + 1$; i.e., $\#\mathcal{C}(\mathbb{F}_{q^2})$ attains the Hasse-Weil upper bound.

Proof: By the substitution $x \longmapsto -(1/w)$ we obtain the equation

$$y^r = \frac{w^q - 1}{w^{q-1}} \tag{3}$$

Now by [3] Example 6.3, the curve given by the equation

$$z^m = t(t+1)^{q-1}, \qquad m \mid q^2 - 1, \tag{4}$$

is maximal. But making the substitutions $t = \frac{1}{w-1}$ and $z = \frac{1}{y}$ in (4), we obtain the Equation (3).

$\square$

5 Constructions based on certain products of irreducible polynomials

To construct some of those polynomials $\ell(x)$ which are certain products of irreducible polynomials, observe that the number $N_p(n)$ of irreducible polynomials of degree n over $\mathbb{F}_p$ is given by the formula

$$N_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$

where $\mu(\cdot)$ is the Moebius function. (See [9], Th 3.25).

Then taking products $\ell(x)$ of j irreducible polynomials of degree n, we see that there exist at least $\binom{N_p(n)}{j}$ polynomials $\ell(x)$ of degree jn with all their roots in $\mathbb{F}_q$ with $q = p^n$. In particular, if we suppose that $f(x)$ is another polynomial such that $1 = \gcd(f(x), \ell(x))$ then the number of rational points of the curve $\mathcal{C}$ over $\mathbb{F}_q$ given by the equation

$$y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))}, \qquad \text{with } r \text{ a divisor of } q-1,$$

satisfies $\#\mathcal{C}(\mathbb{F}_q) \geq rjn$. This gives already many rational points and moreover one can check that in the special case $r = q-1$ the actual value of the number of rational points is some times close (if $\kappa = 0$) to the lower bound rjn given above. For $r \neq q-1$ one has to look for the possible extra rational points (see Remark 3.2)

5.1 Construction of curves over $\mathbb{F}_q$

Proposition 5.1.1 *Let a, b be elements of $\mathbb{F}_q^*$ with $q \geq 3$ such that $a+b \neq 0$. Then the non-singular complete geometrically irreducible curve $\mathcal{C}$ over $\mathbb{F}_q$ defined by the affine Kummer equation*

$$y^r = \frac{ax^{q-1}+b}{a+b}\ ,\ \textit{with } r \textit{ a divisor of } q-1,$$

has genus $g(\mathcal{C}) = \frac{(q-3)(r-1)}{2}$ *and the number of rational points satisfies*

$$\#\mathcal{C}(\mathbb{F}_q) = \begin{cases} r(q+1), & \textit{if } \alpha^{\frac{q-1}{r}} = \beta^{\frac{q-1}{r}} = 1. \\ rq, & \textit{if } \alpha^{\frac{q-1}{r}} = 1 \textit{ and } \beta^{\frac{q-1}{r}} \neq 1. \\ rq, & \textit{if } \alpha^{\frac{q-1}{r}} \neq 1 \textit{ and } \beta^{\frac{q-1}{r}} = 1. \\ r(q-1), & \textit{if } \alpha^{\frac{q-1}{r}} \neq 1 \textit{ and } \beta^{\frac{q-1}{r}} \neq 1. \end{cases}$$

where $\alpha = \frac{a}{a+b}$ *and* $\beta = \frac{b}{a+b}$. *In the particular case* $r = (q-1)$, *we always have* $\#\mathcal{C}(\mathbb{F}_q) = (q-1)^2$.

Proof: The formula for the genus follows of the fact that the polynomial $f(x) = ax^{q-1} + b$ is separable and that the points corresponding to $x = \infty$ are unramified. Note also that the ramification points (which are the zeros of $ax^{q-1} + b = 0$) are not rational over $\mathbb{F}_q$, since $a + b \neq 0$.

To compute the number of rational points, if we take $\ell(x) = x^{q-1} - 1$ then $ax^{q-1} + b = a(x^{q-1} - 1) + (a + b)$ and hence $\mathcal{R}_\ell(f(x)) = a + b$. Therefore we have $\#(\mathcal{C}(\mathbb{F}_q)) \geq r(q-1)$.

The remaining possibilities for rational points are the points with $x = 0$ or $x = \infty$. For the points over $x = \infty$, we denote by $\alpha = \frac{a}{a+b}$, then the points corresponding to $x = \infty$ are rational if and only if $\alpha^{\frac{q-1}{r}} = 1$. For the points over $x = 0$ we denote by $\beta = \frac{b}{a+b}$, then the points corresponding to $x = 0$ are rational if and only if $\beta^{\frac{q-1}{r}} = 1$. □

We now give three examples of good curves over the field $\mathbb{F}_5$ with five elements. The first one illustrates Proposition 5.1.1 and the other two illustrate the method in section 3.

Example 5.1.1 The above proposition gives, for $q = 5$, $r = 4$ and $a = 2 = b$, a curve $\mathcal{C}$ over $\mathbb{F}_5$ given by the equation

$$y^4 = \frac{x^4+1}{2}\,.$$

Then we have $g(\mathcal{C}) = 3$ and $\#\mathcal{C}(\mathbb{F}_5) = 16$. This curve $\mathcal{C}$ attains the Serre's bound over $\mathbb{F}_5$. $\square$

Example 5.1.2 Let $q = 5$, $\ell(x) = x^2 + x$ and $f(x) = x^3 - x^2 + x - 1$, then $f(x) = \ell(x)(x-2) + (3x-1)$. Therefore, the curve $\mathcal{C}$ over $\mathbb{F}_5$ given by the equation:

$$y^4 = \frac{f(x)}{3x-1} = 2(x-1)(x-3)$$

has genus $g(\mathcal{C}) = 1$ and $\#\mathcal{C}(\mathbb{F}_5) = 10$, i.e. this curve $\mathcal{C}$ attains the Serre's bound over $\mathbb{F}_5$. $\square$

Example 5.1.3 Taking $q = 5$, $\ell(x) = x^5 - x$ and $f(x) = (x^2+x+1)^3$, then we can write $f(x) = \ell(x)(x+3) + (x^4 + 2x^3 + 2x^2 + x + 1)$. The curve $\mathcal{C}$ over $\mathbb{F}_5$ given by the Kummer equation

$$y^4 = \frac{(x^2+x+1)^3}{x^4+2x^3+2x^2+x+1}\,,$$

has $g(\mathcal{C}) = 7$ and $\#\mathcal{C}(\mathbb{F}_5) = 22$. This is the best value known to $(q, g) = (5, 7)$. See table in [14].

The genus $g(\mathcal{C}) = 7$ since we have 6 totally ramified points, namely the ones corresponding to the zeros of the polynomials $x^2 + x + 1$ and $x^4 + 2x^3 + 2x^2 + x + 1$ furthermore we have two points corresponding to $x = \infty$ having ramification index $e = 2$. Hence we have $g(\mathcal{C}) = 7$.

Now, since the polynomials x^2+x+1 and $x^4+2x^3+2x^2+x+1$ are irreducible over $\mathbb{F}_5$, the points corresponding to their roots are not rational, then we have $\#\mathcal{C}(\mathbb{F}_5) = 4 \times 5 + 2 = 22$ rational points. The extra 2 points in the counting of rational points are the two points with $x = \infty$. $\square$

5.2 Construction of curves over $\mathbb{F}_{q^2}$

In this section, we will construct curves over $\mathbb{F}_{q^2}$ with many rational points.

For r a divisor of q^2-1, with $r \geq q-1$, we give a characterization of the polynomial $\mathcal{R}_\ell(f(x))$ when $\ell(x) = \frac{x^{q^2}-x}{x^q-x}$ and $f(x) = (x^q-x)^r$, (see Lemma 5.2.1). After that we consider polynomials $\ell(x)$ which are product of irreducible polynomials over $\mathbb{F}_q$ of degree 2 or $2n$, and we will reduce modulo $\ell(x)$ some appropriate polynomials $f(x)$.

Theorem 5.2.1 *Let r be a divisor of q^2-1 and $d = \gcd(r, q-1)$. Let ω be an element of $\mathbb{F}_{q^2}$ with $w^d = -1$. Then the curve $\mathcal{C}$ given by*

$$y^{\frac{r}{d}} = \omega(x^q - x)^{\frac{q-1}{d}}$$

has genus $g(\mathcal{C}) = (q-1)(\frac{r-d}{2d})$ and also $\#\mathcal{C}(\mathbb{F}_{q^2}) = (q^2-q)\frac{r}{d} + q + 1$. Hence $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$;i.e., it attains the Hasse-Weil upper bound.

Proof: Let Let $\ell(x) = \mathcal{P}_2(q) = \frac{x^{q^2}-x}{x^q-x}$ be the product of all monic irreducible polynomials of degree 2 over $\mathbb{F}_q$. Then

$$(x^q-x)^{q-1} = \frac{x^{q^2}-x^q}{x^q-x} = \frac{(x^{q^2}-x)-(x^q-x)}{x^q-x} = \ell(x) - 1.$$

Therefore $\mathcal{R}_\ell(x^q-x)^{q-1} = -1$. It is easy to see that we have $q+1$ points that are totally ramified, and that we have $\frac{r}{d}$ rational points over $\mathbb{F}_{q^2}$ above each $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. From these two facts it follows the formulas for the genus and for the number of rational points. $\square$

As a variation of Theorem 5.2.1 we will construct curves over $\mathbb{F}_{q^2}$ using other polynomials $f(x)$ that we will be reduced modulo $\ell(x) = \mathcal{P}_2(q) = \frac{x^{q^2}-x}{x^q-x}$

Example 5.2.1 In this example we will construct a curve $\mathcal{C}$ over $\mathbb{F}_{16}$ with $g(\mathcal{C}) = 4$ and $\#\mathcal{C}(\mathbb{F}_{16}) = 45$. This is the best value known (see table in [5]).

Observe that if $q = 4$ then $\ell(x) = \mathcal{P}_2(q) = x^{12} + x^9 + x^6 + x^3 + 1$; after some computations we obtain that $\mathcal{R}_\ell((x^3 + x^2 + 1)^4) = x^3(x+1)^3(x^3 + x + 1)$. Now, we consider the curve $\mathcal{C}$ over $\mathbb{F}_{16}$ defined by the Kummer equation

$$y^3 = \frac{(x^3 + x^2 + 1)^4}{x^3(x+1)^3(x^3 + x + 1)}\,.$$

The genus follows from the fact that there are 6 totally ramified points (namely the zeros of $x^3 + x^2 + 1$ and $x^3 + x + 1$). The points corresponding to $x = 0$, $x = 1$, $x = \infty$ and the zeros of $\ell(x)$ split completely and hence $\#\mathcal{C}(\mathbb{F}_{16}) = (12 + 3) \times 3 = 45$.

Observe that the curve $\mathcal{C}$ above can also be given by (see Remark 3.2 i))

$$z^3 = \frac{x^3 + x^2 + 1}{x^3 + x + 1}\,.$$

In fact, just take

$$z = \frac{yx(x+1)}{x^3 + x^2 + 1}\,. \tag{$*$}$$

In this case we have that the roots of the polynomial $x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x$ evaluated in RHS of the equation $(*)$ are cubes in $\mathbb{F}_{16}$. $\square$

The next Theorem provides curves over $\mathbb{F}_{q^2}$ with the same properties (genus and number of rational points) as the ones in Theorem 5.2.1, the equations defining these curves are of the type

$$y^r = R_\ell(f(x)^r) \quad \text{with } \ell(x) = x^{q^2} - x. \tag{5}$$

Before stating it we will prove the following result:

Lemma 5.2.1 *Let $\ell(x) = x^{q^2} - x$ and r be a divisor of q^2-1 such that $r \geq q-1$. Then*
$$\mathcal{R}_\ell((x^q - x)^r) = (-1)^n (x^q - x)^t\,,$$
where $r = (q-1)n + t$ with $0 < t \leq (q-1)$.

Proof: Let we denote by $v(x) = x^q - x$, then $v(x)^r = v(x)^{n(q-1)+t} = v(x)^{nq} v(x)^{t-n}$. Now, since $v(x)^q = x^{q^2} - x^q = \ell(x) - v(x)$, we have

$$\begin{aligned}
(x^{q^2} - x^q)^n &= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \ell(x)^i v(x)^{n-i} \\
&= ((-1)^n v(x)^n + \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} \ell(x)^i v(x)^{n-i}).
\end{aligned}$$

Therefore

$$\begin{aligned}
v(x)^r &= ((-1)^n v(x)^n + \ell(x) \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} \ell(x)^{i-1} v(x)^{n-i}) v(x)^{t-n} \\
&= \ell(x) \cdot (\sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} \ell(x)^{i-1} v(x)^{t-i}) + (-1)^n v(x)^t
\end{aligned}$$

This finishes with the lemma after observing that the expression
$$\sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} \ell(x)^{i-1} v(x)^{t-i}$$
is a polynomial since if $n > t$, then we rewrite this sum as

$$\sum_{i=1}^{t} (-1)^{n-i} \binom{n}{i} \ell(x)^{i-1} v(x)^{t-i} + \sum_{i=t+1}^{n} (-1)^{n-i} \binom{n}{i} \ell(x)^{i-1} v(x)^{t-i}$$

and each term in the second sum above is of the form (writing $i = t + j$, $j = 1, 2, ..., n-t$)
$$(-1)^{n-t-j} \binom{n}{t+j} \frac{\ell(x)^{t+j-1}}{v(x)^j} = (-1)^{n-t-j} \binom{n}{t+j} \ell(x)^{t-1} \left(\frac{\ell(x)}{v(x)}\right)^j$$

and $\frac{\ell(x)^{t+j-1}}{v(x)^j} \in \mathbb{F}_q[x]$ since $v(x)$ divides $\ell(x)$. $\square$

Remark 5.2.1 We have seen in the Lemma above that

$$(x^q - x)^r = (x^{q^2} - x)h(x) + (-1)^n (x^q - x)^t\,,$$

for some polynomial $h(x)$. This equality shows that for $x = \alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ we have that $(-1)^n(\alpha^q - \alpha)^t$ is a nonzero r-th power in $\mathbb{F}_{q^2}$. This will be used for the determination of the number of rational points in the next Theorem.

