HOMOGENIZED POLYNOMIALS AND CURVES WITH MANY POINTS

por

Álvaro Garzón[1]

Resumen

Garzón, A.: Homogenized polynomials and curves with many points. Rev. Acad. Colomb. Cienc. **30** (117): 555-561, 2006. ISSN 0370-3908.

En este artículo construimos una clase de polinomios sobre cuerpos finitos, los cuales surgen como resultado de la homogenización de polinomios simétricos. Estos polinomios son usados para la construcción de cubrimientos de Kummer del cuerpo de funciones hermitiano, el cual tiene muchos lugares de grado uno.

Palabras clave: Cuerpos finitos, curvas algebraicas, puntos racionales.

Abstract

We construct some classes of polynomials over finite fields as homogenization of symmetric polynomials. These polynomials are then used to construct a Kummer covers over the Hermitian function field with many places of degree one.

Key words: Finite fields, algebraic curves, rational points.

1. Introduction

The theory of equations over finite fields is a basic topic in classical number theory. Assuming an analogue of Riemann's hypothesis for the zeta function that he introduced, **Artin** conjectured an upper bound for the number of solutions of equations of type

$$Y^2 = f(X)(\text{modulo a prime number}) \qquad (1)$$

and was widely generalized by **Weil** as follows: Let C be a non-singular projective absolutely irreducible curve of genus g defined over a finite field $\mathbb{F}_q$, then

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q} \qquad (2)$$

where $C(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of C. This inequality is equivalent to validity of Riemann's hypothesis for the zeta function associated to the curve.

[1] Departamento de Matemáticas, Universidad del Valle, Apartado Aéreo 25360, Cali, Colombia E-mail: alvarogr@univalle.edu.co AMS Classification 2000: 14G05.

The interest in curves over finite fields with many rational points (i.e., $\#\mathcal{C}(\mathbb{F}_q)$ is "close" to the upper bound in (2)) was renewed after **Goppa**'s construction of codes with good parameters from such curves [4]. Moreover the number of solutions of congruences in two or more variables is related to estimates of exponential sums over finite fields [7]. The construction of curves with many points over $\mathbb{F}_{q^r}$ 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 $\sigma_{m,j}(X, Y)$, obtained as product of certain symmetric polynomials $s_{m,j}(X)$ defined in [1]. We obtain a nice properties of these new polynomials similar to the ones obtained in [1], and we use them to construct function fields with many places of degree one, equivalently to construct curves with many rational points.

2. The Polynomials $\mathbf{s_{m,j}(X)}$ and $\boldsymbol{\sigma_{m,j}(X, Y)}$

In this section we introduce the polynomials $s_{m,j}(X)$ (see [1]) and we use them to define a new kind of polynomials $\sigma_{m,j}(X, Y) \in \mathbb{F}_q[X, Y]$, which have similar properties to those of the polynomials $s_{m,j}(X)$.

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

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

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

Observe that according to with Definition 2.1,

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

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

Lemma 2.1. *For all $j \subset \mathbb{Z}$ and $m \geq 2$ the following statements hold true*

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. See [1]. □

Remark 2.1. The item iii) in Lemma 2.1 gives two interesting facts: first of all 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 $\bigcup_{1 \leq t \leq m} \mathbb{F}_{q^t}$ ([1, Th. 3.2]).

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

$$\begin{aligned} \sigma_{m,0}(X, Y) &= s_{m,m}(Y) s_{m,0}\left(\frac{X}{Y}\right) \\ &= Y^{1+q+\cdots+q^{m-1}} \\ \sigma_{m,1}(X, Y) &= s_{m,m}(Y) s_{m,1}\left(\frac{X}{Y}\right) \\ &= XY^{q^{m-1}+\cdots+q} + \cdots + X^{q^{m-1}} Y^{q^{m-2}+\ldots+1} \\ &\cdots \\ \sigma_{m,m}(X, Y) &= s_{m,m}(Y) s_{m,m}\left(\frac{X}{Y}\right) = X^{1+q+\cdots+q^{m-1}} \end{aligned}$$

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 $s_{m,j}(X) = \sigma_{m,j}(X, 1)$.

