Revista Colombiana de Matemáticas
Volumen 37 (2003), páginas 37–50

Euclidean algorithm and Kummer covers with many points

Alvaro Garzón
Universidad del Valle, Cali, COLOMBIA

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

Keywords and phrases. algebraic curves, finite fields, rational points, Kummer extensions .

1991 Mathematics Subject Classification. Primary: 14G05.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements and let $\mathcal{C}$ be an affine plane algebraic curve (over the finite field $\mathbb{F}_q$). We will denote by $\mathcal{C}(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points of $\mathcal{C}$ and by $g(\mathcal{C})$ its genus.

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 geometrically irreducible nonsingular curve $\mathcal{C}$ of genus g over a finite field of cardinality q, namely

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

This bound was proved for elliptic curves (i.e, $g = 1$) by H. Hasse in 1933. However, the question of finding the maximum 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]).

The aim of this work is the construction of curves over finite fields with many rational points. The method used is motivated by [4] and 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 consider curves $\mathcal{C}$ over $\mathbb{F}_q$ defined by the affine equation

$$y^r = \mu(x) := \frac{f(x)}{\mathcal{R}_\ell(f(x))} \qquad \text{or} \qquad y^r = \nu(x) := \mathcal{R}_\ell(f(x)^r)$$

where $\mathcal{R}_\ell(f(x)$ is the remainder of the Euclidean division of $f(x)$ by $\ell(x)$ and r a divisor of $q-1$. Then, 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.

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 and others.

The paper is organized as follows: In section 2 we give the details of our method for the construction of good curves over finite fields. In section 3 we construct polynomials $\ell(x)$ as a sum of certain symmetric polynomials in m variables over $\mathbb{F}_q$ and obtain good curves over $\mathbb{F}_{q^3}$. In Section 4 we compute explicitly the polynomial $\mathcal{R}_\ell(f(x))$ when $f(x) = (x^q - x)^r$ and $\ell(x) = x^{q^2} - x$. In Section 5 we construct fiber products of Kummer covers defined by equation of the type described above, and we obtain three new records.

2. 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

$$y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))}, \qquad r \mid q-1. \tag{1}$$

Notation. Given $f(x)$ and $\ell(x)$ polynomials, we will denote by $\mathcal{R}_\ell(f(x))$ the remainder of the Euclidean division of $f(x)$ by $\ell(x)$. This way, we have (essentially)

$$\ell(\alpha) = 0 \Longrightarrow \frac{f(\alpha)}{\mathcal{R}_\ell(\alpha)} = 1.$$

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

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 2.1). So in general the inseparability of this product is desirable.

Remark 2.1. 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 $f(\alpha) \neq 0$,

$$\frac{f(x)}{\mathcal{R}_\ell(f(x))}(\alpha) = 1.$$

(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

$$\frac{\mathcal{R}_\ell(f(x)^{r+k})}{\mathcal{R}_\ell(f(x)^k)}(\alpha)$$

are r-th powers in $\mathbb{F}_q$.

Proposition 2.1. *The curve $\mathcal{C}$ over the finite field $\mathbb{F}_q$ given by the Kummer equation*

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

where r divides $q-1$ and the rational function $\mu(x)$ 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 $(\mu) = \sum_{i=1}^n d_i P_i$ is the divisor of μ 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 [10] Theo III.4.12 and III.7.3. By Remark 2.1, for each point $\alpha \in \mathcal{V}_\ell \cap \mathbb{F}_q$ with $f(\alpha) \neq 0$, we have that $\mu(\alpha) = 1$, 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 2.2. (i) Observe that in the proof of Proposition 2.1 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

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

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 $\ell(\alpha)h(\alpha) \neq 0$ where $f(x) = \ell(x)h(x)+\mathcal{R}_\ell(f(x))$ correspond to the elements $\alpha \in \mathbb{F}_q$ such that $\mu(\alpha)$ is a r-th power in $\mathbb{F}_q$ distinct from 1.

We always have that

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

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. We some times carried out a computer science to determinate the value κ.