Theorem 5.2.2 *Let $r = (q-1)n + t$ be as in the Lemma 5.2.1 and let $d = gcd(r,t)$. Then the non-singular complete geometrically irreducible curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ defined by the affine Kummer equation*

$$y^{\frac{r}{d}} = \omega(x^q - x)^{\frac{t}{d}}\,, \qquad \textit{with } \omega^d = (-1)^n,$$

has genus $g(\mathcal{C}) = (q-1)(\frac{r-d}{2d})$ and its number of rational points satisfies $\#\mathcal{C}(\mathbb{F}_{q^2}) = (q^2 - q)\frac{r}{d} + q + 1$; i.e., $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$.

Proof: The consideration of such curve $\mathcal{C}$ is natural from Equation (6) and Lemma 5.2.1. As in the proof of the Theorem 5.2.1 we have that the point $x = \infty$ and the points with $x^q - x = 0$ are totally ramified and moreover there are the only ramified points of the curve $\mathcal{C}$

The points corresponding to $x = \alpha$ with $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ split completely (see Remark 2.2). From these facts follows the formulas for the genus and for the number of rational points. $\square$

Remark 5.2.2 If one takes divisors of $q^2 - 1$ such that $r = (q-1)n + (q-1)$ with n odd, then the condition $t = q - 1 \geq n$ is equivalent to the condition $r \neq q^2 - 1$. (if $r = q^2 - 1$ then $n = q$) Hence the Theorem 5.2.2 includes some of the curves appearing in the Theorem 5.2.1.

Proposition 5.2.1 *Let $p \neq 2$. The non-singular complete geometrically irreducible curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ defined by the affine Kummer equation*

$$y^r = \frac{x^{\frac{q-1}{2}}(x^{\frac{q-1}{2}}+1)^q}{x^{\frac{q-1}{2}}-1}, \qquad \textit{with } r \textit{ a divisor of } q^2-1,$$

has genus $g(\mathcal{C}) = \frac{(r-1)(q-3)+2(r-d)}{2}$, where $d = \gcd(r, \frac{q-1}{2})$ and the number of rational points satisfies $\#\mathcal{C}(\mathbb{F}_{q^2}) \geq r(\frac{q^2-1}{2}) + (q-1) + 2d$.

Proof: In this case we have $q-1$ totally ramified points, namely, the corresponding to the roots of the polynomials $x^{\frac{q-1}{2}}+1$ and $x^{\frac{q-1}{2}}-1$. There are d points lying over $x=0$ and $x=\infty$, these points have ramification index $e = \frac{r}{d}$, this gives the formula for the genus.

Now, if $\ell(x) = x^{\frac{q^2-1}{2}}+1$ and $f(x) = x^{\frac{q^2-1}{2}} + x^{\frac{q-1}{2}}$ then, the equation defining the curve $\mathcal{C}$ is of the form

$$y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))}$$

and, since the polynomial $\ell(x)$ has its roots in $\mathbb{F}_{q^2}$ then, the Proposition 3.1 guaranteed that at least $\#\mathcal{C}(\mathbb{F}_{q^2}) \geq r(\frac{q^2-1}{2})$.

Observe that, the polynomials $f_1(x) = x^{\frac{q-1}{2}}+1$ and $f_2(x) = x^{\frac{q-1}{2}}-1$ have their roots in $\mathbb{F}_{q^2}$ and for $\alpha \in \mathbb{F}_{q^2}$ such that $f_1(\alpha)=0$ or $f_2(\alpha)=0$ we have $\ell(\alpha) \neq 0$, wich contribute with $q-1$ rational points.

Now, its easy to see that the points lying over $x=0$ and $x=\infty$ are rational see Remark 3.2 and hence we have $2d$ extra rational points. This gives $\#\mathcal{C}(\mathbb{F}_{q^2}) = r(\frac{q^2-1}{2}+\kappa) + (q-1) + 2d$, where κ is the number of solutions of the Equation (2) in Remark 3.2 outside of $\mathcal{V}_\ell$. $\square$

The above proposition gives the following new entries in the tables (see [5] and [14]).

q	r	g	κ	$\#\mathcal{C}(\mathbb{F}_{q^2})$
5	4	5	0	56
	8	13	0	104
	12	21	0	152
	24	45	0	296
9	40	153	0	1616
	80	313	0	3216

Remark 5.2.3 It is not always true that $\kappa = 0$ (see Remark 3.2), for example for $q = 3$ and $r = 2$ we have $\kappa = 2$ and this gives a curve over $\mathbb{F}_9$ with genus 1 and 16 rational points, i.e., a maximal curve. For $q = 9$ and $r = 5$ we obtain $\kappa = 32$ and this provides a maximal curve over $\mathbb{F}_{81}$ of genus 16. For $q = 5$ we have $\kappa = 8$, then we get a maximal curve over $\mathbb{F}_{25}$ of genus 6.

In the next two examples we will construct curves over the finite field $\mathbb{F}_{25}$. In these examples we take $\ell(x)$ as an appropriate product of irreducible polynomials of degree two over the finite field $\mathbb{F}_5$. The values $(g, \#\mathcal{C}(\mathbb{F}_{25}))$ for the genus and the number of rational points obtained in these examples, provide new entries for the tables in [14].

We will use the following irreducible polynomials over $\mathbb{F}_5$:

$$\begin{aligned}
\ell_1(x) &= x^2 + 2\\
\ell_2(x) &= x^2 + 3\\
\ell_3(x) &= x^2 + 2x + 4\\
\ell_4(x) &= x^2 + 3x + 3\\
\ell_5(x) &= x^2 + 3x + 4\\
\ell_6(x) &= x^2 + 4x + 1.
\end{aligned}$$

Example 5.2.2 Let $q = 5$. In this example we will construct a curve $\mathcal{C}$ over $\mathbb{F}_{25}$, with genus $g(\mathcal{C}) = 7$ and $\#\mathcal{C}(\mathbb{F}_{25}) = 76$. This provides a new entry in the table [14].

Consider the polynomials $\ell(x) = \ell_1(x)\ell_2(x)\ell_5(x)\ell_6(x) = x^8 + 2x^7 + 2x^6 + 4x^5 + 2x^3 + 2x^2 + 4x + 4$ and $f(x) = (x+1)^9$ then, after some computations we obtain that

$$(x+1)^9 = \ell(x)(x+2) + (x^2+x+2)^3.$$

Observe that for a divisor r of 24, the equation

$$y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))} = \frac{(x+1)^9}{(x^2+x+2)^3}$$

is not always absolutely irreducible, since the RHS of this equation is a cube. In this case we will consider the curve $\mathcal{C}$ defined by the equation

$$y^{\frac{r}{d}} = \left(\frac{f(x)}{\mathcal{R}_\ell(f(x))}\right)^{\frac{1}{d}}, \text{ with } d = \gcd(3, r).$$

For example, for $r = 24$ we are lead to consider the curve $\mathcal{C}$ over $\mathbb{F}_{25}$ defined by the affine equation

$$y^8 = \frac{(x+1)^3}{x^2+x+2}.$$

In this case we have 4 totally ramified points, namely the points corresponding to $x = -1$, $x = \infty$ and $x = \gamma_i$ with $i = 1, 2$ and $\gamma_i^2 + \gamma_i + 2 = 0$, this gives $g(\mathcal{C}) = 7$.

Now, the only solution of the Equation (2) in Remark 3.2 outside of $\mathcal{V}_\ell$ is $x = 3$, then, the number of rational points is $\#\mathcal{C}(\mathbb{F}_{25}) = 8 \times (8+1) + 4 = 76$. $\square$

Example 5.2.3 Consider the curve $\mathcal{C}$ over $\mathbb{F}_{25}$ defined by the equation

$$y^r = \frac{x^5(x+1)^5}{(x+3)(x^2+2x+3)^4}, \qquad \text{where } r \text{ is a divisor of 24.}$$

This equation was obtained taking $\ell(x) = \ell_1(x)\ell_2(x)\ell_3(x)\ell_4(x)\ell_6(x) = x^{10} + 4x^9 + 4x^8 + 3x^6 + x^4 + 2x^2 + x + 2$ and $f(x) = (x^2+x)^5$. In this case we have 4 points totally ramified (the corresponding to $x=0$, $x=-1$, $x=-3$ and $x=\infty$ and two points (the corresponding to the roots of the polynomial x^2+2x+3) with ramification index $e=\frac{r}{d}$ where $d=\gcd(r,4)$, this gives $g(\mathcal{C})=(r-1)+(r-d)$.

To compute the rational points, we have by Proposition 3.1, that $\#\mathcal{C}(\mathbb{F}_{25})\geq 10r+4$. Now we have to analyze the points corresponding to the zeros of the polynomial x^2+2x+3, when $d=2$ or $d=4$.

For this, let θ and ζ be elements of $\mathbb{F}_{25}$ such that $(x-\theta)(x-\zeta)=x^2+2x+3$, then we have to solve the equation:

$$((x-\zeta)^{\frac{4}{d}}y^{\frac{24}{d}})^d=\frac{x^5(x^5+1)}{(x+3)(x-\theta)^4}$$

in $\mathbb{F}_{25}$, i.e., solve the equation:

$$T^d=\frac{\zeta^5(\zeta^5+1)}{(\zeta+3)(\zeta-\theta)^4} \tag{6}$$

in $\mathbb{F}_{25}$. Since $\zeta+\theta=3=\theta\zeta$, after some computations we obtain that $\zeta^5(\zeta^5+1)=\zeta-1$ and $(\zeta-\theta)^4=-1$, therefore, the Equation (6) becomes in

$$T^d=-\frac{\zeta-1}{\zeta-3}$$

and this equation has d solutions in $\mathbb{F}_{25}$ since $(\zeta-1)^6=\zeta^5-\zeta^4=1=(\zeta+3)^6$.

By the previous analysis the points corresponding to ζ and θ are rational and therefore $\#\mathcal{C}(\mathbb{F}_{25})\geq 10r+2d+4$. For $r=4,12,24$, the Equation (2) in Remark 3.2 has not solutions in $\mathbb{F}_{25}\backslash\mathcal{V}_\ell$ and we have the follow new entries in [14]

r	g	$N(\mathbb{F}_{25})$
4	3	52
12	19	132
24	43	252

$\square$

Example 5.2.4 Let $q = 4$. In this example we will construct two curves $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_{16}$ with $g(\mathcal{C}_1) = 2$ and $\#\mathcal{C}_1(\mathbb{F}_{16}) = 33$, and $g(\mathcal{C}_2) = 12$ and $\#\mathcal{C}_2(\mathbb{F}_{16}) = 83$. These curves attain the best values known for $(q, g) = (16, 2)$ and for $(q, g) = (16, 12)$. (See table in [5]).

Consider the curve $\mathcal{C}$ over $\mathbb{F}_{16}$ defined by the affine equation:

$$y^r = \frac{(x^3+1)^2}{x+1}, \qquad \text{with } r \text{ a divisor of 15.}$$

In this example we took, $\ell(x) = x^4 + x^3 + x^2 + x + 1$ and $f(x) = (x^3 + 1)^2$. We have clearly that $f(x) = (x^2 + x)\ell(x) + (x + 1)$.

Here, we have 3 totally ramified points namely, those corresponding to $x = 1$ and $x = \gamma_i$, $i = 1, 2$ with ${\gamma_i}^2 + \gamma_i + 1 = 0$. Now, if we denote by $d = \gcd(r, 5)$, then the d points corresponding to $x = \infty$ have ramification index $e = \frac{r}{d}$. This gives

$$g(\mathcal{C}) = \frac{(r-1)+(r-d)}{2}.$$

To compute the number of rational points, by Proposition 3.1 we have at least $r \times 4$ rational points, and since $\gamma_i \in \mathbb{F}_{16}$ for $i = 1, 2$ then we have 2 extra rational points.

