Revista Colombiana de Matemáticas
Volumen 42(2008)1, páginas 73-84

A family of Kummer covers over the hermitian function field

Una familia de cubrimientos de Kummer sobre el campo de funciones hermitianas

ÁLVARO GARZÓN

Universidad del Valle, Cali, Colombia

ABSTRACT. We construct a family of Kummer covers over the Hermitian Function Field by using a class of polynomials $\tau_2(X,Y)$ wich arises as a generalization of certain simmetryc polynomials $s_2(X)$. The number of rational places of such covers is often rather close to the best value listed in [6].

Key words and phrases. Finite fields, algebraic function fields, rational places, hermitian function field, Kummer extensions.

2000 Mathematics Subject Classification. 14G05.

RESUMEN. Construimos una familia de cubrimientos Kummer sobre el cuerpo de las funciones Hermitianas usando una clase de polinomios $\tau_2(X,Y)$ que surge como una generalización de cierto tipo de polinomios $s_2(X)$. El número de lugares racionales de tales cubrimientos es cercano al mejor valor que se encuentra en [6].

Palabras y frases clave. Campos finitos, campos de funciones algebraicas, lugares racionales, campos de funciones hermitianas, extensiones de Kummer.

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 [4]. 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 [3]).

The construction of curves with many points over $\mathbb{F}_{q^m}$ is often performed using special polynomials $\sigma(X) \in \mathbb{F}_q[X]$. The goal of this paper is to consider a special class of polynomials $\tau_m(X, Y)$, obtained as sums of products of certain symmetric polynomials $s_{m,j}(X)$ defined in [1] to construct a family of Kummer covers over the Hermitian Function Field (Hermitian curve). These new covers has many places of degree one. In this way we provides explicit equations of curves over the field $\mathbb{F}_{q^2}$ which reach in many cases the best value listed in [6].

2. The polynomials $\tau_m(X, Y)$

In this section we give some properties of a certain class of polynomials $\tau_m(X, Y)$ which was introduced in [2]. These polynomials arise as product of symmetric polynomial $s_m(X)$ where $s_m(X) = s_m\left(X, X^q, \ldots, X^{q^{m-1}}\right)$ is the m-th symmetric elementary polynomial.

Definition 2.1. *For integers $m \geq 1$ and $j = 1, \ldots, m$ we define a polynomial $s_{m,j}(X) \in \mathbb{F}_q[X]$ as follows*

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

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 $j > m$ and for $j < 0$.

Observe that according to with 2.1:

$$\begin{aligned}
s_{m,1}(X) &= X + X^q + \ldots + X^{q^{m-1}} \\
s_{m,2}(X) &= X^{1+q} + X^{1+q^2} + \ldots + X^{q^{m-2}+q^{m-1}} \\
&\vdots \\
s_{m,m}(X) &= X^{1+q+\ldots+q^{m-1}} \\
s_{m,j}(X) &= 0, \qquad \text{for } j > m
\end{aligned}$$

and $\deg(s_{m,j}(X)) = q^{m-1} + q^{m-2} + \ldots + q^{m-j}$ for $1 \leq j \leq m$.

Definition 2.2. *For integers $m \geq 1$ and $j = 1, \ldots, m$ we define a polynomial $\sigma_{m,j}(X,Y) \in \mathbb{F}_q[X,Y]$ as*

$$\sigma_{m,j}(X,Y) := s_{m,m}(Y) s_{m,j}\left(\frac{X}{Y}\right).$$

In this case we have

$$\sigma_{m,0}(X,Y) = s_{m,m}(Y) s_{m,0}\left(\frac{X}{Y}\right) = Y^{1+q+\ldots+q^{m-1}}$$

$$\sigma_{m,1}(X,Y) = s_{m,m}(Y) s_{m,1}\left(\frac{X}{Y}\right) = XY^{q^{m-1}+\ldots+q} + \ldots + X^{q^{m-1}} Y^{q^{m-2}+\ldots+1}$$

$$\vdots$$

$$\sigma_{m,m}(X,Y) = s_{m,m}(Y) s_{m,m}\left(\frac{X}{Y}\right) = X^{1+q+\ldots+q^{m-1}}.$$

Observe that the polynomials $s_{m,j}(X)$ can be obtained from the $\sigma_{m,j}(X,Y)$ for appropriate values of X or Y, more precisely we have $s_{m,j}(X) = \sigma_{m,j}(X,1)$.

