PRODUCTOS FIBRADOS DE EXTENSIONES DE KUMMER Y ARTIN-SCHREIER

Adriana Alexandra Albarracín Mantilla[1] , Álvaro Garzón Rojas[2]

Resumen

Albarracín Mantilla, A. A., A. Garzón Rojas: Productos fibrados de extensiones de Kummer y Artin-Schreier. Rev. Acad. Colomb. Cienc. **34** (133): 513-520, 2010. ISSN 0370-3908.

En este artículo se construyen cuerpos de funciones algebraicas con cuerpo de constantes el cuerpo finito $\mathbb{F}_q$ cuyo número de lugares de grado uno es "grande" en comparación con su género. Dichos cuerpos de funciones resultan del producto fibrado de extensiones de Kummer y Artin-Schreier.

Palabras clave: cuerpos de funciones algebraicas, cuerpos finitos, lugares racionales, extensiones de Kummer, extensiones de Artin-Schreier.

Abstract

We construct algebraic function fields over the finite field $\mathbb{F}_q$ with many rational points with respect to their genus. The curves constructed are fibre products of Kummer and Artin-Schreier covers of the projective line.

Key words: algebraic function fields, finite fields, rational places, Kummer extensions, Artin-Schreier extensions.

1. Introducción

Sean $\mathbb{F}_q$ un cuerpo finito con $q = p^n$ elementos, $\overline{\mathbb{F}_q}$ una clausura algebraica de $\mathbb{F}_q$ y $f(x, y) \in \mathbb{F}_q[x, y]$ un polinomio absolutamente irreducible. Al conjunto de puntos

$$C_f = \{(\alpha, \beta) \in \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q} : f(\alpha, \beta) = 0\}$$

lo llamaremos *la curva algebraica afín inducida por el polinomio* $f(x, y)$. Los puntos $P = (\alpha, \beta) \in C_f$ tal que $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ los llamaremos *puntos racionales* de la curva C_f sobre $\mathbb{F}_q$ y $C_f(\mathbb{F}_q)$ denotará el conjunto de puntos racionales de la curva C_f.

1 Escuela de Matemática, Universidad Industrial de Santander, Bucaramanga, Santander, Colombia. Correo electrónico: sadrialba@matematicas.uis.edu.coetb.net.co.

2 Departamento de Matemáticas, Universidad del Valle, Cali, Valle, Colombia. Correo electrónico: alvarogr@univalle.edu.co

En 1940 **André Weil** [6] probó la hipótesis de Riemann para curvas sobre cuerpos finitos obteniendo como consecuencia de este resultado, una cota superior para el número de puntos racionales de una curva C de género g definida sobre un cuerpo finito de cardinalidad q, a saber:

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

Posteriormente, en 1980, **V. D. Goppa** ([6]) introdujo los llamados códigos geométricos, esto es, códigos inducidos por curvas algebraicas, también conocidos como *códigos geométricos de Goppa.* En la construcción de códigos geométricos se destacan principalmente, dos propiedades que debe tener una curva de tal forma que el código inducido tenga buenos parámetros, estas son:

1 . La curva debe ser explícita, es decir debe obtenerse mediante una ecuación de la forma $f(x, y) = 0$.
2 . El número de puntos racionales de dicha curva debe estar cercano a la cota de Weil.

A partir de este hecho algunos matemáticos empezaron a trabajar en el mejoramiento de la cota de Weil y muchos otros encaminaron esfuerzos hacia la construcción de curvas con muchos puntos racionales.

En este artículo se construyen curvas algebraicas (cuerpos de funciones algebraicas) sobre cuerpos finitos con muchos puntos racionales (lugares de grado uno) entendiendo por esto, que el número $N(F/\mathbb{F}_q)$ de puntos racionales satisface $a \leq N(F/\mathbb{F}_q) \leq b$, donde b es la cota de **Weil, Ihara** o **Serre** (véanse [7],[5]) para un cuerpo de funciones de género g y $a = b/\sqrt{2}$.

Dichas curvas serán obtenidas por medio de recubrimientos dobles de la recta proyectiva $\mathbb{F}_q(x)$ mediante extensiones de Kummer y Artin–Schreier, Para la construcción de las extensiones de Kummer utilizaremos el método desarrollado en ([2]) el cual explicaremos en la sección 2.1.1. Para las extensiones de Artin–Schreier desarrollamos un método que nos permitirá escoger de una manera adecuada una función racional que definirá nuestra extensión y que a su vez garantizará la existencia de un buen número de lugares de grado uno.

2. Recubrimientos dobles

En esta sección construiremos cuerpos de funciones algebraicas $E = E_1E_2$ con cuerpo de constantes el cuerpo finito $\mathbb{F}_q$ donde E_1 está definido por una ecuación de Kummer y E_2 por una de Artin–Schreier, (ver [8]). Tales cuerpos de funciones serán construidos de forma tal que el número de lugares de grado 1 esté cercano bien sea a las cotas de Weil, Serre o Ihara.