We now claim that $x = 0$ is the only solution of the equation (2) in $\mathbb{F}_{16} \backslash \mathcal{V}_\ell$. In fact, if there exists another solution ζ we would have that $\zeta^4 + \zeta + 1 = 0$ or $\zeta^4 + \zeta^3 + 1 = 0$. Suppose that $\zeta^4 + \zeta + 1 = 0$ and $r = 5$, then (2) implies

$$\begin{aligned} 1 = [(\zeta+1)(\zeta^2+\zeta+1)^2]^3 &= (\zeta^3+\zeta+1)^3 \\ &= \zeta^9+\zeta^7+\zeta^6+\zeta^5+\zeta^2+\zeta+1 \\ &= \zeta^3+\zeta^2. \end{aligned}$$

This implies that $\zeta \in \mathbb{F}_8$ and therefore $\zeta \in \mathbb{F}_2$. This contradiction prove our claim (the other cases, $r = 3$ and $\zeta^4 + \zeta^3 + 1 = 0$ are similar) and hence we have $\#\mathcal{C}(\mathbb{F}_{16}) = 5r + d + 3$.

This gives for $r = 5$, $g(\mathcal{C}_1) = 2$ and $\#\mathcal{C}_1(\mathbb{F}_{16}) = 33$ and for $r = 15$, $g(\mathcal{C}_2) = 12$ and $\#\mathcal{C}_2(\mathbb{F}_{16}) = 83$. $\square$

Example 5.2.5 Let $\ell(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$ and $f(x) = (x^2 + x + 1)^4$. Then $\mathcal{R}_\ell(f(x)) = x^6(x + 1)$.

Consider the curve $\mathcal{C}$ over $\mathbb{F}_{16}$, defined by the affine Kummer equation

$$y^r = u(x) := \frac{(x^2 + x + 1)^4}{x^6(x + 1)}, \qquad \text{where } r \text{ is a divisor of } 15.$$

In this example we have four points totally ramified, namely the points corresponding to $x = \theta$ with $\theta^2 + \theta + 1 = 0$, $\theta = 1$ and $\theta = \infty$, the points corresponding to $x = 0$ have ramification index $e = \frac{r}{d}$ with $d = \gcd(r, 3)$ which are rational. This gives $g = \frac{2(r-1)+(r+d)}{2}$.

To compute the number of rational points, first we will analyze the possible solutions of the equation (2), observe that the only elements of $\mathbb{F}_{16}$ not involved up to now are the zeros of the polynomial $x^4 + x^3 + 1$, for such zeros we have that

$$x^4 + x^3 + 1 = 0 \quad \text{implies} \quad \frac{(x^2 + x + 1)^4}{x^6(x + 1)} = \left(\frac{1}{x}\right)^5$$

hence the right hand side $u(x)$ is a 5-th power in $\mathbb{F}_{16}$ for each one of the roots of $x^4 + x^3 + 1$. Therefore, the equation (2) contribute with 20 rational points only in the case $r = 5$. Then, we have

$$\#\mathcal{C}(\mathbb{F}_{16}) = \begin{cases} 12r + d + 4 & \text{if } r = 5 \\ 8r + d + 4 & \text{if } r \neq 5. \end{cases}$$

This gives the follow entries

r	g	$N(\mathbb{F}_{16})$
3	2	31
5	6	65
15	20	127

As in the above example these entries are the best values known. (See tables in [5].) $\square$

5.3 Construction of curves over $\mathbb{F}_{q^3}$

In this section, we will construct curves over $\mathbb{F}_{q^3}$ with many rational points. First, we give, in the following Theorem, a characterization of $\mathcal{R}_\ell(f(x))$ when $f(x) = (x^q - x)^{q^2-1}$ and $\ell(x) = \mathcal{P}_3(q) := \frac{x^{q^3}-x}{x^q-x}$. As an application of this Theorem we obtain some examples of 'good' curves. After that, we will construct the polynomials $\ell(x)$ as a product of irreducible polynomials over $\mathbb{F}_q[x]$ of degree three and reduce modulo $\ell(x)$ an appropriate polynomial $f(x)$, in this way we obtain curves providing new goods entries in the tables.

Theorem 5.3.1 *Let $\ell(x) = \mathcal{P}_3(q) := \frac{x^{q^3}-x}{x^q-x}$ and r be a divisor of q^3-1. The curve $\mathcal{C}$ over $\mathbb{F}_{q^3}$ defined by the affine equation*

$$y^r = \frac{(x^q-x)^{q^2-1}}{\mathcal{R}_\ell((x^q-x)^{q^2-1})} = -\frac{(x^q-x)^{q^2-1}}{(x^q-x)^{q-1}+1}$$

has genus

$$g = \frac{(q+1)((q-2)(r-1)+(r-d))}{2}$$

where $d = gcd(r, q-1)$, and its number of rational points over $\mathbb{F}_{q^3}$ satisfies

$$\#\mathcal{C}(\mathbb{F}_{q^3}) = \begin{cases} r(q^3-q)+d(q+1) & \textit{if } p=2 \textit{ or } \frac{q-1}{d} \textit{ is even} \\ r(q^3-q) & \textit{otherwise} \end{cases}$$

Proof: Since

$$(x^q-x)^{q^2-1} = \frac{(x^q-x)^{q^2}}{x^q-x} = \frac{(x^{q^3}-x)-(x^{q^2}-x)}{x^q-x} = \mathcal{P}_3(q)-\mathcal{P}_2(q),$$

then $\mathcal{R}_\ell((x^q-x)^{q^2-1}) = -\mathcal{P}_2(q) = -(x^q-x)^{q-1}-1$. Now, since degree$(\mathcal{P}_2(q)) = q^2-q$ and its roots belong to $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$ we have q^2-q totally ramified points.

There are d points above $x=\infty$ and above each $x=\alpha$ with $\alpha\in\mathbb{F}_q$, each one with ramification index $e=\frac{r}{d}$. The genus follows of the Hurwitz formula. (See Proposition 2.1).

The number of rational points follows from Proposition 3.1, and the following fact:

For all $\alpha\in\mathbb{F}_q$ we define the polynomial $\phi_\alpha(x) := \frac{x^q-x}{x-\alpha}$, then $\phi_\alpha(\alpha)\in{\mathbb{F}_q}^*$, now, if we rewrite the equation defining the curve $\mathcal{C}$ as

$$y^r = -\frac{(x-\alpha)^{q^2-1}\phi_\alpha(x)^{q^2-1}}{(x^q-x)^{q-1}+1}$$

then we have

$$\left(\frac{y^{\frac{r}{d}}}{(x-\alpha)^{\frac{q^2-1}{d}}}\right)^d = -\frac{\phi_\alpha(x)^{q^2-1}}{(x^q-x)^{q-1}+1}$$

one see that the RHS of this equality take the value -1 when $x=\alpha$, and hence by Remark 3.2, the points corresponding to $\alpha\in\mathbb{F}_q$ are rational if and only if $p=2$ or $\frac{q-1}{d}$ is even. $\square$

As an illustration of the results in Theorem 5.3.1 we give three examples of 'goods' curves over $\mathbb{F}_{q^3}$.

Example 5.3.1 For $q = 3$, we obtain the curve $\mathcal{C}$ over $\mathbb{F}_{27}$ given by

$$y^r = -\frac{(x^3 - x)^8}{x^6 + x^4 + x^2 + 1}, \qquad r \text{ a divisor of } 26.$$

Taking $r = 2$ we have $g(\mathcal{C}) = 2$ and $\#\mathcal{C}(\mathbb{F}_{27}) = 48$; this curve attains Serre's bound.

For $r = 13$, we obtain $g(\mathcal{C}) = 48$ and $\#\mathcal{C}(\mathbb{F}_{27}) = 316$. This number is very close to best known value which is 325 (see table in [5]). □

Example 5.3.2 Taking $q = 5$ we leads to consider the curve $\mathcal{C}$ given by

$$y^2 = -\frac{(x^5 - x)^{24}}{x^{20} + x^{16} + x^{12} + x^8 + x^4 + 1} \quad (\text{or by} \quad z^2 = x^{20}+x^{16}+x^{12}+x^8+x^4+1)$$

.

In this case $g(\mathcal{C}) = 9$ and $\#\mathcal{C}(\mathbb{F}_{125}) = 252$, this is the best known value for $(q, g) = (125, 9)$ see [14] □

In the following proposition we will construct a family of curves over $\mathbb{F}_{q^3}$ using the method of section 3. We take $\ell(x) = x^{q^2} + x^q + x - 1$ and observe that the roots of $\ell(x)$ are exactly the elements of the set set $\{\alpha \in \mathbb{F}_{q^3}$ such that $Tr(\alpha) = 1\}$, where $Tr(x)$ is the trace function of $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$. As an application of the next proposition we will obtain (for $q = 3$) a curve $\mathcal{C}$ over $\mathbb{F}_{27}$ which provides a new entry in the table. (See [5].)

Proposition 5.3.1 *Let $q \geq 3$. The non-singular complete geometrically irreducible curve $\mathcal{C}$ over $\mathbb{F}_{q^3}$ defined by the affine Kummer equation*

$$y^r = -\frac{x^q(x^{q-1}+1)^q}{x-1}, \qquad \textit{with } r \textit{ a divisor of } q^3-1,$$

has genus

$$g(\mathcal{C}) = \begin{cases} \frac{(r-1)(q-3)+2(r-d)}{2} & \textit{if } p=2 \\ \frac{(r-1)(q-1)+(r-d)}{2} & \textit{if } p\neq 2 \end{cases}$$

where $d = gcd(q^2-1, r)$*, and the number of rational points satisfies:*

$$\#\mathcal{C}(\mathbb{F}_{q^3}) \geq \begin{cases} r(q^2-1)+2d+q-1 & \textit{if } p=2 \\ rq^2+d+2 & \textit{if } p\neq 2 \textit{ and } \frac{q-1}{d} \textit{ is even} \\ rq^2+2 & \textit{if } p\neq 2 \textit{ and } \frac{q-1}{d} \textit{ is odd} \end{cases}$$

Proof: If $p=2$, then the points corresponding to $x=1$, and $x=\infty$, has ramification index $e=\frac{r}{d}$, the other points corresponding to $\alpha \in \mathbb{F}_q$ with $\alpha \neq 1$ are totally ramified. If $p \neq 2$, then, in this case we have $q+1$ totally ramified points, and the d points corresponding to $x=\infty$ has ramification index $e=\frac{r}{d}$. Then the genus follows of the Riemann-Hurwitz formula.

Now, observe that the equation defining the curve $\mathcal{C}$ is nothing but

$$y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))},$$

where $\ell(x) = x^{q^2}+x^q+x-1$ and $f(x)=x^{q^2}+x^q$.

Then, to compute the number of rational points, since the polynomial $\ell(x) = x^{q^2}+x^q+x-1$ has its roots in $\mathbb{F}_{q^3}$, the Proposition 3.1 guaranteed at least $r(q^2-1)$ if $p=2$ (since $x+1=\gcd(f(x),\ell(x))$ in this case) and rq^2 rational points if $p\neq 2$.

On the other hand, by Remark 3.2, the d points corresponding to $x=\infty$ and $x=1$ are rational if $p=2$. In the case $p\neq 2$, the equation $x^{q-1}=-1$

has not solution in $\mathbb{F}_{q^3}$, therefore the points corresponding to the roots of this equation are not rational; finally, for this case by Remark 3.2, the d points corresponding to $x = \infty$ are rational if and only if $\frac{q-1}{d}$ is even. $\square$

Example 5.3.3 As an application of Proposition 5.3.1 we have for $q = 3$ and $r = 26$, a curve $\mathcal{C}$ over $\mathbb{F}_{27}$ with genus $g(\mathcal{C}) = 37$ and $\#\mathcal{C}(\mathbb{F}_{27}) = 236$. In this case $\kappa = 0$. This is a new entry in [5]. $\square$

6 Other Examples

As in the previous sections p is a prime number, $\mathbb{F}_q$ a finite field with $q = p^n$ elements and $\bar{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$. In this section we will construct curves over the finite field $\mathbb{F}_q$ using the method in section 3, taking the polynomial $\ell(x)$ as a product of irreducible polynomials of degree n over $\mathbb{F}_p$

Construction of curves over $\mathbb{F}_8$

In the next example, we will combine one Kummer and one Artin-Schreirer cover. In section 8, we will combine two Kummer covers.

Example 6.1 Taking $p = 2$, $n = 3$ and $\ell(x) = \mathcal{P}_3(2) = \frac{x^8+x}{x^2+x} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, we have $\mathcal{R}_\ell(x^3(x+1)^3) = x^2 + x + 1$. Now we consider the curve $\mathcal{C}$ over $\mathbb{F}_8$ given by the Kummer equation

$$y^7 = \frac{x^3(x+1)^3}{x^2+x+1}.$$

Then, the points corresponding to $x = 0$, $x = 1$, $x = \infty$ and $x^2 + x + 1 = 0$ are totally ramified, and the points corresponding to the roots of $\ell(x)$ split completely. This gives $g(\mathcal{C}) = 9$. Now it is clear that the points above $x = 0$, $x = 1$ and $x = \infty$ are rational, therefore $\#\mathcal{C}(\mathbb{F}_8) = 7 \times 6 + 3 = 45$ this is best values in [5] for $(q, g) = (8, 9)$.

