Uma familia de curvas maximais não recobertas pela curva Hermitiana

Arnoldo Teherán Herrera

IMECC
UNIVERSIDADE ESTADUAL DE CAMPINAS

Seminário de álgebra

Doutorado Matemáticas aplicadas
Unicamp

Março de 2014

1. Preliminares
   - Curvas maximais e a curva Hermitiana
   - Recobrimentos
   - A curva *GK*
   - A curva *GGS*

2. Uma familia de curvas maximais não recobertas pela curva Hermitiana
   - Definição e maximalidade
   - χ não é recoberta pela Hermitiana
   - χ não é Galois recoberta pela Hermitiana

Curvas maximais e a curva Hermitiana

$\mathbb{F}_{q^2}$ o corpo finito com q^2 elementos, onde q uma potencia de um primo p.

$\mathcal{C}$ uma curva sobre $\mathbb{F}_{q^2}$, i.e, $\mathcal{C}$ é projetiva, não singular e geometricamente irredutivel sobre $\mathbb{F}_{q^2}$.

$N(\mathcal{C}(\mathbb{F}_{q^2}))$ o conjunto de $\mathbb{F}_{q^2}-$ pontos racionais

$g := g\,(\mathcal{C})$ o gênero de $\mathcal{C}$

Cota de Hasse-Weil: $\#N(\mathcal{C}(\mathbb{F}_{q^2})) \leq 1 + q^2 + 2qg$

$\mathcal{C}$ é $\mathbb{F}_{q^2}-$ **maximal** se $\#N(\mathcal{C}(\mathbb{F}_{q^2})) = 1 + q^2 + 2qg$

Se $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal então $g \leq \frac{1}{2}q(q-1)$.

Se $n \in \mathbb{Z}^+$ é impar, então $\mathcal{C}$ é $\mathbb{F}_{q^{2n}}-$ maximal.

Curvas maximais e a curva Hermitiana

A curva **Hermitiana** sobre $\mathbb{F}_{q^2}$: $\mathcal{H}_q : X^q + X = Y^{q+1}$.

1. $g\left(\mathcal{H}_q\right) = \frac{1}{2}q(q-1)$
2. $\#N(\mathcal{H}_q(\mathbb{F}_{q^2})) = 1 + q^3$
3. $\mathcal{H}_q$ é $\mathbb{F}_{q^2}$ - maximal.
4. $\mathcal{H}_q$ é a única curva $\mathbb{F}_{q^2}-$ maximal com gênero $g = \frac{1}{2}q(q-1)$.

Dem. [10], [9] ■

Teorema

Se uma curva $\mathcal{C}$ esta contida numa $\mathbb{F}_{q^2}-$ variedade Hermitana então $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal.

Dem. ver [11], Korchmaros, Torres.■

Recobrimentos

Definição

Se $\mathcal{C}_1$ *e* $\mathcal{C}_2$ *são curvas sobre* $\mathbb{F}_{q^2}$. *Um* $\mathbb{F}_{q^2}-$ *morfismo sobrejetivo,* $\varphi : C_1 \to C_2$ *é chamado* $\mathbb{F}_{q^2}-$ **recobrimento** *de* $\mathcal{C}_1$ *em* $\mathcal{C}_2$.
Em termos de corpos isto significa que $\mathbb{F}_{q^2}(\mathcal{C}_2) \subseteq \mathbb{F}_{q^2}(\mathcal{C}_1)$

$\mathcal{C}_1$ **recobre** *à curva* $\mathcal{C}_2$, *também que* $\mathcal{C}_2$ **recoberta** *pela curva* $\mathcal{C}_1$.

φ *é* **recobrimento de Galois** *se* $\mathbb{F}_{q^2}(\mathcal{C}_1) | \mathbb{F}_{q^2}(\mathcal{C}_2)$ *é uma extensão de Galois*

φ *tem* **grau finito** d *se* $\mathbb{F}_{q^2}(\mathcal{C}_1) | \mathbb{F}_{q^2}(\mathcal{C}_2)$ *tem grau finito* d.

Teorema

Toda curva recoberta por uma curva $\mathbb{F}_{q^2}-$ *maximal é* $\mathbb{F}_{q^2}-$ *maximal.*

Dem. [8], Lachaud.■

Recobrimentos

Teorema

Se $\mathcal{C}$ é uma curva $\mathbb{F}_{q^2}-$ maximal e $g(\mathcal{C}) > \dfrac{q^2 - q + 4}{6}$, então $\mathcal{C}$ é recoberta pela curva Hermitiana.

Dem. [6], Garcia, Torres.■

Teorema

Seja $\mathcal{C}$ uma curva $\mathbb{F}_{q^2}-$ recoberta pela curva Hermitiana $\mathcal{H}_q$; se $\phi : \mathcal{H}_q \longrightarrow \mathcal{C}$ é um $\mathbb{F}_{q^2}-$ recobrimento de grau d, então

$$\frac{\#\mathcal{H}_q\left(\mathbb{F}_{q^2}\right)}{\#\chi\left(\mathbb{F}_{q^2}\right)} \leq d \leq \frac{2g\left(\mathcal{H}_q\right) - 2}{2g\left(\chi\right) - 2}$$

Recobrimentos

Em particular, toda curva recoberta pela curva Hermitiana $\mathcal{H}_q$ é $\mathbb{F}_{q^2}-$ maximal.