Definition 2.3. *Given a sequence $(c_1, c_2, \ldots, c_m)$ of elements in $\mathbb{F}_q$, we define a sequence of polynomials $\tau_{(c_1,c_2,\ldots,c_m)}(X,Y) \in \mathbb{F}_q[X,Y]$ by*

$$\tau_{(c_1,c_2,\ldots,c_m)}(X,Y) = \sum_{i=0}^{m} c_i \sigma_{m,m-i}(X,Y) \qquad \text{for all } m \geq 1,$$

where the polynomials $\sigma_{m,m-i}(X,Y)$ are defined as in 2.2.

According with 2.3 we have:

$$\tau_{(c_0,c_1)}(X,Y) = c_0 X + c_1 Y$$

$$\tau_{(c_0,c_1,c_2)}(X,Y) = c_0 X^{q+1} + c_1 XY^q + c_1 X^q Y + c_2 Y^{q+1}$$

$$\tau_{(c_0,c_1,c_2,c_3)}(X,Y) = c_0 X^{q^2+q+1} + c_1 X^{q^2+q} Y + c_1 X^{q^2+1} Y^q + c_1 X^{q+1} Y^{q^2} + c_2 X^{q^2} Y^{q+1} + c_2 X^q Y^{q^2+1} + c_2 XY^{q^2+q} + c_3 Y^{q^2+q+1}$$

$$\vdots$$

Remark 2.1. First, observe that if the equality $c_i = c_{m-i}$ holds then we have $\tau_{(c_0,\ldots,c_m)}(X,Y) = \tau_{(c_m,\ldots,c_0)}(Y,X)$, on the other hand by taking the sequence $(1,-1,1,\ldots)$ with alternating 1 and -1 and denoting by $M(m) = 1 + q + \ldots + q^{m-1}$ the exponent of the norm for the extension $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we have $\tau_{(1,-1,1,\ldots)}(X,Y) = (X-Y)^{M(m)}$.

Theorem 2.1. *([2] Th 2.1). For all sequence $(c_0, \ldots, c_m)$ in $\mathbb{F}_q$ we have the following equality:*

$$\tau_{(c_0,\ldots,c_m)}(X,Y)^q - \tau_{(c_0,\ldots,c_m)}(X,Y) = (X^{q^m} - X)\tau_{(c_0,\ldots,c_{m-1})}(X,Y)^q + (Y^{q^m} - Y)\tau_{(c_{m-1},\ldots,c_0)}(Y,X)^q .$$

To see some properties of the polynomials $\tau_{(c_0,\ldots,c_m)}(X,Y)$ we refer to [2].

3. A Kummer cover over the hermitian function field

In this section we use the polynomials $\tau_{(c_0,\ldots,c_m)}$ defined above to construct a family of function fields with many places of degree one over $\mathbb{F}_{q^2}$.

We define the function field $F = \mathbb{F}_{q^2}(x,y,z)$ over $\mathbb{F}_{q^2}$, where q is a prime power, by the equations

$$ly^q + y = x^{q+1}$$
$$z^r = u(x,y) \quad r \mid q+1,$$

where $u(X,Y) \in \mathbb{F}_q[X,Y]$ is the polynomial $\tau_{(c_0,c_1,c_2)}(X,Y) \pm c$ with $c \in \mathbb{F}_q$ and $\tau_{(c_0,c_1,c_2)}(X,Y)$ is defined as (2.3) associated to an appropriate sequence (c_0,c_1,c_2) of elements $c_i \in \mathbb{F}_q$, i.e., $\tau_{(c_0,c_1,c_2)}(X,Y) = c_0X^{q+1} + c_1X^qY + c_1XY^q + c_2Y^{q+1}$.