Now we consider the Artin-Schreier cover $\tilde{\mathcal{C}}$ of the curve $\mathcal{C}$ given by

$$z^2 + z = u(x) = \frac{\ell(x)}{\mathcal{R}_\ell(x^3(x+1)^3)} = \frac{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1}{x^2 + x + 1}.$$

The only ramified points are the points above the roots of $x^2+x+1 = 0$ and they are totally ramified; the place P_∞ above $x = \infty$ is unramified, in fact, by Proposition 1.3, if we take $w = x^2 + x$ the we have:

$$\frac{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1}{x^2 + x + 1} + w^2 + w = \frac{1}{x^2 + x + 1}.$$

and therefore $\nu_{P_\infty}(u(x) + w^2 + w) > 0$.

This gives $g(\tilde{\mathcal{C}}) = 25$. Now, for the rational points, we see that there exist 2 points over each of the $(x, y) \in \mathcal{V}_\ell \times \mathbb{F}_8^*$, these points are rational; the two points corresponding to P_∞ are also rational (Observe that the equation $z^2 + z = 0$ has two distinct solutions in $\mathbb{F}_2$), and we have two extra rational points, then $\#\tilde{\mathcal{C}}(\mathbb{F}_8) = 86$ and this is the best values in [5] for $(q, g) = (8, 25)$. $\square$

Example 6.2 Taking $f(x) = (x^2+x+1)^4$ and $\ell(x) = x^8+x$, then $\mathcal{R}_\ell(f(x)) = x^4 + x + 1$. The curve $\mathcal{C}$ over $\mathbb{F}_8$ given by

$$y^7 = \frac{(x^2 + x + 1)^4}{x^4 + x + 1}.$$

has seven points which are totally ramified, and this gives $g(\mathcal{C}) = 15$. All points $x = \alpha$ with $\alpha \in \mathbb{F}_8$ split completely and the unique point above $x = \infty$ is also rational, then $\#\mathcal{C}(\mathbb{F}_8) = 7 \times 8 + 1 = 57$. This is the best known value for $(q, g) = (8, 15)$ in [5]. $\square$

Construction of curves over $\mathbb{F}_{32}$

In the next two examples we will construct curves over $\mathbb{F}_{32}$ taking $\ell(x)$ as a product of irreducible polynomials of degree 5 over $\mathbb{F}_2$. The values obtain here for the genus and number of rational points are the best values know in the tables (see [5]).

Example 6.3 Let $p = 2$, $n = 5$ and $\ell(x) = x^5 + x^2 + 1$. Consider the curve $\mathcal{C}$ given by the Kummer cover over $\mathbb{F}_{32}$

$$y^{31} = \frac{x^5}{(x+1)^2}.$$

Then we have three totally ramified points, namely the points above $x = 0$, $x = 1$ and $x = \infty$ this gives $g(\mathcal{C}) = 15$ and we have 31 rational points over each root of $\ell(x)$ then we obtain $31 \times 5 + 3 = 158$ rational points this attains the best value know $(32, 15)$ in [5] $\square$

Example 6.4 For $\ell(x) = (x^5+x^3+1)(x^5+x^2+1) = x^{10}+x^8+x^7+x^5+x^3+x^2+1$ and $f(x) = (x+1)^{10}$ we have $\mathcal{R}_\ell(f(x)) = x^3(x^2+x+1)^2$. Therefore in the Kummer extension

$$y^{31} = \frac{(x+1)^{10}}{x^3(x^2+x+1)^2},$$

we have 5 totally ramified points, this gives $g(\mathcal{C}) = 45$ and $31 \times 10 + 3 = 313$ rational points. This is equal to the best known value (see table in [5]).

$\square$

Construction of curves over $\mathbb{F}_{64}$

Example 6.5 Let $p = 2$ and $n = 6$. We are going to construct here, a curve over $\mathbb{F}_{64}$ with genus $g = 25$ and 335 rational points. This provides a (good) entry in the table [5]. In this construction we will take a polynomial $\ell(x)$ which is the product of 5 irreducible polynomials over $\mathbb{F}_2$ of degree 6.

Let $\ell(x) = x^{30}+x^{28}+x^{25}+x^{24}+x^{23}+x^{19}+x^{15}+x^{11}+x^7+x^6+x^5+x^2+1 = (x^6+x+1)(x^6+x^3+1)(x^6+x^4+x^2+x+1)(x^6+x^5+1)(x^6+x^5+x^4+x^2+1)$ and $f(x) = (x+1)^{30}$. We then obtain that $\mathcal{R}_\ell((x+1)^{30}) = x^4(x^2+x+1)^3(x^4+x^3+x^2+x+1)^4$. Then the Kummer cover over $\mathbb{F}_{64}$ given by the equation

$$y^9 = \frac{(x+1)^{30}}{x^4(x^2+x+1)^3(x^4+x^3+x^2+x+1)^4},$$

has genus $g = 25$, in fact we have 6 totally ramified points corresponding to $x = 0$, $x = \infty$ and the zeros of $x^4+x^3+x^2+x+1$, and 9 points with ramification index $e = 3$ (they are rational points and lies above the ones with $x^3+1=0$) . Now for the number of rational points, we have 9×30 guaranteed by Proposition 3.1. The Equation (2) in Remark 3.2 has $\kappa = 6$ solutions, therefore we obtain 54 extra rational points. This gives $\#\mathcal{C}(\mathbb{F}_{64}) = 9 \times 36 + 9 + 2 = 335$ rational points. $\square$

Example 6.6 In this example we will construct two maximal curves $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_{64}$ with genus $g(\mathcal{C}_1) = 3$ and $g(\mathcal{C}_2) = 12$. Their equations are obtained using a polynomial $\ell(x)$ of degree 24 which is the product of 4 irreducible polynomials over $\mathbb{F}_2$ of degree 6.

Let $\ell(x) = x^{24}+x^{23}+x^{22}+x^{19}+x^{18}+x^{14}+x^{12}+x^{10}+x^6+x^5+x^2+x+1$, and $f(x) = (x+1)^{30}$. (Observe that $\ell(x)$ is the product of four irreducible polynomials over $\mathbb{F}_2$, namely $(x^6+x^4+x^3+x+1)$, $(x^6+x^5+x^2+x+1)$, $(x^6+x^5+x^3+x^2+1)$ and $(x^6+x^5+x^4+x+1)$).

Now, we have that

$$f(x) = (x+1)^{30} = x(x+1)^2(x^3+x+1)\ell(x) + (x+1)^2(x^3+x+1)^7. \quad (7)$$

Therefore $\mathcal{R}_\ell(f(x)) = (x+1)^2(x^3+x+1)^7$ and since the rational function $u(x) := \frac{f(x)}{\mathcal{R}_\ell(f(x))}$ is a 7-th power in $\mathbb{F}_{64}(x)$, then we can consider the curve $\mathcal{C}$ defined by the equation

$$y^{\frac{r}{d}} = u(x)^{\frac{1}{d}} = \left(\frac{(x+1)^{28}}{(x^3+x+1)^7}\right)^{\frac{1}{d}}$$

where r is a divisor of 63 and $d = \gcd(7, r)$.

In this case, we have 5 totally ramified points, this gives $g(\mathcal{C}) = \frac{3(r-d)}{2d}$, and $\#\mathcal{C}(\mathbb{F}_{64}) \geq \frac{r}{d}24 + 5$, The number κ of solutions of Equation (2) in Remark 3.2 is given in the following table

r	g	κ	$N(\mathbb{F}_{64})$
21	3	12	113
63	12	4	257

Observe that in case $r = 63$ the value $\kappa = 4$ is given by the Equation 7.

□

7 The particular case $\mathcal{R}_\ell(f(x)) = 1$

In this section we will consider polynomials $g(x)$ and $\ell(x)$ in $\mathbb{F}_q[x]$ such that $\gcd(g(x), \ell(x)) = 1$. This property implies that there exist polynomials $h(x)$ and $v(x)$ in $\mathbb{F}_q[x]$ such that

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

This means that $\mathcal{R}_\ell(f(x)) = 1$ with $f(x) = g(x)v(x)$. Furthermore this equality implies that, for all $\alpha \in \mathbb{F}_q \cap \mathcal{V}_\ell$, we have $g(\alpha)v(\alpha) = 1$ and hence we hope that the curve $\mathcal{C}$ over $\mathbb{F}_q$ defined by the Kummer equation

$$y^r = f(x) := g(x)v(x)\,, \text{ with } r \text{ a divisor of } q-1, \tag{8}$$

has many rational points. In fact we have that $\#\mathcal{C}(\mathbb{F}_q) \geq r\lambda$ where

$$\lambda = \#\{\alpha \in \mathbb{F}_q \text{ such that } \ell(\alpha) = 0\}.$$

We are interested in the case when the polynomial $f(x)$ has many multiple roots. This will ensure a lower genus for the curve given by an equation as in (8) above.

Examples

In the following examples we will construct goods curves over $\mathbb{F}_{q^m}$, by taking $\ell(x)$ as a product of irreducible polynomials over $\mathbb{F}_q$. Note that an irreducible polynomial of degree m over $\mathbb{F}_q$ is separable and has all roots in $\mathbb{F}_{q^m}$.

Example 7.1 In this example we will construct a curve $\mathcal{C}$ over $\mathbb{F}_{25}$ with genus $g(\mathcal{C}) = 7$ and $\#\mathcal{C}(\mathbb{F}_{25}) = 84$. This curve provides an entry in [14] better than the one obtained in the Example 5.2.2.

Let $\ell(x) = (x^2+2)(x^2+3)(x^2+2x+3)(x^2+3x+3) = x^8+2x^6+2x^2+4$ and $g(x) = (x-1)^8$, then $h(x) = 3(x+1)(x+3)^2(x^4+2x^2+3)$ and $v(x) = 3x^3(x+2)^3(x-1)$.

Observe that the polynomial $f(x) = g(x)v(x) = 3x^3(x+2)^3(x-1)^9$ is a cube in $\mathbb{F}_{25}[x]$ (the equation $x^3 - 3$ has its roots in $\mathbb{F}_{25}$).

Hence the equation $y^{24} = g(x)v(x)$ is not irreducible and taking the third root of it, we consider the curve $\mathcal{C}$ over $\mathbb{F}_{25}$ defined by the Kummer equation

$$y^8 = \omega x(x+2)(x-1)^3, \text{ with } \omega^3 = 3.$$

Here one has 4 totally ramified points, and hence $g(\mathcal{C}) = 7$. The number of rational points satisfies $\#\mathcal{C}(\mathbb{F}_{25}) \geq 8 \times 8 + 4 = 68$, where the number 4 comes from the 4 totally ramified points and the number $64 = 8 \times 8$ comes from the roots of $\ell(x)$. In this case the number $\kappa = 2$ and hence we have 16 extra rational points (see Remark 3.2). In fact $\kappa = 2$ corespond to the two roots $x = -1$ and $x = 2$ of the polynomial $h(x)$ above. $\square$

In the following three examples we will construct curves over $\mathbb{F}_{27}$, which provide new entries in [5]. The polynomials $\ell(x)$ used to construct these curves are products of irreducible polynomials over $\mathbb{F}_3$ of degree 3 and hence $\ell(x)$ has its roots in $\mathbb{F}_{27}$.

We will use the following irreducible polynomials over $\mathbb{F}_3$:

$$\begin{aligned}
\ell_1(x) &= x^3 + 2x + 1 \\
\ell_2(x) &= x^3 + 2x + 2 \\
\ell_3(x) &= x^3 + x^2 + x + 2 \\
\ell_4(x) &= x^3 + x^2 + 2x + 1 \\
\ell_5(x) &= x^3 + 2x^2 + 1 \\
\ell_6(x) &= x^3 + 2x^2 + x + 1 \\
\ell_7(x) &= x^3 + 2x^2 + 2x + 2.
\end{aligned}$$

Example 7.2 Let $\ell(x) = \ell_6(x)\ell_7(x) = x^6 + x^5 + x^4 - x^2 + x - 1$ and $g(x) = (x-1)^6$, then $v(x) = -(x-1)(x^3 + x^2 - 1)$ and $h(x) = 2(x+1)^2(x^2+1)^2$. We obtain the following equality

$$-(x-1)^7(x^3 + x^2 - 1) = 2(x+1)^2(x^2+1)^2\ell(x) + 1$$

Then, curve $\mathcal{C}$ over $\mathbb{F}_{27}$ defined by the equation

$$y^{13} = f(x) := -(x-1)^7(x^3 + x^2 - 1),$$

has genus $g(\mathcal{C}) = 18$ and $\#\mathcal{C}(F_{27}) = 148$. In fact we have 5 totally ramified points, this gives $2g(\mathcal{C}) - 2 = 13(-2) + 60 = 34$.

For the number of rational points, observe that the greatest common divisor of the polynomials $f(x)^2 - 1$ and $x^{27} - x$ is the polynomial $x^{11} - x^8 - x^5 + x^4 - x^3 + x^2 - x = x(x+1)\ell_4(x)\ell(x)$. Then we obtain $\#\mathcal{C}(\mathbb{F}_{27}) = 13 \times 11 + 5 = 148$ $\square$

Example 7.3 Taking $\ell(x) = \ell_3(x)\ell_4(x)\ell_5(x)\ell_7(x) = x^{12} - x^9 + x^8 + x^7 + x^6 + x^5 + x^4 - x^2 - x + 1$ and $g(x) = (x^2 + x - 1)^3$, we obtain $v(x) = (x^2 + x - 1)(x^4 - x^3 - x^2 + x - 1)$ and $h(x) = 1$.