Proposition 2.1. *For all $l \in \mathbb{Z}$ and $r \geq 2$ it holds that*

i) $\sigma_{m,j}(X, Y) = X^{q^{m-1}} \sigma_{m-1,j-1}(X, Y) + Y^{q^{m-1}} \sigma_{m-1,j}(X, Y)$.

ii) $\sigma_{m,j}(X, Y) = Y \sigma_{m-1,j}(X, Y)^q + X \sigma_{m-1,j-1}(X, Y)^q$.

iii) $\sigma_{m,j}(X, Y)^q - \sigma_{m,j}(X, Y) = (X^{q^m} - X) \sigma_{m-1,j-1}(X, Y)^q + (Y^{q^m} - Y) \sigma_{m-1,j}(X, Y)^q$.

Proof. Since $s_{m,m}(Y) = Y^{q^{m-1}} s_{m-1,m-1}(Y)$, by Lemma 2.1, ii), we have

$$\begin{aligned} \sigma_{m,j}(X, Y) &= Y^{q^{m-1}} s_{m-1,m-1}(Y) \left(\left(\frac{X}{Y}\right)^{q^{m-1}} s_{m-1,j-1}\left(\frac{X}{Y}\right) + s_{m-1,j}\left(\frac{X}{Y}\right)\right) \\ &= X^{q^{m-1}} s_{m-1,m-1}(Y) s_{m-1,j-1}\left(\frac{X}{Y}\right) + Y^{q^{m-1}} s_{m-1,m-1}(Y) s_{m-1,j}\left(\frac{X}{Y}\right) \\ &= X^{q^{m-1}} \sigma_{m-1,j-1}(X,Y) + Y^{q^{m-1}} \sigma_{m-1,j}(X,Y) \end{aligned}$$

On the other hand, by 2.1, i),

$$\begin{aligned}\sigma_{m,j}(X,Y) &= s_{m,m}(Y)s_{m,j}\left(\frac{X}{Y}\right)\\ &= Ys_{m-1,m-1}(Y)^q s_{m-1,j}\left(\frac{X}{Y}\right)^q\\ &\quad + Xs_{m-1,m-1}(Y)^q s_{m-1,j-1}\left(\frac{X}{Y}\right)^q\\ &- Y\sigma_{m-1,j}(X,Y)^q + X\sigma_{m-1,j-1}(X,Y)^q\end{aligned}$$

Now, by i) we have

$$\sigma_{m,j}(X,Y)^q = X^{q^m}\sigma_{m-1,j-1}(X,Y)^q + Y^{q^m}\sigma_{m-1,j}(X,Y)^q$$

and by ii),

$$\sigma_{m,j}(X,Y) = Y\sigma_{m-1,j}(X,Y)^q + X\sigma_{m-1,j-1}(X,Y)^q\,,$$

Combining these equalities we obtain $iii)$ □

Remark 2.2. Additionally to the result obtained in the Proposition 2.1 we have other properties of the polynomials $\sigma_{m,j}(X,Y)$ for example, since $s_{m,j}(X) = s_{m,m}(X)s_{m,m-j}(\frac{1}{X})$ we have that:

$$\begin{aligned}\sigma_{m,j}(X,Y) &= s_{m,m}(Y)s_{m,j}\left(\frac{X}{Y}\right)\\ &= s_{m,m}(Y)s_{m,m}\left(\frac{X}{Y}\right)s_{m,m-j}(\frac{Y}{X})\\ &= s_{m,m}(X)s_{m,m-j}\left(\frac{Y}{X}\right) = \sigma_{m,m-j}(Y,X).\end{aligned}$$

And therefore $\sigma_{m,j}(X,Y) = \sigma_{m,j}(Y,X)$ if and only if m is even and $j = \frac{m}{2}$.