(ii) By Remark 2.1, *ii*) if the curve $\mathcal{C}$ in Proposition 2.1 is defined by an 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 construction of curves defined by equations of kind (1). Before this, observe that since our interest is the construction of curves with many rational points it is reasonable to suppose that there exist at most one element $\alpha \in \mathbb{F}_q$ such that $\mu(\alpha)$ is a r-th power in $\mathbb{F}_q$ i.e., the rational points in the curve $\mathcal{C}$ not only coming from of the ramification points.

Proposition 2.2. *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 $(x, y) \mapsto (x, (x-\theta)y)$ gives the desired isomorphism. ☑

3. 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 $j = 1, \ldots m$ we define (see [2])) a polynomial $s_{m,j}(x) \in \mathbb{F}_q[x]$ as follows

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

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

Lemma 3.1. *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 $\alpha := (\alpha_1, \ldots, \alpha_j)$ with $0 \leq \alpha_i \leq m-1$ and $\alpha_1 < \alpha_2 < \cdots < \alpha_j$. Let $\Lambda^*_{m,j} = \{\alpha \in \Lambda_{m,j} \ ; \ \alpha_1 > 0\}$. Clearly we have a bijection

$$\begin{aligned} \Lambda_{m,j} &\longleftrightarrow \{\text{Monomials of } s_{m,j}(x)\} \\ \alpha &\longmapsto x^{q^{\alpha_1}} x^{q^{\alpha_2}} \cdots x^{q^{\alpha_j}} \end{aligned}$$

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 $g(x) = x^{q^{\beta_1}} \cdots x^{q^{\beta_{j-1}}}$ with $\beta = (\beta_1, \ldots, \beta_{j-1}) \in \Lambda^*_{m,j-1}$. Hence $g(x) = (x^{q^{\beta_1 - 1}} \cdots x^{q^{\beta_{j-1}-1}})^q$ with $\beta - 1 := (\beta_1 - 1, \ldots, \beta_{j-1} - 1) \in \Lambda_{m-1,j-1}$.

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

Remark 3.1. The item (iii) in Lemma 3.1 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], Theorem 3.2).

Lemma 3.2. *The polynomial $\tau_m(x) := \sum_{j=0}^{m-1} s_{m,j}(x)$ is separable, it has $deg(\tau_m) = t_m := q^{m-1} + \cdots + q$ 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 3.1, item (i) we have

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

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). ☑

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 3.3. *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 3.2 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 that

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

On the other hand, again by the proof of the Lemma 3.2,

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

Therefore

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

The important features of taking $\ell(x)$ and $f(x)$ as in Lemma 3.3 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 3.1. *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*

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

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 Lemma 3.2, $u = \gcd(t_{m-1}+1, r)$, $v = \gcd(q-1, r)$ 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 [10], III-7-4).

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 and the estimate for number of rational points over $\mathbb{F}_{q^m}$ follows from Proposition 2.1. ☑

Remark 3.2. If $m = 2$ in the above Theorem, we obtain a curve over $\mathbb{F}_{q^2}$ defined by the equation $y^r = -\frac{(x+1)^q}{x}, \quad r|q^2-1$, which is a maximal curve; to see this observe that the substitution $x \longmapsto -(1/w)$ leads to 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).

The following examples are applications of Theorem 3.1 in the case $m = 3$.

Example 3.1. 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 $g(\mathcal{C}) = 9$.

The points corresponding to $x = 0$, $x = 1$ and $x = \infty$ are rational; therefore the number of $\mathbb{F}_8$-rational points is $\mathcal{C}(\mathbb{F}_8) = 7 \times 6 + 3 = 45$. We do not know any curve over $\mathbb{F}_8$ of genus 9 having more than 45 rational points (see table in [5]).

Example 3.2. 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 $g(\mathcal{C}) = 1$, and $\#\mathcal{C}(\mathbb{F}_{27}) = 2 \times (12 + 6) + 1 + 1 = 38$; 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 $\#\mathcal{C}(\mathbb{F}_{27}) = 26 \times 12 + 1 + 1 = 314$. We do not know any curve over $\mathbb{F}_{27}$ of genus 49 having more than 314 rational points (see table in [5]).