2.1. Construcción mediante extensiones de Kummer. Sean r un divisor de $q - 1$ y $\mu(x) \in \mathbb{F}_q(x)$ una función racional en x. Supongamos que el polinomio

$$\varphi(T) \in \mathbb{F}_q(x)[T] = T^r - \mu(x)$$

es irreducible en $\mathbb{F}_q(x)[T]$ y para cada $\alpha \in \mathbb{F}_q$ definamos

$$\varphi_\alpha(T) := T^r - \mu(\alpha) \in \mathbb{F}_q[T].$$

Observe que si existe un elemento $\beta \in \mathbb{F}_q$ tal que $\mu(\beta)$ es una r-ésima potencia en el cuerpo $\mathbb{F}_q$, esto es,

$$(\mu(\beta))^{(q-1)/r} \equiv 1 \bmod (q-1), \tag{2}$$

entonces el polinomio $\varphi_\beta(T)$ se factoriza en $\mathbb{F}_q[T]$como

$$\varphi_\beta(T) = (T - \theta)(T - \tau\theta) \cdots (T - \tau^{r-1}\theta)\,, \tag{3}$$

donde τ es una raíz r-ésima de la unidad y $\theta \in \mathbb{F}_q$ es tal que $\theta^r = \mu(\beta)$.

Sea y una raíz del polinomio $\varphi(T)$ y consideremos la curva algebraica afín sobre el cuerpo finito $\mathbb{F}_q$ definida por la ecuación $\varphi(y) = \mu(x)$.

Es claro que por cada elemento $\gamma \in \mathbb{F}_q$ que satisface la ecuación (2) obtenemos r puntos sobre la curva

$$C_\varphi = \{(\alpha, \beta) \in \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q} : \varphi(\alpha, \beta) = 0\},$$

cuyas coordenadas son del tipo $(\gamma, \tau^j\theta)$ con $0 \leq j \leq r - 1$, τ como en (3) y $\theta^r = \mu(\gamma)$. En resumen, por cada elemento $\gamma \in \mathbb{F}_q$ tal que $\mu(\gamma)$ sea una r-ésima potencia en $\mathbb{F}_q$, tendremos r puntos racionales en la curva C_φ.

Dado que en este trabajo usaremos el lenguaje de los cuerpos de funciones, el parágrafo anterior, puede ser reinterpretado como sigue:

El cuerpo de funciones algebraicas $E_1 = \mathbb{F}_q(x, y)$ definido por la ecuación de Kummer $\varphi(y) = y^r - \mu(x) = 0$, satisface:

$$|C_\varphi(\mathbb{F}_q)| \geq r \cdot |\Lambda_\mu|, \tag{4}$$

donde

$$\Lambda_\mu = \{\gamma \in \mathbb{F}_q\,;\, \mu(\gamma)\text{es una } r\text{-ésima potencia en } \mathbb{F}_q\}\,,$$

y $|C_\varphi(\mathbb{F}_q)|$ significará el cardinal del conjunto de lugares de grado uno (puntos racionales) del cuerpo de funciones E_1 (de la curva definida por la ecuación $\varphi(y) = 0$).

El número exacto de lugares de grado uno de E_1 resultará de sumar al número obtenido en (4) aquellos puntos de rama de la función $\mu(x)$, (esto es, aquellos lugares que son ceros ó polos de $\mu(x)$) que aporten lugares racionales .

2.1.1. Construcción de un $\mu(x) \in \mathbb{F}_q(x)$ apropiado. En esta sección describiremos brevemente un método desarrollado en ([2]) y ([3]) para la construcción de una función racional $\mu(x)$ de tal manera que el conjunto de elementos $\alpha \in \mathbb{F}_q$ tales $\mu(\alpha)$ sea una r-ésima potencia en $\mathbb{F}_q$ sea "grande".

Sean $f(x)$ y $\ell(x) \in \mathbb{F}_q[x]$ polinomios con las siguientes propiedades:

1. m.c.d.$(f(x), \ell(x)) = 1$ en $\mathbb{F}_q[x]$.
2. $\ell(x)$ tiene todas (o casi todas) sus raíces en $\mathbb{F}_q$
3. grad$(f(x)) \geq$ grad$(\ell(x))$

Por el algoritmo de la división existen $h(x), \mathcal{R}_\ell((f(x)) \in \mathbb{F}_q[x]$ tales que

$$f(x) = \ell(x)h(x) + \mathcal{R}_\ell((f(x))\,, \tag{5}$$

donde $\mathcal{R}_\ell((f(x))$ es el residuo de la división de $f(x)$ por $\ell(x)$. Ahora, definamos la función racional $\mu(x)$ como:

$$\mu(x) := \frac{f(x)}{\mathcal{R}_\ell((f(x))}. \tag{6}$$

Observe que para todo $\alpha \in \mathcal{V}_\ell := \{\alpha \in \mathbb{F}_q;\, \ell(\alpha) = 0\}$, se tiene que

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

Esto es, la función racional $\mu(x)$ toma el valor de 1 en el conjunto de ceros del polinomio $\ell(x)$ y puesto que en $\mathbb{F}_q$ existen todas las raíces r-ésimas de la unidad, entonces el cardinal del conjunto de lugares racionales del cuerpo de funciones E_1 dada por la ecuación de Kummer,

$$y^r = \mu(x) := \frac{f(x)}{\mathcal{R}_\ell((f(x))} \tag{7}$$

está íntimamente ligado al conjunto de ceros del polinomio $\ell(x)$ en el cuerpo finito $\mathbb{F}_q$.