This is a Kummer extension of degree r of the Hermitian function field

$$H = \mathbb{F}_{q^2}(x,y) \text{ with } y^q + y = x^{q+1}.$$

We compute the genus of $F/\mathbb{F}_{q^2}$ by using the genus formula for Kummer extensions ([5, Prop. III.7.3]):

$$g(F) = 1 + r(g(H) - 1) + \frac{1}{2}\sum_{P \in \mathbb{P}(H)} (r - r_P)\deg(P), \tag{1}$$

where $r_P = \gcd(\nu_P(u), r)$ for a place P in H with discrete valuation ν_P in H. By considering the ramification of the places of degree one of H in F we then determine the number of places of degree one in $F/\mathbb{F}_{q^2}$. In order to use the genus formula (1) for computing the genus of the Kummer extension F of H we have to determinate the divisor of u in H.

Let us first recall some properties of the Hermitian function field ([5, p. 203]).

The genus of H is $g = \dfrac{q(q-1)}{2}$, the number $N = N(H)$ of places of degree one is $N = q^3 + 1$, namely

(1) the common pole P_∞ of x and y and,

(2) for each rational point $(a,b) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ with $b^q + b = a^{q+1}$ there is a unique place $P_{a,b}$ of degree one in H such that $x(P_{a,b}) = a$ and $y(P_{a,b}) = b$.

The pole divisors of x and y in $H/\mathbb{F}_{q^2}$ are

$$(x)_\infty = qP_\infty \quad \text{and} \quad (y)_\infty = (q+1)P_\infty. \tag{2}$$

4. A particular case

In this section we construct a particular Kummer cover over the hermitian function field. We compute the genus and the number of rational places to illustrate the technique we used to obtain these values.

We consider the function field $F = \mathbb{F}_{q^2}(x, y, z)$ over $\mathbb{F}_{q^2}$ with

$$y^q + y = x^{q+1}$$
$$z^r = u(x, y),$$

where $u(x, y) = \tau_{(c_0,c_1,c_2)}(X, Y) - 1$ and $\tau_{(c_0,c_1,c_2)}(X, Y)$ is associated to the sequence $(1, 1, 0)$ of $\mathbb{F}_q$, i.e. $u(x, y) = x^{q+1} + x^q y + xy^q - 1$ and $r \mid q + 1$. Now we want to compute the genus $g = g(F)$ and the number $N(F)$ of places of degree one of $F/\mathbb{F}_{q^2}$.

4.1. **The divisor of u.** By (2) we get for the pole divisor of $u = x^{q+1} + x^q y + xy^q - 1$

$$(u)_\infty = \left(q^2 + 2q\right) P_\infty.$$

To compute the zero divisor of u in H is much harder work. Let us first consider the constant field extension $\overline{H} = H\overline{K}$ where $\overline{K}$ is the algebraic closure of $\mathbb{F}_{q^2}$. Let $P = P_{a,b}$ with $a, b \in \overline{K}$ and $b^q + b = a^{q+1}$ be a place of $\overline{H}/\overline{K}$. If P is a zero of u then

$$b^q + b = a^{q+1} \tag{3}$$

and

$$a^{q+1} + a^q b + ab^q - 1 = 0. \tag{4}$$

Lemma 4.1.1. *A place $P = P_{a,b}$ with $a, b \in \overline{K}$ and $b^q + b = a^{q+1}$ is a zero of u in $\overline{H} = H\overline{K}$ if and only if either*

i) $a^{q-1} = 1$ *and* $a^3 + a^2 - 1 = 0$ *or,*

ii) $a^{q-1} \neq 1$ *and* $b = \dfrac{a^{q+2} + a^{q+1} - 1}{a - a^q}$.

Proof. Suppose that $P = P_{a,b}$ is a zero of u and $a^{q-1} = 1$, t hen from (3) and (4) follows that $b^q = a^2 - b$ and $a^2 + ab + ab^q = 1$, therefore $a^2 + ab + a\left(a^2 - b\right) = 1$ and $a^3 + a^2 - 1 = 0$. Conversely suppose that $a, b \in \overline{K}$ with $a^{q-1} = 1$, $a^3 + a^2 - 1 = 0$ and $b^q + b = a^{q+1}$. Then we have

$$\begin{aligned} a^{q+1} + a^q b + ab^q - 1 &= a^2 + ab + ab^q - 1 \\ &= a^2 + a\left(b + b^q\right) - 1 \\ &= a^3 + a^2 - 1 \end{aligned}$$

which means that $P_{a,b}$ is a zero of u.