Example 3.3. 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 [11]).

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 number of rational points is given by $\#\mathcal{C}(\mathbb{F}_{125}) = 2 \times (30 + 43) + 5 = 151$.

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

4. 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], Theorem 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 (1) or

$$y^r = \mathcal{R}_\ell(f^r(x)) \tag{5}$$

with r a divisor of $q-1$, satisfies $\#\mathcal{C}(\mathbb{F}_q) \geq rjn$. This gives already many rational points.

The next Theorem provides curves over $\mathbb{F}_{q^2}$ with the same properties (genus and number of rational points) as those obtained in [1] Example 4.1; the equations defining these curves are of the type (5), where $\ell(x) = x^{q^2} - x$. Before stating it we will prove the following result:

Lemma 4.1. *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. If $v(x) = x^q - x$, 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

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

The lemma follows 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. ☑

Remark 4.1. 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 $x = \alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 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 4.1. *Let $r = (q-1)n + t$ be as in the Lemma 4.1 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*

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

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 $\mathbb{F}_{q^2}$.

5. Fiber Products of Kummer Covers

In this section we will consider algebraic function fields of the type $E = K(x, y_1, y_2)$, where for $i = 1, 2$

$$y_i^{r_i} = \mu_i(x) = \mathcal{R}_\ell(f(x)^{r_i}) \in K(x)$$

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 $\mu_1(x) \neq \mu_2(x)$.

Our next theorem gives a formula to compute the genus is this type of extensions. Before stating it, 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 $P_\alpha \in \mathbf{P}^1(\bar{K})$. For each $i = 1, 2$, let

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

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

and

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

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 5.1. *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 [10] III-8-9, 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 $e(P_\alpha) = \frac{r_1 r_2}{\delta}$.

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 $e(P_\alpha) = \frac{r_1 r_2}{\delta}$.

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

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

the formula for the genus follows from Hurwitz formula. ☑

Remark 5.1. *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*

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

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 $[E : K(x)] = r_1 r_2$ 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:

$$\#\mathcal{C}(\mathbb{F}_q) \geq r_1 r_2 \lambda$$

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 5.1. Let $\mathcal{C}$ be the curve over $\mathbb{F}_{27}$ which is the fibre product of the curves $\mathcal{C}_1$ and $\mathcal{C}_2$ given by

$$y^2 = \frac{-(x^3-x)^8}{x^6+x^4+x^2+1} \quad \text{and} \quad y^2 = x(x+1)^2(x^2+1)(x^2-x-1)^3$$

This curve satisfies $g(\mathcal{C}) = 5$ and $\#\mathcal{C}(\mathbb{F}_{27}) = 72$; the former best known value was 68 rational points.

Observe that the curve $\mathcal{C}_1$ is defined by an equation of the type $y^r = \frac{f(x)}{\mathcal{R}_\ell(f(x))}$ by taking $f(x) = (x^3-x)^8$ and $\ell_1(x) = \frac{x^{27}-x}{x^3-x}$ (see [1], Example 4.8). On the other hand, for the equation defining $\mathcal{C}_2$ we took $f(x) = (x^4 - x^3 - 1)^3$ and $\ell_2(x) = x^{12} - x^{11} + x^{10} + x^9 - x^8 - x^6 + x^5 - x^2 - x - 1$, then $\mathcal{R}_{l_2}(f(x)^2) = x(x+1)^2(x^2+1)(x^2-x-1)^3$. In this case we have $\tau = 4$, and this gives $g = 5$. For the rational points observe that we have that the degree of $\gcd(\ell_1(x), \ell_2(x))$ is exactly 18, therefore $\#\mathcal{C}(\mathbb{F}_{27}) = 2 \times 2 \times 18 = 72$.