Nótese que en el proceso de cálculo del número de lugares de grado 1 en el cuerpo de funciones $\mathbb{F}_q(x,y)/\mathbb{F}_q$ sólo hemos considerado los ceros del polinomio $\ell(x)$ en $\mathbb{F}_q$, otros lugares de grado 1 pueden obtenerse de los puntos de rama y además del conjunto

$$\{\alpha \in \mathbb{F}_q; \mu(\alpha) = \zeta^r\},$$

con $\zeta \in \mathbb{F}_q$, y $\zeta^r \neq 1$.

En general, los lugares de grado uno del cuerpo de funciones E_1 no provenientes de la ramificación, pueden obtenerse por el siguiente resultado, conocido como el teorema de Euler.

Proposición 2.1.1. *Sean p un número primo, $q = p^n$ y $\alpha \in \mathbb{F}_q$. La congruencia $x^r \equiv \mu(\alpha)\ (mod\ q)$ tiene $\kappa = m.c.d.(r, q-1)$ soluciones si y solamente si*

$$\mu(\alpha)^{(q-1)/\kappa} \equiv 1\ (mod\ q)\,. \tag{8}$$

De acuerdo con la proposición anterior, tenemos que

$$\#N(\mathbb{F}_q(x,y)/\mathbb{F}_q) = r \cdot grad(d(x)) + \rho. \tag{9}$$

donde $d(x)$ es el máximo común divisor entre $x^q - x$ y el numerador de la función racional $\mu(x)^{\frac{q-1}{r}} - 1$ y ρ es el número de lugares de grado uno obtenido de la ramificación de $\mu(x)$.

Como una ilustración de lo discutido anteriormente, sean $q = p^n$ con $n \geq 3$, $f(x)$ y $\ell(x)$ polinomios en $\mathbb{F}_p[x]$ tales que,

$$f(x) = (x^p - x)^{p^{n-1}-1} \qquad \text{y} \qquad \ell(x) = \frac{x^q - x}{x^p - x},$$

es fácil verificar que $f(x)$ y $\ell(x)$ satisfacen la siguiente relación

$$f(x) = \ell(x) - \frac{x^{p^{n-1}} - x}{x^p - x},$$

esto es,

$$\mathcal{R}_\ell((f(x)) = -\frac{x^{p^{n-1}} - x}{x^p - x}.$$

Proposición 2.1.2. *El cuerpo de funciones $E_1 = \mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ donde y satisface la ecuación de Kummer,*

$$\begin{array}{ccc} \mathbb{F}_q(x,y) & & \\ \downarrow & \searrow & y^r = \mu(x) = -\dfrac{(x^p - x)^{p^{n-1}-1}}{\dfrac{x^{p^{n-1}} - x}{x^p - x}} \\ \mathbb{F}_q(x) & \nearrow & \end{array}$$

tiene género

$$g = \frac{(p^{n-1} - p - 2)(r-1) + (p+1)(r-d)}{2}$$

donde $d = m.c.d.(r, p-1)$ y el número de lugares racionales satisface

$$\#N(E_1) \geq r \cdot (q - p).$$

Demostración. Los lugares P_α, correspondientes a $x-\alpha$ con $\alpha \in \mathbb{F}_p$ y el polo P_∞ de x, tienen índice de ramificación r/d, mientras que los lugares correspondientes a los ceros del polinomio $\mathcal{R}_\ell((f(x))$, estos son totalmente ramificados, con índice de ramificación $r-1$. Luego la fórmula para el género se sigue de ([8], 3.4.12).

Para el cálculo del número de lugares racionales, observe que todo elemento $\beta \in \mathbb{F}_q \setminus \mathbb{F}_p$ induce un lugar P_β en $\mathbb{F}_q(x)$ que es totalmente descompuesto en la extensión $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$, además aquellos lugares de $\mathbb{F}_q(x,y)$ que caen sobre P_β son racionales. Otros lugares de grado uno pueden obtenerse del análisis de la ramificación de $\mu(x)$. □

Ejemplo 2.1.1. Con $p=2$ y $n=3$ obtenemos que $f(x)=x^3(x+1)^3$ y $\ell(x)=x^6+x^5+x^4+x^3+x^2+x+1=(x^3+x^2+1)(x^3+x+1)$, luego el cuerpo de funciones $E_1=\mathbb{F}_8(x,y)/\mathbb{F}_8(x)$ está definido por la ecuación