Now, we consider the curve $\mathcal{C}$ over $\mathbb{F}_{27}$ defined by the Kummer equation

$$y^{13} = f(x) = (x^2 + x - 1)^4(x^4 - x^3 - x^2 + x - 1).$$

In this case we have 7 totally ramified points and this gives $g(\mathcal{C}) = 30$. The number of rational points is at least $13 \times 12 + 1 = 157$, the number one comes from the point corresponding to $x = \infty$. Now, to determine the exact number of rational points, we have that Equation (2) in Remark 3.2 has 3 solutions outside of $\mathcal{V}_\ell$, (equivalently, the greatest common divisor of $f^2(x) - 1$ and $x^{27} - x$ is the polynomial $(x^3 - x)\ell(x)$). Then we have $13 \times 3 = 39$ extra rational points. This gives $\#\mathcal{C}(\mathbb{F}_{27}) = 157 + 39 = 196$. $\square$

Example 7.4 In this example we are going to construct a curve $\mathcal{C}$ over $\mathbb{F}_{27}$ with genus $g(\mathcal{C}) = 44$ and $\#\mathcal{C}(\mathbb{F}_{27}) = 278$.

Let $\ell(x) = \ell_1(x)\ell_2(x)\ell_5(x) = x^9 - x^8 + x^7 + x^5 - x^3 - x^2 - 1$ and $g(x) = x^4(x+1)$. After some computations we obtain that $v(x) = x^3(x+1)^2(x^3 + x^2 + x - 1)$ and $h(x) = (x+2)\ell_2(x)$. Then we define the curve $\mathcal{C}$ over $\mathbb{F}_{27}$ by the equation

$$y^{26} = f(x) := x^7(x+1)^3(x^3 + x^2 + x - 1).$$

Here we have 5 totally ramified points, and the 13 points above $x = \infty$ have ramification index $e = 2$. This gives $2g(\mathcal{C}) - 2 = 26(-2) + 25 \times 5 + 13 = 86$ and hence $g(\mathcal{C}) = 44$.

Now, for the rational points, observe that $2(x+2)\ell_2(x)\ell(x) + g(x)v(x) = 1$. Since $r = 26$, the only solution of the Equation (2) in Remark 3.2 is the one coming from the root $x = -2$ of the polynomial $h(x)$ above (observe that $\ell_2(x)$ is a factor of $\ell(x)$) and hence $\kappa = 1$. This gives $\#\mathcal{C}(\mathbb{F}_{27}) \geq 260 + 5$. Observing that the points corresponding to $x = \infty$ are rational, then we have 265+13=278 rational points. $\square$

In the following examples we will construct curves $\mathcal{C}$ over the finite field $\mathbb{F}_{64}$. The values for the genus $g(\mathcal{C})$ and for the number of rational points $\#\mathcal{C}(\mathbb{F}_{64})$ obtained here for these curves coincide with the best values known in tables (see [5]). Some of these curves attain the Hasse-Weil upper bound; i¿e, some of them are maximal curves.

For the construction of the polynomial $\ell(x)$ we will use the following irreducible polynomials over $\mathbb{F}_2$ which have their roots in $\mathbb{F}_{64}$.

$$\begin{aligned}
\ell_1(x) &= x^3 + x + 1\\
\ell_2(x) &= x^3 + x^2 + 1\\
\ell_3(x) &= x^6 + x + 1\\
\ell_4(x) &= x^6 + x^3 + 1\\
\ell_5(x) &= x^6 + x^4 + x^2 + x + 1\\
\ell_6(x) &= x^6 + x^4 + x^3 + x + 1\\
\ell_7(x) &= x^6 + x^5 + x^2 + x + 1\\
\ell_8(x) &= x^6 + x^5 + x^3 + x^2 + 1\\
\ell_9(x) &= x^6 + x^5 + x^4 + x + 1\\
\ell_{10}(x) &= x^6 + x^5 + x^4 + x^2 + 1.
\end{aligned}$$

Example 7.5 Let $\ell(x) = \ell_1(x)\ell_7(x) = x^9 + x^8 + x^7 + x^4 + 1$ and $g(x) = (x+1)^3(x^2+x+1)^4$. Then we have that

$$g(x)(x^2 + x + 1)^4 = (x^9 + x^6 + x^5 + x^4 + x^2 + x + 1)\ell(x) + 1.$$

Therefore the curve $\mathcal{C}$ over $\mathbb{F}_{64}$ defined by the Kummer equation

$$y^3 = (x+1)^3(x^2+x+1)^8 \quad \text{(or by} \quad z^3 = (x^2+x+1)),$$

has genus $g(\mathcal{C}) = 1$ and $\#\mathcal{C}(\mathbb{F}_{64}) = 81$, i.e., this curve attains the Hasse-Weil upper bound. In fact, we have three totally ramified points and this gives $2g(\mathcal{C}) - 2 = -2(3) + 6 = 0$, hence $g(\mathcal{C}) = 1$.

To compute the number of rational points, observe that $\kappa = 16$ (equivalently, the greatest common divisor of $(x^2+x+1)^{21}+1$ and $x^{64}+x$ is the polynomial $x(x+1)(x^6+x^5+1)\ell_2(x)\ell_8(x)\ell(x))$, therefore $\#\mathcal{C}(\mathbb{F}_{64}) = 3\times(9+17)+3 = 81$. $\square$

Example 7.6 Taking $\ell(x) = \ell_6(x)\ell_7(x)\ell_8(x) = x^{18}+x^8+x^7+x^6+x^3+x^2+1$ and $g(x) = x^9(x+1)^{10}$ we obtain that $v(x) = (x+1)^5(x^3+x+1)^3$. Observe that the polynomial $g(x)v(x)$ is a cube in $\mathbb{F}_{64}[x]$, therefore we have to consider the equation defining $\mathcal{C}$ as follows

$$y^{\frac{r}{d}} = (f(x))^{\frac{1}{d}}, \qquad \text{with } r \text{ a divisor of 63 and } d = \gcd(r, 3).$$

Then for $r = 9$, we consider the curve $\mathcal{C}$ over the finite field $\mathbb{F}_{64}$ defined by

$$y^3 = x^3(x+1)^5(x^3+x+1). \qquad \text{(or by} \quad z^3 = \frac{x^3+x+1}{x+1}.)$$

In this case we have 5 totally ramified points (corresponding to $x = 1$, $x = \infty$ and to $x = \gamma_i$ with ${\gamma_i}^3 + \gamma_i + 1 = 0$). This gives $g(\mathcal{C}) = 3$.

For the rational points, observe that the ramified points are rational and that Equation (2) in Remark (3.2) has 17 solutions (equivalently, there exists 18 elements $\alpha \in \mathbb{F}_{64}$ such that $\frac{\alpha^3+\alpha+1}{\alpha+1}$ is a cube in $\mathbb{F}_{64}$ with $\ell(\alpha) \neq 0$ namely, the roots of the polynomial $x(x^2+x+1)\ell_2(x)\ell_4(x)\ell_9(x)$). Therefore $\#\mathcal{C}(\mathbb{F}_{64}) = 3 \times (18 + 18) + 5 = 113$. $\square$

Example 7.7 We are now going to construct here a maximal curve over the finite field $\mathbb{F}_{64}$ with genus $g(\mathcal{C}) = 4$.

If $\ell(x) = \ell_1(x)\ell_2(x)\ell_8(x) = x^{12}+x^9+x^6+x^4+x^3+x+1$ and $g(x) = (x^2+x+1)^9$, then $v(x) = (x^2+x+1)^5$ and $h(x) = (x^2+x)\ell_1(x)\ell_2(x)\ell_8(x)$. The curve $\mathcal{C}$ given by the equation

$$y^9 = (x^2+x+1)^{14} \qquad \text{(or by} \quad z^9 = (x^2+x+1)^5),$$

has genus $g(\mathcal{C}) = 4$.

To compute the number of rational points observe that the elements α of $\mathbb{F}_{64}$ such that $\alpha^2 + \alpha + 1$ is a 9-th power in $\mathbb{F}_{64}$ are the roots of the polynomial $x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 + x = (x^2+x)\ell(x)$ (i.e, this last polynomial is the greatest common divisor of $(x^2+x+1)^7 + 1$ and $x^{64} + x$). Hence $\#\mathcal{C}(\mathbb{F}_{64}) = 9 \times 14 + 3 = 129$, since the 3 ramified points are also rational. $\square$

Example 7.8 The polynomial$\ell(x) = \ell_3(x)\ell_9(x) = x^{12}+x^{11}+x^{10}+x^6+x^4+x^2+1$ has no common roots with the polynomial $g(x) = (x^3+x)^6$. Then we get the following equality (thru computer search)

$$g(x)v(x) = \ell(x)h(x) + 1,$$

with $v(x) = x^4(x+1)^3(x^2+x+1)$ and $h(x)$ a polynomial of degree 15 without roots in $\mathbb{F}_{64}$. Now, the curve $\mathcal{C}$ over $\mathbb{F}_{64}$ given by the equation

$$y^9 = x^{10}(x+1)^{15}(x^2+x+1), \text{ or by } z^9 = \frac{x(x^2+x+1)}{(x+1)^3},$$

has genus $g(\mathcal{C}) = 7$. In fact we have 3 totally ramified points (and they are rational) and three points (corresponding to $x = 1$) with ramification index $e = 3$; the 9 points above $x = \infty$ are unramified. This gives $2g(\mathcal{C}) - 2 = 9 \times (-2) + 3 \times 8 + 3 \times 2 = 12$ and hence $g(\mathcal{C}) = 7$.

Besides the roots of $\ell(x)$ we have 6 elements $\alpha \in \mathbb{F}_{64}$ (computer search) such that $\frac{\alpha(\alpha^2+\alpha+1)}{(\alpha+1)^3}$ is a 9-th power in $\mathbb{F}_{64}$. On the other hand, it is easy to see that the 3 points above $x = 1$ and the 9 points above $x = \infty$ are rational. Therefore the number of rational points satisfies $\#\mathcal{C}(\mathbb{F}_{64}) = 9 \times (12+6) + 9 + 3 + 3 = 177$. $\square$

Example 7.9 In this example we will construct a curve $\mathcal{C}$ over $\mathbb{F}_{64}$ with $g(\mathcal{C}) = 10$ and with 225 rational points. It is a maximal curve.

Let $\ell(x) = \ell_3(x)\ell_6(x) = x^{12}+x^{10}+x^9+x^5+x^3+x^2+1$ and choose $g(x) = (x^4+x)^6$. In this case we have that $v(x) = x^2(x^2+x+1)^2$ and $h(x) = \ell_2^2(x)\ell(x)$. Therefore the curve $\mathcal{C}$ defined by equation

$$y^9 = f(x) = x^8(x+1)^6(x^2+x+1)^8 \text{ (or by } z^9 = \frac{(x+1)^6}{x(x^2+x+1)}),$$

has three totally ramified points (and they are rational) and six points (corresponding to $x = 1$ and to $x = \infty$) with ramification index $e = 3$. This gives $g(\mathcal{C}) = 10$.

The number of rationalpoints follows from the fact that the the greatest common divisor of the polynomials $f(x)^7+1$ and $x^{64}+x$ is the polynomial of degree 24, $\ell_1(x)\ell_2(x)\ell_9(x)\ell(x)$ and that the 6 points above $x=1$ and $x=\infty$ are rational. Hence we have $9 \times 24 + 6 + 3 = 225$ rational points. $\square$

Example 7.10 The curve $\mathcal{C}$ over $\mathbb{F}_{64}$ defined by the Kummer equation

$$y^9 = x^5(x+1)^{10}(x^3+x+1) \quad (\text{or by } z^9 = x^5(x+1)(x^3+x+1)),$$

has genus $g(\mathcal{C}) = 12$ and has 257 rational points, i.e., $\#\mathcal{C}(\mathbb{F}_{64})$ attains the Hasse-Weil upper bound.

We observe that the equation defining this curve $\mathcal{C}$ was obtained by taking $\ell(x) = \ell_4(x)\ell_8(x)\ell_{10}(x) = x^{18}+x^{15}+x^{14}+x^{13}+x^{10}+x^7+x^6+x^5+1$ and $g(x) = (x+1)^{10}$. Then we have that $v(x) = x^5(x^3+x+1)$ and $h(x) = 1$.

We have 5 totally ramified points, and hence by Hurwitz formula $2g(\mathcal{C})-2 = -18+40 = 22$. This shows that $g(\mathcal{C}) = 12$.

It is easy to see that the nine points corresponding to $x=\infty$ are rational. Also the ramification points corresponding to $x=0$, $x=1$ and to the three roots of x^3+x+1 (in fact, this irreducible polynomial has its roots in $\mathbb{F}_8$) are rational. Now, Equation (2) in Remark 3.2 has 9 solutions namely the roots of the polynomial $\ell_2(x)(x^6+x^5+1)$, and hence we have $\#\mathcal{C}(\mathbb{F}_{64}) = 9 \times (18+9)+9+5 = 257$. $\square$

Example 7.11 We are going to construct a maximal curve $\mathcal{C}$ over $\mathbb{F}_{64}$ with genus $g(\mathcal{C}) = 28$.