Now we consider the case $a^{q-1} \neq 1$. If $P_{a,b}$ is a zero of u, then (3) and (4) implies $b^q = a^{q+1} - b$ and $a^{q+1} + a^q b + a\left(a^{q+1} - b\right) = 1$, therefore $b\left(a^q - a\right) = 1 - a^{q+1} - a^{q+2}$.

Conversely, let $a, b \in \overline{K}$ with $a^{q-1} \neq 1$, $b = \dfrac{a^{q+2} + a^{q+1} - 1}{a - a^q}$ and $b^q + b = a^{q+1}$. Then $a^{q+1} + a^q b = 1 - a^{q+2} + ab$ which implies that

$$\begin{aligned} a^{q+1} + a^q b + ab^q - 1 &= 1 - a^{q+1} + ab + ab^q - 1 \\ &= -a^{q+2} + ab + a\left(a^{q+1} - b\right) \\ &= 0 \end{aligned}$$

and therefore $P_{a,b}$ is a zero of u in $\overline{H}/\overline{K}$ ☑

Lemma 4.1.2. *Let $a, b \in \overline{K}$ with $b^q + b = a^{q+1}$. If $P_{a,b}$ is a zero of u in $\overline{H}$, then*

i) *If $a^{q-1} = 1$, then $a, b \in \mathbb{F}_{q^2}$.*
ii) *If $a^{q-1} \neq 1$, then $a, b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ or $a^3 + a^2 - 1 = 0$.*

Proof. If $P_{a,b}$ is a zero of u in $\overline{H}$, then from (4) follows that $a^2 + ab + ab^q = 1$ and obviously $a, b, \in \mathbb{F}_{q^2}$.

If $a^{q-1} \neq 1$, from Lemma 4.1.1, $b = \dfrac{a^{q+2} + a^{q+1} - 1}{a - a^q}$, therefore from (3), we have the following equation

$$\frac{a^{q^2+2q} + a^{q^2+q} - 1}{a^q - a^{q^2}} + \frac{a^{q+2} + a^{q+1} - 1}{a - a^q} = a^{q+1}$$

which implies $\left(a^{q^2} - a\right)\left(a^3 + a^2 - 1\right)^q = 0$, therefore the result follows. ☑

In accordance with the previous result we should analyze the behavior of the polynomial $f(x) = x^3 + x^2 - 1$, but before this, we will analyze the multiplicities of the zeros $P_{a,b}$ of u.

Lemma 4.1.3. *Let $P = P_{a,b}$ be a zero of u; then $t = y - b$ is a P-prime element, and $\nu_P(u) > 1$ if and only if $b = -\left(a^2 + a\right)$.*

Proof. Let $\delta_t : H \longrightarrow H$ be the derivation of $H/\mathbb{F}_{q^2}$ with respect to t ([5, chap. IV]). Then $\delta_t(z) = \dfrac{dz}{dt}$ for $z \in H$, and from the $P-$adic power series expansion of u with respect to t we have

$$\nu_P(u) > 1 \quad \text{if and only if} \quad \frac{du}{dt}(P) = 0. \tag{5}$$

From the equation $y^q + y = x^{q+1}$ follows $\dfrac{dy}{dt} = x^q \dfrac{dx}{dt}$ and since $dy = dt$ we have $\dfrac{dx}{dt} = \dfrac{1}{x^q}$, therefore

$$\begin{aligned}\frac{du}{dt} &= \frac{d}{dt}\left(x^{q+1} + x^q y + x y^q - 1\right) \\ &= x^q \frac{dx}{dt} + x^q + y^q \frac{dx}{dt} \\ &= 1 + x^q + \frac{x^q}{y^q}.\end{aligned}$$

Finally

$$0 = \frac{du}{dt}(P_{a,b}) \quad \text{if and only if} \quad \left(1 + a + \frac{b}{a}\right)^q = 0 \tag{6}$$

then the assertion follows ☑

The following result shows the relationship among the polynomial $f(x) = x^3 + x^2 - 1$ and the number of zeros of u, more precisely we have