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

cuyo género es

$$g=\frac{(4-2-2)6+3(6)}{2}=9.$$

En cuanto al número de lugares de grado uno sólo nos resta analizar los puntos de rama. Puesto que el grado de la extensión es primo, entonces todos los lugares serán ó totalmente ramificados ó no ramificados, de aquí que sólo aportan lugares racionales los correspondientes a $x=0$ $x=1$ y el polo de x en $\mathbb{F}_p(x)$. En resumen tenemos

$$\#N(E_1/\mathbb{F}_8(x))=7\cdot 6+3=45.$$

No se conoce un cuerpo de funciones definido sobre el cuerpo finito $\mathbb{F}_8$ de género 9, con más de 45 lugares de grado uno, ver ([5]).

Observación 2.1.1. Tomando $p=2$ y $n=4$ en la Proposición 2.1.2, obtenemos con $r=15$ un cuerpo de funciones de género $g=49$ y 213 lugares de grado uno, nuevamente es el mejor que se conoce. Con $p=3$ y $n=3$ tenemos, con $r=2$ un cuerpo de funciones maximal, esto es con 48 lugares de grado uno y con $r=13$ un cuerpo de funciones de género 48 y cuyo número de lugares de grado uno 316, este valor es cercano a la mejor cota existente que es 325, ver [5].

2.2. Construcción mediante extensiones de Artin–Schreier. El objetivo de esta sección es el de construir cuerpos de funciones $E_2=\mathbb{F}_q(x,z)/\mathbb{F}_q(x)$ definidos por medio de una ecuación de Artin–Schreier,

$$z^p-z=g(x), \tag{10}$$

con $g(x)\in\mathbb{F}_q(x)$ apropiado.

Como veremos, el problema de encontrar lugares de grado 1 en este tipo de extensiones está estrechamente relacionado con el Teorema 90 de Hilbert en su versión aditiva, más precisamente:

Teorema 2.2.1. *Sea F una extensión finita de $K=\mathbb{F}_q$. Entonces para $\alpha\in F$ tenemos $Tr_{F/K}(\alpha)=0$ si y sólo si $\alpha=\beta^p-\beta$ para algún $\beta\in F$. Donde $Tr_{F/K}$ es la función traza de F a K.* □

En efecto, observe que si $F=\mathbb{F}_{q=p^n}$ y $\alpha\in\mathbb{F}_q$ es tal que $Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(\alpha))=0$, entonces por (2.2.1) existe un $\beta\in\mathbb{F}_q$ tal que $\beta^p-\beta=g(\alpha)$, más aún, para cada elemento $\zeta\in\mathbb{F}_p$, se tiene que

$$(\beta-\zeta)^p-(\beta-\zeta)=\beta^p-\zeta^p-\beta+\zeta=g(\alpha)$$

esto es, por cada elemento en $\alpha\in\mathbb{F}_q$, tal que $Tr_{\mathbb{F}_q/\mathbb{F}_p}((g(\alpha))=0$ tendremos p puntos racionales (lugares de grado uno) en la curva C definida por la ecuación $z^p-z=g(x)$ (en el cuerpo de funciones definido por la ecuación de Artin–Schreier (10)).

Finalmente, para determinar el número de lugares de grado 1 de E_2 que no provienen de la ramificación de $g(x)$, es necesario analizar el polinomio $\delta(x)=$ m.c.d.$(Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(x)),x^q-x)$.

A continuación exhibiremos dos métodos para la construcción de la función racional $g(x)$ que definirá la extensión E_2.

2.2.1. Método 1. Sean $q=p^n$ y $\ell(x)\in\mathbb{F}_q[x]$ el cual es un producto de polinomios irreducibles de grado n sobre $\mathbb{F}_p$.

Si $t(x)$ y $\gamma(x)\in\mathbb{F}_q[x]$ tales que $t(x)$ es un factor de $\ell(x)$ y

$$\text{m.c.d}(\gamma(x)^p-\gamma(x),t(x))=1,$$

entonces existen polinomios $v(x)$ y $\omega(x)$ tales que

$$t(x)v(x)+(\gamma(x)^p-\gamma(x))\omega(x)=1\,; \tag{11}$$

dividiendo por $\omega(x)$ obtenemos:

$$\frac{t(x)v(x)}{\omega(x)}+(\gamma(x)^p-\gamma(x))=\frac{1}{\omega(x)}. \tag{12}$$

Ahora, si $\alpha \in \mathbb{F}_q$ es un cero de $t(x)$, entonces

$$0 = Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{\omega(\alpha)}\right)$$

y en consecuencia por (2.2.1), existe $\zeta \in \mathbb{F}_{p^n}$ tal que

$$\zeta^p - \zeta = \frac{1}{\omega(\alpha)}. \tag{13}$$

Observe que de acuerdo con la discusión anterior, debemos garantizar la existencia de un $\gamma(x) \in \mathbb{F}_q[x]$ tal que m.c.d. $(\gamma(x)^p - \gamma(x), t(x)) = 1$, esta existencia será justificada en el siguiente resultado.