If $\ell(x) = \ell_5(x)\ell_9(x)\ell_{10}(x) = x^{18}+x^{13}+x^{10}+x^8+x^7+x^6+x^5+x^4+x^3+x^2+1$ and $g(x) = (x+1)^{10}$ we obtain $v(x) = x(x+1)^8(x^2+x+1)(x^6+x^4+x^3+x+1)$ and $h(x) = \ell_1(x)\ell_8(x)$. We then consider the curve $\mathcal{C}$ over $\mathbb{F}_{64}$defined by the equation

$$y^9 = x(x+1)^{18}(x^2+x+1)(x^6+x^4+x^3+x+1).$$

In this case there are 9 totally ramified points, therefore we have $2g(\mathcal{C})-2 = -18+72 = 54$.

The roots of the irreducible (over $\mathbb{F}_2$) polynomials $x^6+x^4+x^3+x+1$ and x^2+x+1 belong to $\mathbb{F}_{64}$, hence the corresponding points on $\mathcal{C}$ are rational. Also the 18 points corresponding to $x=1$ and $x=\infty$ are rational. The Equation (2) in Remark 3.2 has 36 solutions, therefore we have $\#\mathcal{C}(\mathbb{F}_{64}) = 9 \times (18+36)+9+9+6+3 = 513$.

Observe that taking $z = \frac{y}{(x+1)^2}$, the equation defining the curve $\mathcal{C}$ can be written as

$$z^9 = x(x^2+x+1)(x^6+x^4+x^3+x+1).$$

$\square$

We end this series of examples of curves over $\mathbb{F}_{64}$ constructing a curve with genus 40 and 489 rational points, again this is the best value know for $(g,q) = (40,64)$ in tables (see [5]). This record was obtained before by F. Ozbudak and H. Stichtenoth (see [10]) using configurations of hyperplanes over finite fields.

Example 7.12 In this example we take $\ell(x) = \ell_5(x)\ell_9(x) = x^{12}+x^{11}+x^9+x^7+x^5+x^3+1$ and $g(x) = (x^3+x)^6$, then we obtain that $v(x) = x^7(x+1)(x^3+x+1)$. Now we consider the curve $\mathcal{C}$ over $\mathbb{F}_{64}$ defined by the Kummer equation

$$y^{21} = x^{13}(x+1)^{13}(x^3+x+1).$$

We see that there are 6 ramification points and they are totally ramified, this gives $2g(\mathcal{C})-2 = -42+120 = 78$. Hence $g(\mathcal{C}) = 40$.

For the rational points, Equation (2) in Remark 3.2 has 11 solutions and the points on $\mathcal{C}$ corresponding to the ramification points are rational. This then gives $\#\mathcal{C}(\mathbb{F}_{64}) = 21 \times (12+11)+6 = 489$. $\square$

In the next four examples we take $\ell(x)$ as a product of two irreducible polynomials of degree 4 over $\mathbb{F}_3$, leading to curves with many rational points over $\mathbb{F}_{81}$. We will use the following polynomials.

$$
\begin{aligned}
\ell_1(x) &= x^4 + x + 2 \\
\ell_2(x) &= x^4 + x^2 + x + 1 \\
\ell_3(x) &= x^4 + x^2 + 2x + 1 \\
\ell_4(x) &= x^4 + x^3 + x^2 + 1 \\
\ell_5(x) &= x^4 + 2x^3 + 2 \\
\ell_6(x) &= x^4 + 2x^3 + x + 1.
\end{aligned}
$$

Example 7.13 We are going to construct here a curve $\mathcal{C}$ over $\mathbb{F}_{81}$ with genus $g(\mathcal{C}) = 11$ and with 220 rational points. This gives a new entry in the tables (See [5]).

Let $\ell(x) = \ell_1(x)\ell_2(x) = x^8 + x^6 - x^5 + x^3 - 1$ and $g(x) = x(x-1)^4$. Then we have $g(x)x^4(x^2+x-1) = \ell(x)(x+1)^3+1$. Consider the curve $\mathcal{C}$ over $\mathbb{F}_{81}$ given by

$$y^{10} = x^5(x-1)^4(x^2+x-1).$$

In this case we have five points with ramification index $e = 2$, namely the five points corresponding to $x = 0$; two points (corresponding to $x = 1$) with ramification index $e = 5$ and three totally ramified points. This gives $2g(\mathcal{C}) - 2 = 10(-2) + 5 + 8 + 27 = 20$ and hence $g(\mathcal{C}) = 11$. It is easy to see that all the ramified points above are rational. Now, the Equation (2) in Remark 3.2 has 13 solutions outside of $\mathcal{V}_\ell$, namely, the roots of the polynomial $(x+1)(x^2+1)(x^2-x-1)(x^4+x^3-1)(x^4-x^3+x^2+1)$. Therefore we have $\#\mathcal{C}(\mathbb{F}_{81}) = 10 \times (8+13) + 5 + 2 + 3 = 220$. □

Example 7.14 In this example we are going to construct a curve $\mathcal{C}$ over $\mathbb{F}_{81}$ with genus $g(\mathcal{C}) = 13$ and 243 rational points, this provides a new record in [5] for $(q, g) = (81, 13)$. The former best known value was 224 rational points.

Let $\ell(x) = \ell_3(x)\ell_4(x) = x^8 + x^7 - x^6 - x^4 - x^2 - x + 1$ and $g(x) = (x-1)^3$. In this case we have $v(x) = (x-1)(x+1)^3(x^3 - x^2 + x + 1)$ and $h(x) = x^2$. Now, consider the curve $\mathcal{C}$ over $\mathbb{F}_{81}$ defined by the equation

$$y^{10} = f(x) := (x-1)^4(x+1)^3(x^3 - x^2 + x + 1).$$

In this case we have that the two points corresponding to $x = 1$ have ramification index $e = 5$, the points above $x = \infty$ are unramified, and the points corresponding to $x = -1$ and to the roots of the polynomial $x^3 - x^2 + x + 1$ are totally ramified. This gives $2g(\mathcal{C}) - 2 = 10(-2) + 9 \times 4 + 8 = 24$ and hence $g(\mathcal{C}) = 13$.

To determine the number of rational points, a computer search shows that there are 23 elements α in $\mathbb{F}_{81}^*$ such that $f(\alpha)$ is a 10-th power in $\mathbb{F}_{81}$, namely the roots of the polynomial $x^{23} + x^{21} - x^{18} + x^{15} - x^{14} + x^{12} + x^{10} - x^9 - x^8 + x^7 - x^5 + x^4 - x^2 + x$ (i.e; this last polynomial is the greatest common divisor of $f^8(x) - 1$ and $x^{81} - x$). It is easy to see that the points corresponding to $x = 1$, $x = -1$ and $x = \infty$ are rational. Then we have $\#\mathcal{C}(\mathbb{F}_{81}) = 10 \times 23 + 10 + 2 + 1 = 243$. $\square$

Example 7.15 The curve $\mathcal{C}$ over $\mathbb{F}_{81}$, defined by the Kummer equation

$$y^{10} = f(x) = -x^3(x-1)^6(x^3 + x^2 + x - 1)^2$$

has genus $g(\mathcal{C}) = 14$ and $\#\mathcal{C}(\mathbb{F}_{81}) = 278$. This is a new entry in [5].

In fact, if we take $\ell(x) = \ell_4(x)\ell_6(x) = x^8 + x^3 + x^2 + x + 1$, and $g(x) = x^3(x-1)^5$, we obtain $g(x)v(x) = h(x)\ell(x) + 1$, with $v(x) = -(x-1)(x^3 + x^2 + x - 1)^2$ and with $h(x) = -(x+1)(x^2+1)(x^4 + x^3 + x^2 + x + 1)$

Therefore we get the equation above defining the curve $\mathcal{C}$.

In this case we have that the five points corresponding to $x = \infty$ have ramification index $e = 2$ and that there are 8 points with ramification index $e = 5$, namely the points corresponding to $x = 1$ and to $x = \zeta$ with $\zeta^3 +$

$\zeta^2+\zeta-1=0$. The point $x=0$ is totally ramified, this gives $2g(\mathcal{C})-2=10(-2)+8\times 4+5+9=26$.

Now, for the rational points, it is easy to see that the points corresponding to $x=0$, $x=1$ and $x=\infty$ are rational. On the other hand, the greatest common divisor of the polynomials $f(x)^8-1$ and $x^{81}-x$ is the polynomial $x^{27}+x^{24}-x^{23}-x^{21}+x^{19}+x^{18}+x^{17}-x^{16}-x^{11}+x^{10}+x^9+x^8-x^6-x^4+x^3+1$. Therefore the number of rational points is $\#\mathcal{C}(\mathbb{F}_{81})=10\times 27+8=278$. $\square$

Example 7.16 In this example we will construct a curve $\mathcal{C}$ over $\mathbb{F}_{81}$, with genus $g(\mathcal{C})=25$ and with $\#\mathcal{C}(\mathbb{F}_{81})=392$. This provides a new entry in [5].

Let $\ell(x)=\ell_4(x)\ell_5(x)=x^8-x^5+x^3-x^2-1$ and $g(x)=x(x-1)^7$. In this case we obtain $v(x)=-x^3(x-1)^2(x^2-x-1)$ and $h(x)=x^7-x^6-x^5+x^4-x^3+x^2-1$. We consider then the curve $\mathcal{C}$ over $\mathbb{F}_{81}$ defined by the Kummer equation

$$y^{20}=f(x):=-x^4(x-1)^9(x^2-x-1).$$

One has 3 totally ramified points (corresponding to $x=1$ and to the roots of x^2-x-1), and 4 points corresponding to $x=0$ that have ramification index $e=5$. The points corresponding to $x=\infty$ have ramification index $e=4$. Then we have $2g(\mathcal{C})-2=20(-2)+3\times 19+5\times 3+4\times 4=48$.

Now, for the number of rational points, observe first that the 12 ramified points above are rational. The greatest common divisor of the polynomials $f(x)^4-1$ and $x^{81}-x$ is the polynomial $x^{19}+x^{17}-x^{15}+x^{13}-x^{12}+x^{11}+x^9+x^8-x^7+x^6-x^5-x^4+x^3-x^2-1$. This gives $\#\mathcal{C}(\mathbb{F}_{81})=20\times 19+12=392$. $\square$

8 Double Kummer Covers

Let $K:=\mathbb{F}_q$ be a finite field with $q=p^n$ elements. In this section we will consider algebraic function fields of the type $E=K(x,y_1,y_2)$, where for $i=1,2$

$$y_i^{r_i} = \mu_i(x) = \frac{f_i(x)}{\mathcal{R}_{\ell_i}(f_i(x))} \in K(x)$$

with $f_i(x)$ and $\ell_i(x)$ polynomials and r_i a divisor of $q-1$. Also we suppose that $\mu_i(x)$ is not the d-th power of an element $\theta(x) \in \bar{\mathbb{F}}_q(x)$ with d a divisor of $q-1$ and $\mu_1(x) \neq \mu_2(x)$.

Theorem 8.2 gives a formula to compute the genus is this type of extensions, for this, we will use the follow result:

Theorem 8.1 (Abhyankar's Lemma) *Let F'/F be a finite, separable extension of function fields. Suppose that $F' = F_1F_2$ is the compositum of two intermediate fields, $F \subseteq F_1, F_2 \subseteq F'$. Let $P' \in \mathbb{P}_{F'}$ be an extension of $P \in \mathbb{P}_F$, and set $P_i := P' \cap F_i$ for $i = 1, 2$. Assume that at least one of the extensions $P_1|P$ or $P_2|P$ is tame (i.e., $e(P_i|P)$ is relative prime to the characteristic of F). Then*

$$e(P'|P) = lcm\{e(P_1|P), e(P_2|P)\}.$$

Proof: See [13], page 125. □

Now, we need to establish some notation:

Let $\bar{E} = \bar{K}(x, y_1, y_2)$ the constant field extension of E/K with $\bar{K}$. For $\alpha \in K$ (resp. $\alpha \in \bar{K}$), P_α is the zero of $x - \alpha$ in $K(x)$ (resp. in $\bar{K}(x)$), and P_∞ the pole of x in $K(x)$ (resp. in $\bar{K}(x)$).

If $(\mu_i) = \sum_{\alpha \in \bar{K} \cup \infty} a_\alpha^i P_\alpha$ is the divisor of $\mu_i(x)$ with distinct $P_\alpha \in \mathbf{P}^1(\bar{K})$. Then we will denote by (for each $i = 1, 2$)

$$T_i = \{\alpha \in \bar{K} \cup \{\infty\}; P_\alpha \in \text{supp } (\mu_i) \text{ ; gcd } (a_\alpha^i, r_i) = 1\}$$

$$U_i = \{\alpha \in \bar{K} \cup \{\infty\}; P_\alpha \in \text{supp } (\mu_i) \text{ ; gcd } (a_\alpha^i, r_i) = r_i\}$$

and by

$$V_i = \{\alpha \in \bar{K} \cup \{\infty\}; P_\alpha \in \text{supp } (\mu_i) \text{ ; gcd } (a_\alpha^i, r_i) = d \text{ with} 1 < d < r_i\}$$

We will assume that $[E : K(x)] = r_1 r_2$ (for example, this is the case if $T_1 \neq T_2$) and we will also assume that the sets V_1 and V_2 are empty; i.e., that we have only totally ramified places for both extensions $E_1/K(x)$ and $E_2/K(x)$. Now, if we denote by $\tau_i := \#T_i$, then we have $2g_i = (\tau_i - 2)(r_i - 1)$ for $i = 1, 2$.