Lemma 4.1.4. *The following properties hold*

i) *If $f(x)$ is separable and has all its roots in $\mathbb{F}_q$, then u has q^2+2q simple zeros of degree 1.*

ii) *If $f(x)$ has a multiple root in $\mathbb{F}_q$, then u has q^2+q-1 simple zeros of degree 1 and one zero of degree 1 and of multiplicity $q+1$.*

iii) *If $f(x)$ has only one root in $\mathbb{F}_q$, then u has q^2-2 simple zeros of degree 1 and 2 multiple zeros of degree 1 and multiplicity $q+1$.*

iv) *If $f(x)$ is irreducible over $\mathbb{F}_q$, then u has q^2-q simple zeros of degree 1 and one zero of degree three and multiplicity q.*

Proof.

i) Let us suppose that $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ with α, β and $\gamma \in \mathbb{F}_q$.

If $P_{a,b}$ is a zero of u with $a^{q-1} = 1$ and $a^3 + a^2 - 1 = 0$, then by (4.1.3) $P_{a,b}$ is a multiple zero, if and only if $ab = -a^3 - a^2 = -1$ and therefore $b = -a^{-1}$ and this implies that $b^q + b = -2a^{-1}$.

On the other hand, from (3) $a^{q+1} = -2a^{-1}$ if and only if $a^3 = -2$ this implies that $a = -2 \cdot 3^{-1}$ and therefore $p = 23$ but $f(x) = (x+15)(x+16)^2$ modulo 23 and therefore $P_{a,b}$ cannot be a multiple zero.

If $a^{q-1} \neq 1$ then, by Lemma (4.1.3) $P_{a,b}$ is a simple zero. Then we have q^2+2q simple zeros of u if $f(x)$ is separable and has all their roots in $\mathbb{F}_q$.

ii) Now suppose that $f(x) = (x-\alpha)(x-\beta)^2$ with α and $\beta \in \mathbb{F}_q$. This occur if and only if $p = 23$. In this case we have $2q-1$ simple zeros of u and one multiple zero, namely, the q zeros $P_{a,b}$ corresponding to the pairs (a,b) with $a = \alpha$ and $b^q + b = \alpha^2$, the $q-1$ simple zeros $P_{a,b}$ corresponding to the pairs (a,b) with $a = \beta$ and $b^q + b = \beta^2$ with

$b \neq -\beta^2 - \beta$, and the corresponding to the pair (a, b) with $a = \beta$ and $b = -\beta^2 - \beta$ which is a multiple zero of u.

If $a^{q-1} \neq 1$ then $P_{a,b}$ is a simple zero of u since $f(x)$ doesn't have zeros outside of $\mathbb{F}_q$ and therefore we have $q^2 - q$ simple zeros.

Now since the degree of the zero divisor equals the degree of pole divisor of u, the multiple zero of u has multiplicity $q + 1$.

iii) If $f(x) = (x - \alpha)\left(x^2 + \beta x + \gamma\right)$ with $x^2 + \beta x + \gamma$ irreducible over $\mathbb{F}_q$, then we have q simple zeros corresponding to pairs (a, b) with $a = \alpha$ and $b^q + b = \alpha^2$.

If $a^{q-1} \neq 1$ and $b = \dfrac{a^{q+2} + a^{q+1} - 1}{a - a^q}$, then by (4.1.3) we have $q^2 - q - 2$ simple zeros and 2 multiple zeros of u, namely, the corresponding to the pairs (a, b) with $a = \zeta_i$.

In order to prove that the multiplicity of these zeros is $q + 1$, we compute the $P_{a,b}$−adic power series expansion of u wit respect to $t = x - a$.

Since $y = b + \alpha_1 t + \alpha_2 t^2 + \ldots + \alpha_{q+1} t^{q+1} + \lambda$ with $\nu_P(\lambda) > q + 1$. Then, the equation $x^{q+1} = y^q + y$ implies

$$t^{q+1} + at^q + a^q t + a^{q+1} = b^q + {\alpha_1}^q t^q + {\alpha_2}^q t^{2q} + \ldots + {\alpha_{q+1}}^q t^{q^2+q} + \lambda^q + b + \alpha_1 t + \alpha_2 t^2 + \ldots + \alpha_{q+1} t^{q+1} + \lambda.$$

We have $\alpha_1 = a^q$, $\alpha_q = a - a^{q^2} = 0$, $\alpha_{q+1} = 1$ and $\alpha_i = 0$ for $i = 2, \ldots, q-1$. This implies that $u(x, y) = -\left(a^{2q+1} + a^{q+2} + a^{q+1} + 1\right) + (2a^q + a)\, t^{q+1} + \omega$ where $\nu_{P_{a,b}}(\omega) > q + 1$.