Lema 2.1. *Con la notación anterior, si $\gamma(x) = (x - \alpha)$ con $\alpha \in \mathbb{F}_q$, entonces*

$$m.c.d\,(t(x), \gamma(x)^p - \gamma(x)) = 1.$$

Demostración. Dado que $\gamma(x) = (x - \alpha)$ con $\alpha \in \mathbb{F}_q$ entonces

$$\gamma(x)^p - \gamma(x) = (x - \alpha)^p - (x - \alpha) = x^p - x.$$

Si suponemos que $m.c.d\,(t(x), \gamma(x)^p - \gamma(x)) \neq 1$ entonces $(x^p - x)|t(x)$ y puesto que $t(x)$ es un factor de $\ell(x)$, tenemos que $(x^p - x)|\ell(x)$, pero $\ell(x)$ es un polinomio irreducible o producto de irreducibles sobre $\mathbb{F}_p$, con todos sus ceros en $\mathbb{F}_q \setminus \mathbb{F}_p$, entonces $x^p - x$ no puede dividir a $\ell(x)$ y en consecuencia

$$\text{m.c.d}\,(t(x), \gamma(x)^p - \gamma(x)) = 1\,. \qquad \square$$

2.2.2. Método 2. Sea $g(x) \in \mathbb{F}_q(x)$ una función racional en x, $h(x)$ el numerador de la función $Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(x))$ y $\ell(x)$ un divisor de m.c.d.$(h(x), x^q - x)$.

El cuerpo de funciones $E_2 = \mathbb{F}_q(x, z)$ será definido por medio de la ecuación de Artin–Schreier

$$z^p - z = g(x) \tag{14}$$

y denotaremos por $\delta(x) = \text{m.c.d.}(Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(x)), x^q - x)$.

Luego E_2 tendrá por lo menos $p \cdot \text{grad}(\delta(x))$ lugares de grado uno, en virtud del Teorema 2.2.1.

2.2.3. Aplicaciones de los Métodos 1 y 2. Como ilustración de los métodos exhibidos tenemos: Los polinomios

$$f(x) = (x^p - x)^{p^{n-1}-1} \qquad \text{y} \qquad \ell(x) = \frac{x^q - x}{x^p - x},$$

satisfacen la siguiente relación

$$\ell(x) \cdot 1 - (x^p - x) \cdot (x^p - x)^{p-2} \cdot \frac{(x^{p^{n-1}} - x)^p}{(x^p - x)^p} = 1. \tag{15}$$

Luego, de acuerdo con la ecuación (13), tenemos,

Proposición 2.2.1. *Para todo primo $p \neq 2$, el cuerpo de funciones $E_2 := \mathbb{F}_q(x, z)/\mathbb{F}_q(x)$ donde z satisface la ecuación de Artin–Schreier,*

$$\begin{array}{ccc} \mathbb{F}_q(x, y) & & \\ \Big\downarrow & \searrow & \\ & & z^p - z = h(x) := -\dfrac{(x^p - x)^2}{(x^{p^{n-1}} - x)^p} \\ & \nearrow & \\ \mathbb{F}_q(x) & & \end{array}$$

tiene género

$$g = (p - 1)\left(\left(\sum_{i=1}^{r} grad\,(h_i(x))\right) - 1\right)$$

donde $h_i(x)$ recorre todos los factores irreducibles del polinomio $h(x)$ y el número de lugares racionales satisface

$$\#N(E_2) \geq p \cdot (q - p)\,.$$

Demostración. En efecto, observe que todos los lugares $P_{h_i(x)}$ inducidos por los factores del polinomio $h(x)$ satisfacen $\nu_P(h(x)) = p$, luego por ([8], 3.3.7), existe un elemento $z \in \mathbb{F}_p(x)$ tal que

$$\nu_P(h(x) - z^p + z) \geq 0 \text{ ó } \nu_P(h(x) - z^p + z) = -m < 0\,,$$

con $m \not\equiv 0 (\text{mod } p)$. Tal elemento reductor z es:

$$z = \frac{\zeta(x)}{(x^p - x)h(x)}$$

donde $\zeta(x)^p = (x^p - x)^2$, (dicho z es obtenido usando el algoritmo 3.2.2 de [1], pág 39), obteniendo después de la reducción $\nu_P(h(x) - z^p + z) = -1$, ahora la fórmula para el género se obtiene de la fórmula de Hurwitz. El valor del número de puntos racionales es claro. $\square$

Observación 2.1. Observe que para $p = 2$ en (15)

$$\ell(x) \cdot 1 + (x^2 + x) \cdot \frac{(x^{2^{n-1}} + x)^2}{(x^2 + x)^2} = 1. \tag{16}$$

Luego nuestro cuerpo de funciones $E_2 := \mathbb{F}_{2^n}(x, z)/\mathbb{F}_2(x)$ esta definido por la ecuación

$$z^2 + z = \frac{(x^2 + x)}{(x^{2^{n-1}} + x)^2}$$

Ejemplo 2.2.3.1. (Método 1.) Sea $p = 2$ y $n = 3$. El cuerpo de funciones $E_2 := \mathbb{F}_8(x, z)/\mathbb{F}_2(x)$ definido a partir del método 1, está dado por la ecuación

$$z^2 + z = \frac{1}{(x^2 + x + 1)^2},$$

el cual tiene género 1 y 14 lugares de grado uno.