Theorem 8.2 *Notation as above. Then the genus of E/K is*

$$g(E/K) = (r_1 - 1)(r_2 - 1) + r_2 g_1 + r_1 g_2 - \frac{\tau}{2}(r_1 r_2 - r_1 - r_2 + \delta)$$

where g_i is the genus of $K(x, y_i)/K$, $\tau = \#(T_1 \cap T_2)$ and $\delta = gcd(r_1, r_2)$. Particularly if $r_1 = r_2 = r$ then $g(E/K) = (r-1)^2 - \frac{\tau}{2} r(r-1) + r(g_1 + g_2)$

Proof: For $\alpha \in T_i \backslash (T_1 \cap T_2)$ the place P_α is totally ramified in the extension $\bar{K}(x, y_i)/\bar{K}(x)$. By Theorem 5.1, the ramification index $e(P_\alpha)$ in the compositum $\bar{E}/\bar{K}(x)$ is r_i, since the ramification is tame. For $\alpha \in (T_1 \cap T_2)$ the ramification index $e(P_\alpha)$ in the compositum $\bar{E}/\bar{K}(x)$ is $e(P_\alpha) = \dfrac{r_1 r_2}{\delta}$.

Then we have $\tau_i - \tau$ points with ramification index and $e(P_\alpha) = r_i$ for $i = 1, 2$ and τ points with ramification index and $e(P_\alpha) = \dfrac{r_1 r_2}{\delta}$.

Then the Different $\mathcal{D}(\bar{E}/\bar{K}(x))$ has degree:

$$(\tau_1 - \tau)(r_1 - 1)r_2 + (\tau_2 - \tau)(r_2 - 1)r_1 + \tau(r_1 r_2 - \delta)$$

On the other hand

$$
\begin{aligned}
(\tau_1-\tau)(r_1-1)r_2 &= [(\tau_1(r_1-1)-\tau(r_1-1)]r_2 \\
&= [(\tau_1-2)(r_1-1)+2(r_1-1)-\tau(r_1-1)]r_2 \\
&= 2g_1r_2-(\tau-2)(r_1-1)r_2
\end{aligned}
$$

and $(\tau_2-\tau)(r_2-1)r_1 = 2g_2r_1-(\tau-2)(r_2-1)r_1$.

Therefore we can write the degree of $\mathcal{D}(\bar{E}/\bar{K}(x))$ as

$$2(2r_1r_2-r_1-r_2)+2g_1r_2+2g_2r_1-\tau(r_1r_2-r_1-r_2+\delta),$$

now the formula for the genus follows from Hurwitz formula. $\square$

Remark 8.1 (i) With notations as Theorem 8.2, Castelnuovo's inequality for the composite E of two function fields F_1 and F_2 says. (See [13], Theo III.10.3):

$$g \leq (r_1-1)(r_2-1)+r_2g_1+r_1g_2.$$

So, the term $\frac{\tau}{2}(r_1r_2-r_1-r_2+\delta)$ in the statement of Theorem 8.2 represents the correction factor needed to turn the Castelnuovo's inequality into an equality.

ii) Suppose that $\ell_1(x), \ell_2(x) \in \mathbb{F}_q[x]$, and (for $i=1,2$) $E_i := K(x, y_i)$ is given by the equation

$$y_i^{r_i} = \frac{f_i(x)}{\mathcal{R}_{\ell_i}(f_i(x))},$$

with r_i a divisor of $q-1$ and $f_i(x) \in \mathbb{F}_q[x]$. Then, if the degree of the compositum E satisfies $[E : K(x)] = r_1r_2$ and we denote by $\mathcal{C}$ the algebraic curve having E as its field of rational functions, the set of $\mathbb{F}_q$-rational points satisfies:

$$\#\mathcal{C}(\mathbb{F}_q) \geq r_1r_2\lambda$$

where, $\lambda := \#\{\alpha \in \mathcal{V}_d \cap \mathbb{F}_q; f_i(\alpha) \neq 0\}$ with $d(x) = gcd(\ell_1(x), \ell_2(x))$.

Example 8.1 We are going to construct here a curve $\mathcal{C}$ over $\mathbb{F}_{16}$ with$g(\mathcal{C}) = 34$ and 183 rational points. This provides a new record in the table [5]. This curve is the fiber product over the x-line of the curves $\mathcal{C}_1$ and $\mathcal{C}_2$ which correspond to two Kummer covers of $\mathbb{F}_{16}(x)$.

Let $q = 16$. Let $\ell_1(x) = \ell_2(x) = \frac{x^{15}+1}{x^3+1} = x^{12}+x^9+x^6+x^3+1$, $f_1(x) = (x^4+x)^3$ and $f_2(x) = (x^2+x+1)^3(x^3+x+1)^2$. Then $\mathcal{R}_{\ell_1}(f_1(x)) = 1$ (see Theorem 5.2.1) and after some computations we obtain $\mathcal{R}_{\ell_2}(f_2(x)) = x(x+1)(x^3+x^2+1)^3$.

We consider the Kummer covers $E_1 := \mathbb{F}_{16}(x, y_1)$ and $E_2 := \mathbb{F}_{16}(x, y_2)$, where

$$y_1^5 = (x^4+x)^3 \quad \text{and} \quad y_2^3 = \frac{(x^2+x+1)^3(x^3+x+1)^2}{x(x+1)(x^3+x^2+1)^3}.$$

Here $T_1 = \{0, 1, \theta_1, \theta_2, \infty\}$ with $\theta_i^2 + \theta_i + 1 = 0$, and $T_2 = \{0, 1, \zeta_1, \zeta_2, \zeta_3, \infty\}$ with $\zeta_i^3 + \zeta_i + 1 = 0$. So $\tau = 3$, $g_1 = 6$, $g_2 = 4$ and $\delta = 1$. Therefore the function field $E := E_1.E_2$ has genus 34 as follows from Theorem 8.2

For the rational places; first observe that the places corresponding to θ_i are not rational, in fact the equation

$$T^3 = \frac{(\theta_i^3 + \theta_i + 1)^2}{\theta_i(\theta_i + 1)} = \theta_i + 1$$

has not solution in $\mathbb{F}_{16}$. Now, since places corresponding to $x = 0$, $x = 1$ and $x = \infty$ are rational (they are totally ramified in E) then, by Remark 8.1 *ii*), then we have $\#\mathcal{C}(\mathbb{F}_{16}) = 3 \times 5 \times 12 + 3 = 183$. □

Example 8.2 In this example we will construct a curve $\mathcal{C}$ over $\mathbb{F}_{16}$ with genus $g(\mathcal{C}) = 19$ and $\#\mathcal{C}(\mathbb{F}_{16}) = 117$. This provides a new record in [5].

First, we take $g(x) = (x^3+x+1)^5(x^3+x^2+1)$ and $\ell(x) = x^2+x+1$. Then we have the equality

$$\ell(x)(x^4+x^3+x^2+x+1)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^5+x^2+x+1)+g(x)=1.$$

Now we consider the curve $\mathcal{C}_1$ defined by the Kummer equation

$$y_1^3=(x^3+x+1)^5(x^3+x^2+1). \tag{9}$$

In this case we have $g(\mathcal{C}_1)=4$. For the rational points, we see that besides of the roots of the polynomial $\ell(x)(x^4+x^3+x^2+x+1)$ there are eight elements $\alpha\in\mathbb{F}_{16}$ such that $g(\alpha)$ are cubes in $\mathbb{F}_{16}$; namely the roots of the polynomial $(x^4+x^3+1)(x^4+x+1)$. This gives $\#\mathcal{C}_1(\mathbb{F}_{16})=(6+8)\times 3+3=45$.

Now, let $\mathcal{C}_2$ be the curve of genus $g(\mathcal{C}_2)=4$ defined as in the above example by the equation

$$y_2^3=\frac{(x^2+x+1)^3(x^3+x+1)^2}{x(x+1)(x^3+x^2+1)^3}. \tag{10}$$

In this case we have $T_1=\{\zeta_1,\zeta_2,\zeta_3,\gamma_1,\gamma_2,\gamma_3\}$ and $T_2=\{0,1,\zeta_1,\zeta_2,\zeta_3,\infty\}$, where $\zeta_i^3+\zeta_i+1=0$ and $\gamma_i^3+\gamma_i^2+1=0$. Therefore $\tau=3$ and we have $g(\mathcal{C})=2\times 2+3\times 4+3\times 4-\frac{3}{2}(9-3)=19$.

For the rational points, first we analyze the points corresponding to $x=0$, $x=1$ and $x=\infty$. Observe that those points are unramified in $\mathcal{C}_1$ but they are totally ramified in $\mathcal{C}_2$.

The equation defining the curve $\mathcal{C}_1$ can be rewriten as

$$z^3=(y_1x(x+1))^3=(x^3+x+1)^5(x^3+x^2+1)x^3(x+1)^3\,,$$

and by (10) we have

$$\left(\frac{y_2^3z(x^3+x^2+1)^2}{(x^3+x+1)^3(x^2+x+1)^3}\right)^3=\frac{(x^3+x^2+1)^2}{(x^3+x+1)^2}. \tag{11}$$

Now we see that the RHS of this equality takes the value 1 when $x = 0$ or $x = 1$. For $x = \infty$ we take $t = \frac{1}{x}$ we have that (11) can be write as

$$T^3 = \frac{1 + \frac{1}{t^4} + \frac{1}{t^6}}{1 + \frac{1}{t^2} + \frac{1}{t^6}}.$$

This expression takes the value 1 when $t = 0$. Therefore the nine points corresponding to $x = 0$, $x = 1$ and $x = \infty$ are rational over $\mathbb{F}_{16}$. On the contrary, one checks easly that the points satisfying $x^2 + x + 1 = 0$ in the curve $\mathcal{C}_2$ are not rational over $\mathbb{F}_{16}$. This then gives $d(x) = \mathcal{P}_2(q) = x^{12} + x^9 + x^6 + x^3 + 1$ and hence we have $\#\mathcal{C}(\mathbb{F}_{16}) = 3 \times 3 \times 12 + 9 = 117$.

$\square$

Example 8.3 Consider the Kummer cover E_1 over $\mathbb{F}_{25}$ defined by the equation given in Theorem 5.2.1, for $q = 5$, i.e:

$$y_1^{\frac{r}{d}} = \omega(x^5 - x)^{\frac{4}{d}}$$

with r a divisor of 24 and $w^d = -1$ where $d = gcd(r, 4)$.

Consider also the cover E_2 of genus 3 defined by

$$y_2^2 = -\frac{x^4(x^4 - a)^5}{a^5x^4 - 1}$$

with $a \in \mathbb{F}_{25}$ and $a^6 = -1$. In this example we have $f(x) = (x^5 - ax)^5$ and $\ell_1(x) = x^{25} - x$, and the condition $a^6 \neq 1$ implies that there is no common roots for the numerator and denominator , and that these roots are not elements of $\mathbb{F}_{25}$, except the root $x = 0$.

Then $T_1 = \{0, 1, 2, 3, 4, \infty\}$ and T_2 has eight elements, namely all roots of the polynomials $(x^4 - a)$ and $(a^5x^4 - 1)$. Then $\tau = 0$ and hence the compositum $E = E_1E_2$ has genus $g(E/\mathbb{F}_{25}) = 8\frac{r}{d} - 5$ as follows from Theorem 8.2.

For the rational points,we claim that: if $\alpha \in \mathbb{F}_5 \cup \{\infty\}$, then the two points lying over each $x = \alpha$ are rational. In fact, for $\alpha \in \mathbb{F}_5^*$, we have

$$y_2^2 = \frac{-x^4(x^4 - a)^5}{a^5x^4 - 1} = \frac{-(1 - a)^5}{a^5 - 1} = 1.$$

This shows that the two points above $x = \alpha \in \mathbb{F}_5^*$ are indeed rational points over $\mathbb{F}_{25}$.

Now for $x = 0$, we have

$$\left(\frac{y_2}{x^2}\right)^2 = -\frac{(x^4 - a)^5}{a^5x^4 - 1} = a^5 = \frac{1}{a}.$$

For the rationality of the two points above $x = 0$, we have to show that $\frac{1}{a}$ is a square in $\mathbb{F}_{25}$; i.e., we have to show that $a^{12} = 1$ and this follows from the hypothesis $a^6 = -1$.

Now for $x = \infty$, we have

$$\left(\frac{y_2}{x^{10}}\right)^2 = -\frac{(1 - \frac{a}{x^4})^5}{(a^5 - \frac{1}{x^4})} = -\frac{1}{a^5} = a.$$

Now the rationality of the two points above $x = \infty$ follows as in the case $x = 0$ trated above.