Definition 2.3. Given a sequence $(c_0, c_1, ..., c_m)$ of elements $c_i \in \mathbb{F}_q$, we define a sequence of polynomials $\tau_m(X,Y) \in \mathbb{F}_q[X,Y]$ by

$$\tau_m(X,Y) = \sum_{i=0}^{m} c_i\sigma_{m,m-i}(X,Y) \qquad \text{for all } m \geq 1.$$

According to Definition 2.3 we have:

$$\begin{aligned}\tau_1(X,Y) &= c_0X + c_1Y\,,\\ \tau_2(X,Y) &= c_0X^{q+1} + c_1XY^q + c_1X^qY + c_2Y^{q+1}\,,\\ \tau_3(X,Y) &= c_0X^{q^2+q+1} + c_1X^{q^2+q}Y + c_1X^{q^2+1}Y^q,\\ &\quad + c_1X^{q+1}Y^{q^2} + c_2X^{q^2}Y^{q+1}\\ &+ c_2X^qY^{q^2+1} + c_2XY^{q^2+q} + c_3Y^{q^2+q+1},\\ &\cdots\end{aligned}$$

Remark 2.3. First, observe that if the equality $c_i = c_{m-i}$ holds then we have $\tau_m(X,Y) = \tau_m(Y,X)$, on the other hand by taking the sequence $(1,-1,1,...)$ with alternating 1 and -1 and denoting by $M(m) = 1 + q + ... + q^{m-1}$ the exponent of the norm for the extension $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we have $\tau_m(X,Y) = (X-Y)^{M(m)}$.

Theorem 2.1. *For all $m \geq 2$ the following equalities holds*

$$\begin{aligned}\tau_m(X,Y)^q - \tau_m(X,Y) &= (X^{q^m} - X)\tau_{m-1}(X,Y)^q\\ &\quad + (Y^{q^m} - Y)\tilde{\tau}_{m-1}(Y,X)^q\end{aligned}$$

where the polynomials $\tau_{m-1}(X,Y)$ and $\tilde{\tau}_{m-1}(Y,X)$ are defined as 2.3 and they are associated to the sequences given by c_i and $\tilde{c}_i = c_{m-1-i}$, $i = 0, ..., m-1$, respectively.

Proof. By definition and since the coefficients $c_i \in \mathbb{F}_q$ we have

$$\begin{aligned}\tau_m(X,Y)^q - \tau_m(X,Y) &= \sum_{i=0}^{m} c_i^q\sigma_{m,m-i}(X,Y)^q\\ &\quad - \sum_{i=0}^{m} c_i\sigma_{m,m-i}(X,Y)\\ &= \sum_{i=0}^{m} c_i(\sigma_{m,m-i}(X,Y)^q - \sigma_{m,m-i}(X,Y))\\ &= (X^{q^m} - X)\left(\sum_{i=0}^{m} c_i\sigma_{m-1,m-i-1}(X,Y)^q\right)\\ &\quad + (Y^{q^m} - Y)\left(\sum_{i=0}^{m} c_i\sigma_{m-1,m-i}(X,Y)^q\right)\\ &= (X^{q^m} - X)\left(\sum_{i=0}^{m-1} c_i\sigma_{m-1,m-1-i}(X,Y)^q\right)\\ &\quad + (Y^{q^m} - Y)\left(\sum_{i=0}^{m-1} c_{m-1-i}\sigma_{m-1,i}(Y,X)^q\right).\end{aligned}$$

The last equality is obtained by the Remark 2.2. □

3. An application: curves with many points over $\mathbb{F}_{q^2}$

In this section we use the polynomials τ_m to construct 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

$$y^q + y = x^{q-1}\,,$$

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

where $u(X,Y) \in \mathbb{F}_{q^2}[X,Y]$ is the polynomial $\tau_2(X,Y) \pm c$ with $c \in \mathbb{F}_q$ and $\tau_2(X,Y)$ defined as 2.3 associated to suitable sequences in $\mathbb{F}_{q^2}$. 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 [8, Prop. III. 7.3]

$$g(F) = 1 + r(g(H) - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}(H)} (r - r_P)\deg(P) \quad (3)$$

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 (3) for computing the genus of the Kummer extension F of H we have to determinate the principal divisor of u in H.

Let us first recall some properties of the Hermitian function field [8, 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 $y(P_{a,b}) = b$.