But $-\left(a^{2q+1} + a^{q+2} + a^{q+1} + 1\right) = -a\left(a^2 + a\right)^q + \left(a^{q+2} + 1\right) = -ab^q + ab^q + ab + 1 = 0$ from 4.1.3 and 3, finally $2a^q + a \neq 0$ since $a \notin \mathbb{F}_q$.

iv) If $f(x)$ is irreducible over $\mathbb{F}_q$, then the zeros of degree one of u i H are the $q^2 - q$ places $P_{a,b}$ with $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $b = \dfrac{a^{q+2} + a^{q+1} - 1}{a - a^q}$. These zeros are simple since if $b = -a^2 - a$, then $f(a) = 0$ which is a contradiction.

We denote these $n = q^2 - q$ places by $P_1, \ldots, P_n$. Then $(u)_0 = P_1 + \ldots + P_n + A$ where A is positive divisor of degree $3q$ in H. In order to prove that A is of the form $A = qP$ with $deg(P) = 3$, we consider the constant field extension $H \cdot \mathbb{F}_{q^6}/\mathbb{F}_{q^6}$ of $H/\mathbb{F}_{q^2}$.

By lemma 4.1.3 the zero divisor of u in $H \cdot \mathbb{F}_{q^6}$ is of the form $\mathcal{P}_1 + \ldots + \mathcal{P}_n + m_1 Q_1 + m_2 Q_2 + m_3 Q_3$, where Q_1, Q_2, Q_3 are the places $P_{a,b}$ with $a \in \mathbb{F}_{q^3}$, $a^3 + a^2 - 1 = 0$, $b = -a^2 - a$ and $m_1 + m_2 + m_3 = 3q$. From ([5, III.1.9]), $con_{H \cdot \mathbb{F}_{q^6}/H}(A) = m_1 Q_1 + m_2 Q_2 + m_3 Q_3$, where $con_{H \cdot \mathbb{F}_{q^6}/H}(A)$ is the conorm divisor of A in the constant field extension $H \cdot \mathbb{F}_{q^6}/H$ of $H/\mathbb{F}_{q^2}$.

Now we show that $A = qP$ with $deg(P) = 3$. Assume that are two different zeros P, P' of u in H with $deg(P)$, $deg(P') > 1$. Then $con_{H\cdot\mathbb{F}_{q^6}/H}(P + P') \leq Q_1 + Q_2 + Q_3$ wich is a contradiction since $deg(con_{H\cdot\mathbb{F}_{q^6}/H}(P + P')) \geq 4$.

Hence $A = mP$ and therefore $con_{H\cdot\mathbb{F}_{q^6}/H}(P) = Q_1 + Q_2 + Q_3$, $deg(P) = 3$ and $m = m_1 = m_2 = m_3 = q$.

☑

4.1.1. **The genus and the number of rational places of $F/\mathbb{F}_{q^2}$.** In order to determinate the genus of $F/\mathbb{F}_{q^2}$ we rewrite the formula (1) by using $g(H) = \frac{q(q-1)}{2}$, and we obtain

$$g(F) = \frac{1}{2}\left[r\left(q^2 - q - 2\right) + 2 + \sum_{P\in\mathbb{P}(H)} (r - r_P)\deg(P)\right], \tag{7}$$

where $r_P = \gcd(\nu_P(u), r)$.