Ejemplo 2.2.3.2. (Método 2.) Sean $p = 2$, $n = 6$ y $g(x) = \dfrac{(x+1)^3}{x^3} \in \mathbb{F}_{64}(x)$. En este caso

$$Tr_{\mathbb{F}_{64}/\mathbb{F}_2}(g(x)) = \frac{1}{x^{96}}+\frac{1}{x^{64}}+\frac{1}{x^{48}}+\frac{1}{x^{24}}+\frac{1}{x^{12}}+\frac{1}{x^6}+\frac{1}{x^3}+\frac{1}{x},$$

y $\delta(x) = 1+x^6+x^{12}+x^{15}+x^{18}+x^{21}+x^{27}+x^{33}+x^{36}+x^{39}$.

Ahora consideremos el cuerpo de funciones $E_2 := \mathbb{F}_{64}(x,z)/\mathbb{F}_{64}(x)$ dado por la ecuación de Artin–Schreier

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

Este cuerpo de funciones tiene género 1 y 81 lugares de grado uno, esto es, E_2 es un cuerpo de funciones maximal.

2.3. Ejemplos de recubrimientos dobles. En esta sección construiremos un cuerpo de funciones $E = E_1E_2$ de tal forma que $E_1 = \mathbb{F}_q(x,y)$ está definido por una ecuación de Kummer del tipo (7) y $E_2 = \mathbb{F}_q(x,z)$ está definido por una ecuación del tipo (10).

Dado que estamos interesados en construir recubrimientos dobles cuyo número de lugares racionales sea "grande" es deseable que el máximo común divisor entre los polinomios $d(x)$ obtenido en la sección 2.1 y el polinomio $\delta(x)$ obtenido en la sección 2.2, tenga grado lo más grande posible, pues por cada cero común de estos polinomios tendremos $p \cdot r$ lugares racionales en la composición $E = E_1E_2$. Precisando lo anterior tenemos la siguiente proposición.

Proposición 2.3.1. *Sean $E = E_1E_2$ con E_1 y E_2 como antes. Si $\tau(x) = m.c.d.(d(x), \delta(x))$, entonces el número de lugares de grado uno del cuerpo de funciones E satisface*

$$\#N(E/\mathbb{F}_q) \geq p \cdot r(grad(\tau)). \qquad \square$$

Ejemplo 2.3.1. Sean E_1 y E_2 los cuerpos de funciones construidos en los ejemplos 2.1.1 y 2.2.3.1 respectivamente y sea $E = E_1E_2$. En este caso los polinomios $d(x)$ y $\delta(x)$ tiene como máximo común divisor a $\tau(x) = \delta(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, y en consecuencia

$$\#N(E/\mathbb{F}_8(x)) \geq 6 \cdot 2 \cdot 7 = 84.$$

Ahora analizamos los puntos de rama. Denotando por P_∞, P_1 y P_0 los lugares de grado uno en la extensión $\mathbb{F}_8(x,y)/\mathbb{F}_8(x)$ que caen sobre $x = \infty$, $x = 1$ y $x = 0$; observamos que existen 2 lugares en la extensión $\mathbb{F}_8(x,y,z)/\mathbb{F}_8(x,y)$ que caen sobre cada uno de ellos. Únicamente los lugares que caen sobre P_∞ son de grado 1.

De otro lado, sobre $P_{\zeta_i}, i = 1,2$ cae un lugar que no es de grado 1, por lo tanto tenemos sólo 2 lugares de grado uno provenientes de los puntos de rama y en consecuencia $\#N(E/\mathbb{F}_8(x)) = 86$.

Para el cálculo del género, observe que, el único lugar totalmente ramificado en $\mathbb{F}_8(x,y,z)/\mathbb{F}_8(x,y)$ es $P_{\zeta_i}, i = 1,2$, los lugares correspondientes a P_∞, P_0 y a P_1 son no ramificados y por lo tanto el género está dado por

$$g(\mathbb{F}_8(x,y,z)/\mathbb{F}_8(x)) = 2 \cdot 9 + \frac{1}{2}(-2+16) = 25.$$

No se conoce un cuerpo de funciones sobre $\mathbb{F}_8$ de género 25 que tenga más de 86 puntos racionales, ver [5].