Example 5.2. Consider the Kummer cover E_1 over $\mathbb{F}_{27}$ given by the equation

$$y^2 = (x^3 - x)(x^4 + x^3 - 1)$$

which have genus $g(\mathcal{C}) = 3$ and 52 rational points over $\mathbb{F}_{27}$, (here we took $\ell_1(x) = x^9 - x^6 - x^5 + x^4 + x^3 + x^2 - 1$, and $f(x) = x^5$) and consider also the cover E_2 of genus 3 and 51 rational points over $\mathbb{F}_{27}$ defined by

$$y_2^2 = \mu_2 = -(x^3 - x)(x^4 - x^3 - 1).$$

We obtain E_2 by taking $\ell_2(x) = x^9 + x^6 - x^5 - x^4 + x^3 - x^2 + 1$ and $f_2(x) = x^5$.

In this case we have $\tau = 4$ and therefore the genus g of the compositum $E = E_1E_2$ is $1 + 2 \times 6 - 4 = 9$.

For the rational points, observe that the point $x = \infty$ is not rational in E_2, and the points corresponding to $x = 0$, $x = 1$ and $x = -1$ are totally ramified and rational in E. In This example again $\mu_2(\alpha)$ is a square in $\mathbb{F}_{27}$ for all α root of the polynomial $\frac{x^{27}-x}{x^3-x}$; this gives $4 \times 24 + 3 = 99$ rational points and therefore a new record in the table [5].

Example 5.3. We are going to construct here a curve $\mathcal{C}$ over $\mathbb{F}_{27}$ with $g(\mathcal{C}) = 11$ and 100 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 $\mathbb{F}_{27}(x)$. Let E_1 the function field defined at the example 5.2 above, $\ell_2(x) = x^8 - x^7 - x^4 + x^3 + x^2 - x + 1$ and $f_2(x) = x^5 + x^4 - 1$. Then we have that $\mathcal{R}_{\ell_2}(f_2(x)^2) = x(x^6 + x^5 + x^3 + x + 1)$.

We consider the Kummer covers $E_1 := \mathbb{F}_{27}(x, y_1)$ and $E_2 := \mathbb{F}_{27}(x, y_2)$, where $y_2^2 = \mu_2(x) = x(x^6 + x^5 + x^3 + x + 1)$. Here $\tau = 2$, $g_1 = 3$, $g_2 = 3$ and $\delta = 2$. Therefore the function field $E := E_1.E_2$ has genus $1 + 2 \times 6 - 2 = 11$ as follows from Theorem 5.1.

For the rational places, observe first that the places corresponding to θ_i and ζ_i are not rational; in fact these roots belong to $\mathbb{F}_{81}$ and $\mathbb{F}_{729} \setminus \mathbb{F}_{27}$ respectively.

The places corresponding to $x = 0$ and $x = \infty$ are totally ramified in E and therefore are rational, and the place corresponding to $x = -1$ is totally ramified in E_1 and splitting completely in E_2 this gives two more rational places. Finally observe that , $\mu_1(\alpha)$ and $\mu_2(\alpha)$ are squares in $\mathbb{F}_{27}$ for all α root of the polynomial $\frac{x^{27}-x}{x^3-x}$. Hence, we have $\#\mathcal{C}(\mathbb{F}_{27}) = 2 \times 2 \times 24 + 2 + 2 = 100$.

References

[1] A. Garcia & A Garzón, *On Kummer Covers whith many Points*, to appear in the Journal of Pure and Applied Algebra.

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

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

[4] G van der Geer & M. van der Vlugt, *Kummer Covers with many Rational Points*, Finite Fields and their Appl. **6** (2000), 327–341.
[5] G van der Geer & 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), 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), 721–724.
[9] R. Lild & H. Niederreiter, *Finite Fields and Applications*, Cambridge Univ. Press, Cambridge, 1994.
[10] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.
[11] V. Shabat, *Tables of curves with many points*, available at the Web site `http://www.wins.uva.nl/~shabat/tables.html`.

(Recibido en julio de 2003)

Departamento de Matemáticas
Universidad del Valle
Apartado Aéreo 25360 Cali, Colombia
e-mail: `alvarogr@univalle.edu.co`