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

$$(x)_\infty = qP_\infty \quad \text{and} \quad (y)_\infty = (q+1)P_\infty. \quad (4)$$

3.1. **An optimal function field over $\mathbb{F}_{q^2}$.**

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

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

with $u(x,y) = (x-y)^{q+1} - 1$ and $r \mid q+1$. Observe that $u(X,Y)$ is nothing but $\tau_2(X,Y) - 1$ with $\tau_2(X,Y)$ associated to the sequence $(1,-1,1)$. Now we want to compute the genus $g = g(F)$ and the number $N(F)$ of places of degree one of $F/\mathbb{F}_{q^2}$.

3.1.1. **The principal divisor of u.**

By (4) we get for the pole divisor of $u = (x-y)^{q+1} - 1$

$$(u)_\infty = (q+1)^2 P_\infty.$$

To compute the zero divisor of u in H is much harder work. If $P = P_{a,b}$ with $a, b \in \overline{\mathbb{F}}_{q^2}$ (where $\overline{\mathbb{F}}_{q^2}$ denotes the algebraic closure of $\mathbb{F}_{q^2}$) is a zero of u then

$$b^q + b = a^{q+1} \quad (5)$$

and

$$(a-b)^{q+1} - 1 = 0. \quad (6)$$

Let us first consider $\zeta \in \mathbb{F}_{q^2}$ such that $\zeta^{q+1} = 1$ and consider the straight line $x = y + \zeta$ now, since $y^q + y = x^{q-1}$ then, the common points of this locus satisfies

$$y^{q+1} + (\zeta - 1)y^q + (\zeta - 1)^q y + 1 = 0 \quad (7)$$

Lemma 3.1.1.1. *Let us consider the family of polynomials*

$$\theta_\zeta(T) = T^{q+1} - (\zeta - 1)T^q + (\zeta - 1)^q T + 1 \text{ with } \zeta^{q+1} = 1.$$

All polynomials in the family above have all roots in $\mathbb{F}_{q^2}$. Moreover, they are separable polinomials except if

i) *$p = 3$ and $\zeta = -1$. In this case $T = 1 - \zeta = -1$ is the only multiple root of $\theta_{-1}(T)$ and its multiciplity is $(q+1)$.*
ii) *$q \equiv 2(\mod 3)$ and $a^2 = a - 1$. For each of the two values of a satisfying $a^2 = a - 1$, we have that $T = 1 - a$ is the only multiple root of $\theta_a(T)$ and its multiplicity is $(q+1)$.*

Proof. It is easy to see that the polynomial $\theta(T)$ satisfies

$$\theta(T)^q - \theta(T) = (T^{q^2} - T)(T - (1 - \zeta))^q.$$

This proves that all roots of $\theta(T)$ are in $\mathbf{F}_{q^2}$. On the other hand, since $\theta'(T) = (T - (1-\zeta))^q$, we have that $\theta(1-\zeta) = 0$ if and only if $\zeta^q + \zeta - 1 = 0$ if and only if ζ satisfies the system

$$S = \begin{cases} \zeta^{q+1} = 1 \\ \zeta^q + \zeta - 1 = 0. \end{cases}$$

But S has one solution, namely $\zeta = -1$, if $q \equiv 0(\mod 3)$; S has two solutions, namely the roots of the polynomial $T^2 - T + 1$ if $q \equiv 2(\mod 3)$; and S has no solution if $q \equiv 1(\mod 3)$. □

Theorem 3.1.1.1. *The following properties hold*

i) *If $q \equiv 0(\mod 3)$, then u has $q^2 + q$ simple zeros and one zero of multiplicity $q+1$, all of degree one.*
ii) *If $q \equiv 1(\mod 3)$, then u has $(q+1)^2$ simple zeros.*
iii) *If $q \equiv 2(\mod 3)$, then u has $q^2 - 1$ simple zeros and two zeros of multiplicity $q+1$, all of degree one.*