Ejemplo 2.1. En este ejemplo construiremos un cuerpo de funciones algebraicas sobre el cuerpo finito $\mathbb{F}_{16}$, con género 20 y 127 lugares racionales. Este es el mejor valor conocido para $(16, 20)$

Sean $p = 2, n = 4, \ell(x) = x^8+x^7+x^6+x^4+1 \in \mathbb{F}_{16}[x]$ y $f(x) = (x^2+x+1)^4 \in \mathbb{F}_{16}[x]$.

Es fácil verificar que $\mathcal{R}_\ell((f(x)) = x^6(x+1)$. Afirmamos que la extensión de Kummer $E_1 = \mathbb{F}_{16}(x,y)$ de $\mathbb{F}_{16}(x)$ dada por la ecuación:

$$y^5 = \frac{f(x)}{\mathcal{R}_\ell((f(x))} = \frac{(x^2+x+1)^4}{x^6(x+1)},$$

tiene género 6 y 65 lugares de grado uno, es decir E_1 es un cuerpo de funciones maximal.

En efecto, para el cálculo del género, observe que los lugares correspondientes a $x = 0, x = 1, x = \infty$ y $x = \zeta_i$ con $\zeta_i^2 + \zeta_i + 1 = 0$ e $i = 1,2$ (los cuales denotaremos por p_0, p_1, p_∞ y p_{ζ_i} respectivamente) son totalmente ramificados, luego el género está dado por ([6], III.7.3.)

$$g(\mathbb{F}_{16}(x,y)/\mathbb{F}_{16}(x)) = 1+5(-1)+\frac{1}{2}(5(4)) = -4+10 = 6.$$

Para hallar el número de lugares de grado 1, resolvemos la congruencia (8) y obtenemos $d(x) = x^{12} + x^9 + x^6 + x^3 + 1$.

Observemos que $\ell(x) \cdot (x^4 + x^3 + 1) = d(x)$, donde los ceros del polinomio x^4+x^3+1 aportan quintas potencias diferentes de 1.

Entonces tenemos que

$$\#N(\mathbb{F}_{16}(x,y)) = 12 \times 5 + 5 = 65.$$

Este cuerpo de funciones es maximal puesto que

$$\#N(\mathbb{F}_{16}(x,y)) = q+1+2g\sqrt{q} = 16+1+2(6)(4) = 65.$$

Ahora sea $t(x) = x^4+x+1$ un factor de $\ell(x)$ y $\gamma(x) = x(x+1)^5$, es fácil comprobar que el polinomio $\omega(x)$ correspondiente a la expresión obtenida en (11) es $\omega(x) = x(x^2+x+1)$, luego el cuerpo de funciones E_2 dado por la ecuación de Artin–Schreier

$$z^2+z = \frac{1}{\omega(x)} = \frac{1}{x(x^2+x+1)},$$

tiene género 20 y 127 lugares de grado uno.

Antes de iniciar los cálculos, denotemos por P_0, P_1, P_∞ y P_{ζ_i} $i = 1,2$, los únicos lugares de E_1 que caen sobre p_0, p_1, p_∞ y p_{ζ_i} respectivamente

De acuerdo con ([8], 3.7.8) los únicos lugares que se ramifican en la extensión $\mathbb{F}_{16}(x,z)/\mathbb{F}_{16}$ son P_0 y P_{ζ_i}, mientras que los lugares P_∞ y P_1 son no ramificados, y por lo tanto, el género está dado por

$$g(\mathbb{F}_{16}(x,y,z)/\mathbb{F}_{16}(x)) = 2\cdot 6+\frac{1}{2}(-2+18) = 20.$$

Para el cálculo de lugares de grado uno, observe que existen 2 lugares en E_2 que caen sobre P_∞ y P_1, estos lugares son de grado 1, así como también aquellos que caen sobre P_0 y P_{ζ_i}, por lo tanto tenemos 7 lugares de grado uno provenientes de los puntos de rama.

De otro lado, puesto que $\delta(x) = (x+1)d(x)$ entonces $\tau(x) := \text{m.c.d}\,(d(x),\delta(x)) = d(x)$, y en consecuencia

$$\#N(E/\mathbb{F}_{16}(x)) = 5\cdot 2\cdot 12+7 = 127.$$

Ejemplo 2.3.2. Sean $p = 2$, $n = 3$ y $g(x) = x \in \mathbb{F}_8[x]$.

En este caso, $h(x) = Tr_{\mathbb{F}_8/\mathbb{F}_2}(g(x)) = x^4+x^2+x$, así, tomando $\ell(x) = x^4+x^2+x$ y $f(x) = (x^2+x+1)^2$ obtendremos un residuo $\mathcal{R}_\ell(f(x)) = x+1$.

La extensión de Kummer $E_1 = \mathbb{F}_8(x,y)$ de $\mathbb{F}_8(x)$ dada por la ecuación:

$$y^7 = \frac{f(x)}{\mathcal{R}_\ell((f(x))} = \frac{(x^2+x+1)^2}{(x+1)},$$

tiene género 6 y 30 lugares de grado uno.