Hence we have 12 rational points coming from the values of x satisfiying $x = \alpha \in \mathbb{F}_5 \cup \{\infty\}$

Now, since $d(x) = \mathcal{P}_2(5) = x^{20} + x^{16} + x^{12} + x^8 + x^4 + 1$, then $\#\mathcal{C}(\mathbb{F}_{25}) = 20 \times 2 \times \frac{r}{d} + 12$. This gives for $r = 24$, a curve $\mathcal{C}$ with genus $g(\mathcal{C}) = 43$ and 252 rational points, and for $r = 6$, a curve $\mathcal{C}$ with genus $g(\mathcal{C}) = 19$ and 132 rational points. This provides two new entries in [14]. □

Example 8.4 Here we are going to construct a curve $\mathcal{C}$ over $\mathbb{F}_8$ with $g(\mathcal{C}) = 57$ and $\#\mathcal{C}(F_8) = 168$. One can not find such a genus $g = 57$ on the tables, but this number (168) of rational points is certainly a big number for such a genus (compare with the table in [5].

Take $q = 8$, $\ell(x) = x^3 + x + 1$ and $f_1(x) = x^4 + x^2$. Then $\mathcal{R}_\ell(f_1(x)) = x$, and we consider the curve $\mathcal{C}_1$ given by

$$y_1^7 = x(x+1)^2.$$

Here we have three totally ramified points, and this gives $g(\mathcal{C}_1) = 3$. Moreover we can check that $\#\mathcal{C}_1(\mathbb{F}_8) = 7 \times 3 + 3 = 24$; i.e., the curve $\mathcal{C}_1$ attains Serre's bound over the finite field $\mathbb{F}_8$.

Now, with $f_2(x) = (x^2 + x + 1)^2$ we have $\mathcal{R}_\ell(f_2(x)) = x + 1$ and we consider the curve $\mathcal{C}_2$ given by

$$y_2^7 = \frac{(x^2 + x + 1)^2}{x + 1}.$$

Here we have 4 totally ramified points, therefore $g(\mathcal{C}_2) = 6$. One check easily that the curve $\mathcal{C}_2$ has $4 \times 7 + 2 = 30$ rational points over $\mathbb{F}_8$.

Now since $\tau = 2$, corresponding to $x = 1$ and $x = \infty$, the compositum E of the function fields has genus $g(E) = 57$ as follows from Theorem 8.2.

Since the zeros of $\ell(x) = x^3 + x + 1$ split completely both in E_1 and E_2, by Remark 8.1 we have at least $7 \times 7 \times 3 = 147$ rational points.

It is easy to see that the 7 points above $x = 0$ are rational. Now we show that the 7 points above $x = 1$ (resp $x = \infty$) are rational.

Denoting by ν_{P_1} the unique valuation of $E_1 := \mathbb{F}_8(x, y_1)$ corresponding to the zero of $x + 1$, we have that $\nu_{P_1}(x + 1) = 7$ and $\nu_{P_1}(y_1) = 2$. Taking $t = \frac{x+1}{y_1^3}$ as a local parameter for P_1, we can write $y_1 = xt^2$ and we see that

$$y_2^7 = \frac{(x^2 + x + 1)^2}{x + 1} = \frac{(x^2 + x + 1)^2}{ty_1^3} = \frac{(x^2 + x + 1)^2}{x^3t^7}.$$

Therefore we obtain the equation

$$(y_2 t)^7 = \frac{(x^2+x+1)^2}{x^3}. \tag{12}$$

Now it is easy to see that the 7 points corresponding to $x = 1$ are rational.

Now for the 7 points above $x = \infty$. Let ν_{P_∞} denote the unique valuation on E_1 corresponding to $x = \infty$. We have $\nu_{P_\infty}(x) = 7$ and $\nu_{P_\infty}(y_1) = -3$.

We then see that $t := \frac{y_1^2}{x}$ is a uniformizer at ν_{P_∞} and we can write

$$\left(\frac{y_2}{y_1}\right)^7 = \frac{(1 + ty_1^{-2} + t^2 y_1^{-4})^2}{(y_1 t^3 + t^4 y_1^{-1})}.$$

Now it is easy to see that the right side in the equality above has the value 1 at the point on the curve $\mathcal{C}_1$ with $x = \infty$, since

$$y_1 t^3 = \frac{(x+1)^2}{x^2}.$$

Hence $\#\mathcal{C}(\mathbb{F}_8) = 147 + 3 \times 7 = 168$. □

Example 8.5 For $q = 27$, let us consider the compositum $E = E_1E_2$ with $E_1 = \mathbb{F}_{27}(x, y_1)$ and $E_2 = \mathbb{F}_{27}(x, y_2)$ where

$$y_1^2 = \mu_1(x) := \frac{x^8(x^2+1)^9}{x^8+1} \quad \text{and} \quad y_2^2 = \mu_2(x) := -\frac{x^8(x^2-1)^8}{(x^4+1)(x^2+1)}.$$

Here we took $f_1(x) = (x^3+x)^9$ and $\ell_1(x) = x^{26}-1$ for the extension $E_1/\mathbb{F}_{27}(x)$. This gives $g_1 = 4$. Also for the extension E_2, we took $f_2(x) = (x^3-x)^8$ and $\ell_2(x) = \mathcal{P}_3(3) = \frac{x^{26}-1}{x^2-1}$. This gives $g_2 = 2$.

On the other hand $gcd(\ell_1(x), \ell_2(x)) = \ell_2(x)$ and $T_1 \cap T_2 = \{\zeta_1, \zeta_2\}$ where $\zeta_i^2 + 1 = 0$. Therefore $\tau = 2$, and this gives $g(\mathcal{C}) = 11$, where $\mathcal{C}$ is the curve corresponding to the compositum $E = E_1E_2$.

Since $\ell_2(x)$ is a polynomial of degree 24 whose roots are exactly the elements of $\mathbb{F}_{27} \backslash \mathbb{F}_3$ and since the points corresponding to those roots split completely both in E_1 and E_2, we have $\#\mathcal{C}(\mathbb{F}_{27}) \geq 2 \times 2 \times 24 = 96$.

The other possible rational points over $\mathbb{F}_{27}$ are those with $x = 0$, $x = \pm 1$ and $x = \infty$.One can show that (because of the minus sign in the equation for y_2) those points are not rational, and hence $\#\mathcal{C}(\mathbb{F}_{27}) = 96$ which is the actual record in the table [5]. We make the details for the case $x = \infty$. We have

$$\left(\frac{x^3 y_2}{x^4(x^2+1)^4}\right)^2 = \frac{-1}{1 + \left(\frac{1}{x}\right)^2 + \left(\frac{1}{x}\right)^4 + \left(\frac{1}{x}\right)^6}.$$

The RHS calculated at $x = \infty$ has value -1, which is not a square in $\mathbb{F}_{27}$, and hence the points over $x = \infty$ are not rational over $\mathbb{F}_{27}$. $\square$

Example 8.6 In this example we are going construct a curve $\mathcal{C}$ over $\mathbb{F}_{64}$ with $g(\mathcal{C}) = 19$ and with 297 rational points. This provides a new entry in the table [5]. This curve is the fiber product over the x-line of two curves $\mathcal{C}_1$ and $\mathcal{C}_2$ given respectively by:

$$y_1^3 = u(x) := \frac{(x+1)^4}{x^3+x+1} \quad \text{and} \quad y_2^3 = (x^8+x)^7.$$

The curve $\mathcal{C}_1$ was analyzed in Example 6.6 and the curve $\mathcal{C}_2$ was obtained from Theorem 5.2.1 with $q = 8$. Then we have $g(\mathcal{C}_1) = 3$ and $g(\mathcal{C}_2) = 7$. On the other hand,

$$T_1 = \{1, \infty, \zeta_1, \zeta_2, \zeta_3\} \quad \text{and} \quad T_2 = \{0, 1, \infty, \zeta_1, \zeta_2, \zeta_3, \theta_1, \theta_2, \theta_3\},$$

with $\zeta_i^3 + \zeta_i + 1 = 0$ and $\theta_i^3 + \theta_i^2 + 1 = 0$. Therefore $\tau = 5$ and this gives $g(\mathcal{C}) = 19$ (see Theorem 8.2).

Now to compute the number of rational points, observe that in the Example 6.6 we have obtained that $\kappa = 12$, more precisely, thru a computer serch one seez that the points $\alpha \in \mathbb{F}_{64}$ such that $u(\alpha)$ is a 3-rd power in $\mathbb{F}_{64}^*$ are exactly the roots of the polynomial $\ell_1(x) = x^{36} + x^{35} + x^{34} + x^{33} + x^{29} + x^{26} + x^{24} + x^{22} + x^{21} + x^{17} + x^{16} + x^{15} + x^{14} + x^7 + x$.

On the other hand, the polynomial used to reduce $(x^8 + x)^7$ was $\mathcal{P}_6(2) = \frac{x^{64}+x}{x^8+x}$; then we obtain $\deg(gcd(\ell_1(x), \mathcal{P}_6(2))) = 30$ and this gives at least $3 \times 3 \times 30 = 270$ rational points.

The points satisfying $x = 1$, $x = \infty$ or $x = \zeta$ with $\zeta^3 + \zeta + 1 = 0$ are totally ramified both in E_1 and in E_2. Hence they are unramified in the extension $E = E_1E_2$ over E_1 and we have 3 points on the curve $\mathcal{C}$ corresponding to E for each first coordinate equal to $x = 1$ or $x = \infty$ or $x = \zeta$. This gives us a total amount of 15 poitns and they are indeed rational points over $\mathbb{F}_{64}$. We sketch below the proof of the rationality of the three points on $\mathcal{C}$ above $x = \zeta$. We can describe the extension E/E_1 by the equation

$$\left(\frac{y_1y_2}{(x^8+x)(x+1)}\right)^3 = (x+1)(x^2+x)(x^3+x^2+1).$$

The RHS above computed at $x = \zeta$ gives the value $\zeta^4 \in \mathbb{F}_8$ and hence it is a third power in $\mathbb{F}_{64}^*$. The rationality of the points above $x = 1$ or $x = \infty$ is proven similarly.

The other possible rational points over $\mathbb{F}_{64}$ are the ones above $x = 0$ or above $x = \theta_i$, $i = 1, 2, 3$. We are going to show that those 12 points are indeed rational points over $\mathbb{F}_{64}$ and hence $\#\mathcal{C}(\mathbb{F}_{64}) = 270 + 15 + 12 = 297$.

Since the equation for $\mathcal{C}_1$ is

$$y_1^3 = u(x) := \frac{(x+1)^4}{x^3+x+1},$$

we have clearly that the value of the RHS at $x = 0$ is equal to 1 and hence the points above $x = 0$ are indeed rational. Now we compute the value of RHS at $x = \theta$ with $\theta^3 + \theta^2 + 1 = 0$. We have

$$\frac{(\theta+1)^4}{\theta^3+\theta+1} = \frac{(\theta+1)^4}{\theta^2+\theta} = \frac{(\theta+1)^3}{\theta} = \frac{\theta^3+\theta^2+\theta+1}{\theta} = 1,$$

and hence the nine points with $x = \theta_i$ (for $i = 1, 2, 3$) are also rational points over $\mathbb{F}_{64}$. $\square$

References

[1] A. Garcia and L Quoos, *A Construction of Curves over Finite Fields* , to appear in Acta Arithm.

[2] A. Garcia and H. Stichtenoth , *A Class of Polynomials over Finite Fields*, Finite Fields and their Appl. 5 (1999), 424-435.

[3] A. Garcia , H. Stichtenoth and C. P. Xing , *On Subfields of the Hermitian Function Field*, Compositio Math.120 (2000), 137-170.

[4] G van der Geer and M. van der Vlugt, *Kummer Covers with many Rational Points*,Finite Fields and their Appl. 6 (2000), 327-341.

[5] G van der Geer and M. van der Vlugt, *Tables for the function* $N_q(g)$, available at http://www.wins.uva.nl/ geer.

[6] H. Hasse, *Theorie der relativ zyklischen algebraischen Funktionenkorper*, J. Reine Angew. Math 172 (1934), 37-54.

[7] V. D. Goppa, *Codes on algebraic curves.* Sov. Math. Dokl.24 (1981), p 170-172.

[8] Y. Ihara,*Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo 28 (1981), p 721-724.

[9] R. Lild and H. Niederreiter, *Finite Fields and Applications*, Cambridge Univ. Press, Cambridge, 1994.

[10] F. Ozbudak and H. Stichtenoth , *Curves with many points and configurations of hyperplnes over finite fields*, Finite Fields and Appl 5. (1999),p.436-449. Springer-Verlag, Berlin, 1993.

[11] J-P. Serre. *Sur le nombre de points rationnels d'une courbe alge'brique sur un cops fini.* C.R.Sci. Paris 296, Serie I (1993) p. 397-402.

[12] J-P. Serre. *Rational points on curves over finite fields* Notes of lectures at Harvard University 1985.

[13] H. Stichtenoth , *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[14] V. Shabat, *Tables of curves with many points*, available at http://www.wins.uva.nl/ shabat/tables.html.