Proof. It follows directly from Lemma 3.1.1.1. □

3.1.2. The genus and the number of rational places of $\mathbf{F}/\mathbb{F}_{q^2}$. In order to determinate de genus of $F/\mathbb{F}_{q^2}$ we rewrite the formula (3) by using $g(H) = \dfrac{q(q-1)}{2}$, and we obtain

$$g(F)=\frac{1}{2}\left[r(q^2-q-2)+2+\sum_{P\in\mathbb{P}(H)}(r-r_P)\deg(P)\right] \quad (8)$$

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

Theorem 3.1.2.1. *The genus $g(F)$ of the function field $F/\mathbb{F}_{q^2}$ satisfies:*

$$g(F)=\begin{cases}(r(q^2-q)+(r-1)(q^2+q-2))/2 \\ \qquad\qquad \text{if } q\equiv 0(\text{mod } 3)\,, \\ (r(q^2-q)+(r-1)(q^2+2q-1))/2 \\ \qquad\qquad \text{if } q\equiv 1(\text{mod } 3)\,, \\ (r(q^2-q)+(r-1)(q^2-3))/2 \\ \qquad\qquad \text{if} q\equiv 2(\text{mod } 3)\,.\end{cases}$$

Proof. It follows from Lemma 3.1.1.1 and formula (8). □

Theorem 3.1.2.2. *The number $N(F)$ of rational places of the function field $F/\mathbb{F}_{q^2}$ satisfies:*

$$N(F)=\begin{cases}r(q^3-q^2-q+1)+(q^2+q) \\ \qquad\qquad \text{if } q\equiv 0(\text{mod } 3)\,, \\ r(q^3-q^2-2q)+(q+1)^2 \\ \qquad\qquad \text{if } q\equiv 1(\text{mod } 3)\,, \\ r(q^3-q^2)+(q^2-1) \\ \qquad\qquad \text{if } q\equiv 2(\text{mod } 3)\,.\end{cases}$$

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. The second case holds for the zeros P with $\nu_P(u) = q+1$, for the pole P_∞, 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 $u(P) = (a-b)^{q+1} - 1 \in \mathbb{F}_q^*$. Then 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 one of the zeros with $\nu_{P_{a,b}}(u) = q+1$. We claim that if $p \neq 3$ then there is no place of degree one in F lying over $P_{a,b}$. In order to prove this claim we consider the $P_{a,b}-$adic expansion of u with respect to $t - x-a$. Since $y(P_{a,b}) = b$, then $y = b+\alpha_1 t+\alpha_2 t^2+\ldots+\alpha_{q+1}t^{q+1}+\lambda$ with $\nu_P(\lambda) > q+1$. On the other hand, the equation $x^{q+1} = y^q + y$ implies

$$\begin{aligned}t^{q-1}+at^q+a^q t+a^{q+1} = b^q+{\alpha_1}^q t^q+{\alpha_2}^q t^{2q}+\cdots \\ +{\alpha_{q+1}}^q t^{q^2+q}+\lambda^q+b+\alpha_1 t+\alpha_2 t^2+\cdots \\ +\alpha_{q+1}t^{q+1}+\lambda\,.\end{aligned}$$

Therefore we have $\alpha_1 = a^q, \alpha_q = a - a^{q^2}, \alpha_{q+1} = 1$ and $\alpha_i = 0$ $i = 2, \ldots q-1$, and this implies that $u(x,y) = -(a-b)^q t^{q+1} + \omega$ where $\nu_{P_{a,b}}(\omega) > q+1$. Now since $P_{a,b}$ is a multiple zero of u then, by Lemma 3.1.1.1 we have

$$\begin{cases} a = 1 \text{ and } b = -1 & \text{if } q\equiv 0(\text{mod } 3) \\ a = 1 \text{ and } b = 1-\gamma & \text{if } q\equiv 2(\text{mod } 3)\end{cases}$$

with γ being one of the two roots of the polynomial $\gamma^2 - \gamma + 1$. If a place of degree one in F lies over $P_{a,b}$ then by the equation $z^r = u(x,y)$ and the expression $u = -(a-b)qt^{q+1} + \omega$, we obtain

$$\left(\frac{z}{t^{q+1}}\right)^r (P) = -(a-b)^q.$$

Hence there has to exist an element $\beta \in \mathbb{F}_{q^2}$ such that

$$\beta^r - u(P_{a,b}) = \begin{cases} -(-1)^q = 1 \text{ if } q\equiv 0(\text{mod } 3) \\ -(a-b)^q = -\gamma^q = \gamma \quad 1 \\ \qquad\qquad\qquad \text{if } q\equiv 2(\text{mod } 3)\end{cases}$$

Then, the r places lying over P are rational if and only if $q \equiv 0$ (mod 3).