Puesto que r es primo, sólo ocurre ramificación total, esto ocurre en los lugares p_1, p_{ζ_i} y p_∞, luego el género está dado por

$$g(\mathbb{F}_8(x,y)/\mathbb{F}_8(x)) = 1+7(-1)+\frac{1}{2}(4(6)) = -6+12 = 6.$$

Para hallar el número de lugares de grado 1, resolvemos la congruencia (8) y obtenemos $d(x) = x^4+x^2+x$.

Entonces tenemos que

$$\#N(\mathbb{F}_8(x,y)) = 4\cdot 7+2 = 30.$$

Ahora consideremos la extensión E_2 de E_1 dada por la ecuación de Artin-Schreier

$$z^2+z = x.$$

El único lugar totalmente ramificado es P_∞. Para el cálculo de lugares de grado uno, observemos que existen 2 lugares que caen sobre cada uno de los 7 lugares que caen sobre p_0, 2 lugares que caen sobre P_1 y $P_{\zeta_i}, i = 1,2$ respectivamente y solamente un lugar que cae sobre P_∞ que además es el único de grado 1, por lo tanto tenemos sólo un lugar de grado uno proveniente de los puntos de rama.

De otro lado, por la escogencia de $g(x)$ tenemos que $\delta(x) = \ell(x)$ y por lo tanto

$$\tau(x) = x^4+x^2+x.$$

Puesto que el polinomio $\tau(x)$ coincide con el polinomio $\ell(x)$, tenemos que

$$\#N(E/\mathbb{F}_8(x)) = 4\cdot 2\cdot 7+1 = 57.$$

No se conoce aún una curva (o su equivalente un cuerpo de funciones) sobre $\mathbb{F}_8$ de género 15 con más de 57 lugares de grado uno.

Ejemplo 2.3.3. En este ejemplo construiremos dos cuerpos de funciones maximales sobre el cuerpo finito $\mathbb{F}_{64}$.

Sean $\ell(x) = x^6+x^5+1$ y $f(x) = (x^2+x)^6$. Para esta escogencia obtenemos $\mathbb{R}_{\ell_1}(f(x)) = 1$. El cuerpo de funciones $E_1 := \mathbb{F}_{64}(x,y)/\mathbb{F}_{64}(x)$ definido por la ecuación de Kummer:

$$y^9 = \frac{f(x)}{\mathbb{R}_{\ell_1}(f(x))} = x^5(x+1),$$

tiene género 3 y 113 lugares racionales. En efecto, resolviendo la congruencia (8) obtenemos que $d(x) = x^{12}+x^6+x^4+x^3+x^2+x+1 = (x^3+x+1)(x^3+x^2+1)\ell(x)$, luego

$$\#N(\mathbb{F}_{64}(x,y)) = 12\cdot 9+5 = 113.$$

Ahora consideremos la extensión E_2 de E_1 (véase el Ejemplo 2.2.3.2) dada por la ecuación de Artin–Schreier

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

El único lugar totalmente ramificado es P_0 y los lugares correspondientes a P_∞ y P_1 son no ramificados y por lo tanto el género está dado por

$$g(\mathbb{F}_{64}(x,y,z)/\mathbb{F}_{64}(x)) = 2 \cdot 3 + \frac{1}{2}(-2+10) = 10.$$

Para el cálculo de lugares de grado uno, observemos que existen 2 lugares que caen sobre cada uno de los 3 lugares correspondientes a P_∞, 2 lugares que caen sobre P_1 y únicamente un lugar que cae sobre P_0 y todos son de grado 1, por lo tanto tenemos 9 lugares de grado uno provenientes de los puntos de rama.

Ahora, luego de hacer los respectivos cómputos, obtenemos que los lugares de grado uno en la extensión E que no provienen de la ramificación son precisamente aquellos $P_{\alpha,\beta,\gamma}$ donde α es un cero del polinomio $d(x)$, esto implica que

$$\#N(E/\mathbb{F}_{64}(x)) = 12 \cdot 2 \cdot 9 + 9 = 225.$$

Este cuerpo de funciones es maximal puesto que

$$\#N(\mathbb{F}_{64}(x,y,z)) = q+1+2g\sqrt{q} = 64+1+2(10)(8) = 225.$$

Referencias

[1] **R. Fraatz**, *Computation of Maximal Orders of Cyclic Extensions of Function Fields.* PhD Thesis. Universität Berlin, 2005.

[2] **A. Garcia and A Garzón**, *On Kummer Covers whith many Points.* J.P.A.A. **185** (2003), 177–192

[3] **A. Garcia and L. Quous**, *A construction of curves over finite fields.* Acta Arithmetica, **98** (2001), 181–195.

[4] **G. van der Geer & M. van der Vlugt**, *Kummer covers with many points.* Finite Fields and their applications **6** (4) (2000), 327–341.

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

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

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

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

Recibido el 19 de julio de 2009

Aceptado para su publicación el 15 de marzo de 2010