Theorem 4.1.1.1. *The genus $g(F)$ of the function field $F/\mathbb{F}_{q^2}$ satisfies:*

$$g(F) \quad = \frac{(2r-1)q^2 - rq}{2} + \begin{cases} \frac{(r-1)(2q-1)}{2} & \text{if } f(x) \text{ is separable and has all their roots in } \mathbb{F}_q. \\ \frac{(r-1)(q-2)}{2} & \text{if } f(x) \text{ has multiple roots in } \mathbb{F}_q. \\ \frac{-3(r-1)}{2} & \text{if } f(x) \text{ has only one root in } \mathbb{F}_q. \\ \frac{(r-1)(2-q)}{2} & \text{if } f(x) \text{ is irreducible over } \mathbb{F}_q, \end{cases}$$

where as in the Lemma 4.1.4 $f(x) = x^3 + x^2 - 1$.

Proof. It follows from Lemma (4.1.4) and formula (7). ☑

Theorem 4.1.1.2. *The number $N(F)$ of rational places of the function field $F/\mathbb{F}_{q^2}$ satisfies:*

$$N(F) = \begin{cases} r\left(q^3-q^2-2q\right)+\left(q^2+2q+1\right) & \text{if } f(x) \text{ is separable and has all their roots in } \mathbb{F}_q. \\ \geq r\left(q^2-1\right)(q-1)+\left(q^2+q\right) & \text{if } f(x) \text{ has multiple roots in } \mathbb{F}_q. \\ \geq r\left(q^3-q^2\right)+\left(q^2-1\right) & \text{if } f(x) \text{ has only one root in } \mathbb{F}_q. \\ r\left(q^3-q^2+q\right)+\left(q^2-q+1\right) & \text{if } f(x) \text{ is irreducible over } \mathbb{F}_q, \end{cases}$$

where as in the Lemma 4.1.4 $f(x)=x^3+x^2-1$.

Proof. Let P be a place of degree one of H, then P is either totally ramified with exactly one extension of degree one in F or P is unramified. The first case holds for the simple zeros of u and for the pole P_∞. The second case holds for the zeros P with $\nu_P(u)=r$, and for the places P such that $\nu_P(u)=0$. Let us first consider the case of rational places $P=P_{a,b}$ of the hermitian function field H with $\nu_P(u)=0$. If $\nu_P(u)=0$ then by ([2, Th. 2.1]), $u(P)=a^{q+1}+a^qb+ab^q-1\in\mathbb{F}_q^*$. Therefore the polynomial $T^r-u(P_{a,b})$ has r distinct roots in $\mathbb{F}_{q^2}$. Therefore there exist r extensions of degree one in F.

Now, consider the zeros with $\nu_{P_{a,b}}(u)=r$. In this case we consider the $P_{a,b}-$adic expansion of u with respect to $t=x-a$.

Since $y(P_{a,b})=b$, then $y=b+\alpha_1t+\alpha_2t^2+\ldots+\alpha_{q+1}t^{q+1}+\lambda$ with $\nu_P(\lambda)>q+1$. On the other hand, the equation $x^{q+1}=y^q+y$ implies

$$\begin{aligned} t^{q+1}+at^q+a^qt+a^{q+1} &= b^q+\alpha_1{}^qt^q+\alpha_2{}^qt^{2q}+\ldots+\alpha_{q+1}{}^qt^{q^2+q}+\lambda^q \\ &\quad +b+\alpha_1t+\alpha_2t^2+\ldots+\alpha_{q+1}t^{q+1}+\lambda. \end{aligned}$$

Therefore we have $\alpha_1=a^q$, $\alpha_q=a-a^{q^2}=0$, $\alpha_{q+1}=1$ and $\alpha_i=0$ for $i=2,\ldots q-1$, this implies that $u(x,y)=(2a^q+a)t^{q+1}+\omega$ where $\nu_{P_{a,b}}(\omega)>q+1$.

Now, to determinate if a place of degree one in F lies over P we should to analyze the equation $z^r=(2a^q+a)$. ☑

Remark 4.1.1. For $q=2$ and $r=3$ we get $g(F)=7$ and $N(F)=21$ rational places, this value is the best value known. For $q=3$ and we get $g(F)=24$ and $N(F)=91$, this value is again the best value known, however we point out that the curve that appear in [6] for $q^2=9$ and $g=24$ was obtained by using methods that do not provide explicit equations of that curve.