For the pole, let $t = \dfrac{x}{y}$ be an uniformizer to P_∞, then

$$u(x,y) = (x-y)^{q+1} - 1 = y^{q+1}(t-1)^{q+1} - 1$$

and therefore all places lying over P_∞ are rational. □

Remark 3.1.1. For $q = 2$ and $r = q+1$ we get $g(F) = 4$ and $N = 15$, which is optimal since there is no other function field over $\mathbb{F}_4$ with genus 4 and more than 15 places of degree one [2].

3.2. Another Example.

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

$$y^q + y = x^{q+1}$$

$$z^r = u(x,y)$$

with $r \mid q+1$ and $u(X,Y) = Y^{q+1} + Y^q X + Y X^q$.

3.2.1. **The principal divisor of u**. In this case we have that the pole divisor of u is $(u)_\infty = (q+1)^2 P_\infty$. In order to compute the zero divisor of u we proceed as follows:

If $P = P_{a,b}$ with $a, b \in \overline{\mathbb{F}}_{q^2}$ (where $\overline{\mathbb{F}}_{q^2}$ denotes the algebraic closure of $\mathbb{F}_{q^2}$) is a zero of u then

$$\sigma_{2,1}(1,b) = \sigma_{2,2}(a,1)\,, \tag{9}$$

$$\sigma_{2,1}(a,b) - \sigma_{2,0}(a,b) = 0\,. \tag{10}$$

By definition of $\sigma_{m,j}$, the equation (10) can be rewritten as

$$0 = s_{2,2}(b)s_{2,1}\left(\frac{a}{b}\right) + s_{2,2}(b) = s_{2,2}(b)\left[s_{2,1}\left(\frac{a}{b}\right) + 1\right]. \tag{11}$$

Let us first consider $\zeta \in \mathbb{F}_{q^2}$ such that $s_{2,1}(\zeta) + 1 = 0$; i.e., $\zeta^q + \zeta = -1$ and then consider the straight line $x = y\zeta$. Now since $y^q + y = x^{q+1}$ then, the common points of this locus satisfies

$$y^q + y = (y\zeta)^{q+1}\,. \tag{12}$$

Lemma 3.2.1. *The polynomial $\theta_\zeta(T) = (\zeta T)^{q+1} - T^q - T$ is separable and has its roots in $\mathbb{F}_{q^2}$*

Proof. The polynomial $\theta_\zeta(T)$ satisfies

$$\theta_\zeta(T)^q - \theta_\zeta(T) = -(T^{q^2} - T)(\zeta^{q-1}T - 1)^q.$$

Now the lemma follows from

$$\theta_\zeta'(T) = (\zeta^{q+1}T - 1)^q,$$

and since $T = \zeta^{-(q+1)}$ is not a root of $\theta_\zeta(T)$. □

Remark 3.2.1. First observe that the equation (11) implies that $P_{0,0}$ is a zero of u [$s_{2,2}(b) = 0$ implies $b = 0 = a$]. On the other hand by Lemma 3.2.1 for each $\zeta \in \mathbb{F}_{q^2}$ such that $\zeta^q + \zeta = -1$ and for each root β of the polynomial $\theta_\zeta(T)$, the pair $(\zeta\beta, \beta)$ satisfies the equations (9) and (10), but $T = 0$ is zero of $\theta_\zeta(T)$ for all ζ, therefore $P_{0,0}$ is a multiple zero of u.