5. Final comments

We concludes this work giving a table in which we consider all the possibilities to the polynomials $\tau_{(c_0,c_1,c_2)}(X,Y)$ for the particular case $q=3$. We give the

genus and the number of rational places of the function field obtained. The column "Entry" makes reference to the tables in [6]. We point out that we use Kash 3 package, to compute this values.

Extension	$g(F)$	$N(F)$	Entry
$z^2 = x^4 + x^3y + xy^3 - 1$	10	49	54
$z^2 = x^4 - x^3y - xy^3 + 1$	10	49	54
$z^2 = x^2 + x^3y + xy^3 + 1$	9	44	48
$z^2 = x^4 - x^3y - xy^3 - 1$	9	44	48
$z^2 = -x^4 - x^3y - xy^3 - 1$	9	44	48
$z^2 = -x^4 - x^3y - xy^3 + 1$	10	49	54
$z^2 = -x^4 + x^3y + xy^3 - 1$	9	44	48
$z^2 = -x^4 + x^3y + xy^3 + 1$	10	49	54

Extension	$g(F)$	$N(F)$	Entry
$z^4 = x^4 + x^3y + xy^3 - 1$	24	91	91
$z^4 = x^4 - x^3y - xy^3 + 1$	24	91	91
$z^4 = x^4 + x^3y + xy^3 + 1$	21	80	88
$z^4 = x^4 - x^3y - xy^3 - 1$	21	80	88
$z^4 = -x^4 - x^3y - xy^3 - 1$	21	80	88
$z^4 = -x^4 - x^3y - xy^3 + 1$	24	91	91
$z^4 = -x^4 + x^3y + xy^3 - 1$	21	80	88
$z^4 = -x^4 + x^3y + xy^3 + 1$	24	91	91

Extension	$g(F)$	$N(F)$	Entry
$z^2 = y^4 + x^3y + xy^3 - 1$	9	48	48
$z^2 = y^4 - x^3y - xy^3 + 1$	9	48	48
$z^2 = y^4 + x^3y + xy^3 + 1$	10	49	54
$z^2 = y^4 - x^3y - xy^3 - 1$	10	49	54
$z^2 = -y^4 - x^3y - xy^3 - 1$	10	49	54
$z^2 = -y^4 - x^3y - xy^3 + 1$	9	48	48
$z^2 = -y^4 + x^3y + xy^3 - 1$	10	49	54
$z^2 = -y^4 + x^3y + xy^3 + 1$	9	48	48

Extension	$g(F)$	$N(F)$	Entry
$z^4 = y^4 + x^3y + xy^3 - 1$	21	80	88
$z^4 = y^4 - x^3y - xy^3 + 1$	24	91	91
$z^4 = y^4 + x^3y + xy^3 + 1$	24	91	91
$z^4 = y^4 - x^3y - xy^3 - 1$	21	80	88
$z^4 = -y^4 - x^3y - xy^3 - 1$	24	91	91
$z^4 = -y^4 - x^3y - xy^3 + 1$	21	80	88
$z^4 = -y^4 + x^3y + xy^3 - 1$	24	91	91
$z^4 = -y^4 + x^3y + xy^3 + 1$	21	80	88

Acknowoledgements. The author deeply appreciates the help received for F. Hess in implementation the of the `Kash3` package.

References

[1] GARCIA, A., AND STICHTENOTH, H. A class of polynomials over finite fields. *Finite Fields and Their Appl. 5* (1999), 424–435.

[2] GARZÓN, A. Homogenized polynomials and curves with many points. *Revista de la Academia Colombiana de Ciencias Exactas, Fisicas y Naturales XXX*, 117 (2006), 555–561.

[3] GOPPA, V. D. Codes on algebraic curves. *Sov. Math. Dokl. 24* (1981), 170–172.

[4] HASSE, H. Theorie der relativ zyklischen algebraischen funktionenkorper. *J. Reine Angew. Math. 172* (1934), 37–54.

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

[6] VAN DER GEER, G., AND VAN DER VLUGT, M. Tables for the function $N_q(g)$. http://www.wins.uva.nl/ geer. Accedido en enero de 2008.

(Recibido en octubre de 2007. Aceptado en marzo de 2008)

DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD DEL VALLE
APARTADO AÉREO 25360
CALI, COLOMBIA
e-mail: alvarogr@univalle.edu.co