Lemma 3.2.2. *Let $P = P_{a,b}$ be a zero of u; then $t = x - a$ is a P-prime element, and $\nu_P(u) > 1$ iff $b = -\dfrac{a^2}{a+1}$.*

Proof. Denoting by δ_t the derivation of $F/\mathbb{F}_{q^2}$ with respect to t, then from the P-adic power series expansion of u with respect to t we have

$$\nu_P(u) > 1 \text{ iff } \frac{du}{dt}(P) = 0$$

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

$$\frac{du}{dt} = y^q\frac{dy}{dt} + y^q\frac{dx}{dt} + x^q\frac{dy}{dt}$$

implies $\dfrac{du}{dt}(P) = \left(ab + b + a^2\right)^q$. □

Lemma 3.2.3. $\nu_{P_{0,0}}(u) = 2q + 1$.

Proof. In order to prove that the multiplicity of $P = P_{0,0}$ is $q+1$ we compute the P-adic power series expansion of u with respect to $t = x$. We write $x = t$ and $y = \alpha_1 t + \alpha_2 t^2 + \ldots + \alpha_{q+1}t^{q+1} + \lambda$ with $\nu_P(\lambda) > q+1$ and $\alpha_i \in \mathbb{F}_{q^2}$. From the equation $y^q + y = x^{q+1}$ by comparing coefficients we obtain $y = t^{q+1} + \alpha_{q+2}t^{q+2} + \alpha$, therefore

$$\begin{aligned} u(x,y) &= x^q y + xy^q + y^{q+1} \\ &= (t^q)(t^{q+1} + \alpha_{q+2}t^{q+2} + \alpha) \\ &+ t(t^{q+1} + \alpha_{q+2}t^{q+2} + \alpha)^q + \omega \end{aligned}$$

with $\nu_P(\omega) > (q+1)^2$. □

3.2.2. **The genus and the number of rational places of $\mathbf{F}/\mathbb{F}_{q^2}$.** As in the section 3.1.2 we use (8) together with lemma 3.2.3 to compute the genus and the number of rational places of the function field $F/\mathbb{F}_{q^2}$.

Theorem 3.2.1. *The genus and the number of places of degree one of the function field $F/\mathbb{F}_{q^2}$ are given by*

$$g(F) = \frac{r(2q^2 - q - 1) - (q^2 - 1)}{2}$$

and

$$N(F) = r(q^3 - q^2) + (q^2 + 1)\,.$$

Proof. The proof is similar to (3.1.2.1), by (3.2.3) the only multiple zero of u is $P_{0,0}$, and we have $r_{P_{0,0}} = 1$; for the pole P_∞; $r_{P_\infty} = r$, and therefore the formula to genus follows of (8). To compute the number of rational places observe that if 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. The second case holds for the the pole P_∞ 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 $u(P) = \tau_2(a,b) \in \mathbb{F}_q$ and therefore, the polynomial $T^r - u(P)$ has r distinct roots in $\mathbb{F}_{q^2}$. Therefore there exist r extensions of degree one in F. For the pole, again let $t = \frac{x}{y}$ be an uniformizer to P_∞, then

$$u(x,y) = (xt)^{q+1} + t^q x^{q+1} + tx^{q+1}$$

and therefore all places lying over P_∞ are rational. □

Remark 3.2.2. For $q = 2$ and $r = 3$ we get $g(F) = 6$ and $N(F) = 17$ rational places, this value is close to the best value know of 20 rational points, however this curve was obtained by using methods from general class field theory and this method produces a mere existence result and not an explicit curve, see [2]. For $q = 3$ and $r = 4$ we get $g(F) = 24$ and $N(F) = 82$, the best value know is 91 and as before case this curve was obtained by using methods of class field theory based on Drinfeld modules of rank one, see [2].

Acknowledgements. The author deeply appreciates the helpful comments of the referee on this work.

References

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

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

[3] **H. Hasse**. *Theorie der relativ zyklischen algebraischen Funktionenkörper*, J. Reine Angew. Math **172** (1934), 37–54.

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

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

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

[7] **C. J. Moreno**. *Algebraic Curves over Finite Fields*, Cambridge Univ. Press, Cambridge, 1991.

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

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

Recibido el 2 de mayo de 2006

Aceptado para su publicación el 10 de agosto de 2006