É verdadeiro a reciproca?, i.e, se $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal então $\mathcal{C}$ é recoberta pela curva Hermitiana $\mathcal{H}_q$?

Na teoria, todas as curvas maximais obtidas eram sempre **curvas maximais recobertas pela curva Hermitiana**, por exemplo [2], Cossidente, Korchmáros, Torres.

Posteriormente foi encontrada uma curva que não era **Galois recobertas pela curva Hermitiana**, [4], Garcia, Stichtenoth.

A curva *GK*

Curva *GK* (Giulietti - Korchmáros, 2009, [7]) p primo, seja $q = p^h$ com $h \in \mathbb{Z}^+$; a curva *GK* é definida como a intersecção das superficies contida em $\mathbb{P}^3$ sobre $\mathbb{F}_{q^6}$, com equações afins:

$$x^q + x = y^{q+1} \quad \text{e} \quad yh(x) = z^{\frac{q^3+1}{q+1}},$$

com $h(x) = \sum_{i=0}^{q} (-1)^{i+1} x^{i(q-1)}$, portanto $(x^q + x)\, h(x) = x^{q^2} - x$.

1. A curva *GK* é absolutamente irredutivel sobre $\mathbb{F}_{q^6}$ e não singular.
2. *GK* esta contida na variedade $\mathbb{F}_{q^6}-$ Hermitiana sobre com equação afim

$$X^{q^3} + X = Y^{q^3+1} + Z^{q^3+1},$$

portanto é $\mathbb{F}_{q^6}-$ maximal.

A curva GK

1. O gênero é

$$g\left(GK\right) = \frac{\left(q^3+1\right)\left(q^2-2\right)}{2} + 1,$$

2. Para $q > 2$ a curva GK não é $\mathbb{F}_{q^6}-$ recoberta pela curva Hermitiana.
3. Este é até agora o único exemplo existente na teoria, com a propriedade anterior.

A curva GGS

([5],Garcia - Güneri - Stichtenoth, 2010), q uma potencia de p, $n \in \mathbb{Z}^+$ impar com $n \geq 3$:

$$x^q + x = y^{q+1} \quad \text{e} \quad y^{q^2} - y = z^{\frac{q^n+1}{q+1}},$$

- Para cada $n \geq 3$: $\mathcal{C}_n$ é $\mathbb{F}_{q^{2n}}-$ maximal com gênero

$$g\left(\mathcal{C}_n\right) = \frac{(q-1)\left(q^{n+1} + q^n - q^2\right)}{2},$$

- Para $n = 3$, $\mathcal{C}_3$ e a curva GK sao $\mathbb{F}_{q^6}-$ isomorfas.
- Para $n > 3$ e $q > 2$, $\mathcal{C}_n$ não é $\mathbb{F}_{q^{2n}}-$ Galois recoberta pela curva Hermitiana, ver [3], Duursma, Mak.

A curva *GGS*

Observação

- *A equação* $y^{q^2} - y = z^{\frac{q^n+1}{q+1}}$, *é* $\mathbb{F}_{q^{2n}}-$ *maximal para cada n impar [1], Abdón Bezerra, Quoos.*
- *Se* $n = q = 3$: $y^9 - y = z^7$ *é* $\mathbb{F}_{3^6}-$ *maximal com gênero* $g = 24$ *e não é* $\mathbb{F}_{3^6}-$ *Galois recoberta pela curva Hermitiana, [4], Garcia, Stichtenoth.*
- $x^q + x = y^{q+1}$ *é* $\mathbb{F}_{q^2}-$ *maximal e portanto é* $\mathbb{F}_{q^{2n}}-$ *maximal.*
- *Temos duas curvas* $\mathbb{F}_{q^{2n}}-$ *maximais, cujo produto fibrado é uma curva* $\mathbb{F}_{q^{2n}}-$ *maximal.*
- *Em geral isto não sempre ocorre, por exemplo, para q impar, seja*

$$\mathcal{C} : \begin{cases} y^{q^2} - y & = & z^{\frac{q^n+1}{q+1}} \\ x^q + x & = & y^{(q+1)/2}, \end{cases}$$

Em particular, para $q = n = 3$, *obtemos* $g(\mathcal{C}) = 85$ *e* $\#\mathcal{C}(\mathbb{F}_{3^6}) = 2296$.

Definição e maximalidade

$a, b, s, n \in \mathbb{Z}^+$

$n \geq 3$ impar,

$q = p^a$, com p primo.

$N = \frac{q^n+1}{q+1}$

Supor b/a, s/N

$M := \frac{N}{s}$

$a = \ell b$

$c \in \mathbb{F}_{q^2}$, com $c \neq 0$ tal que $c^q + c = 0$.

$$t(x) := \sum_{i=0}^{\ell-1} x^{p^{bi}}$$

Definição e maximalidade

$\mathcal{C}_n : u^q + u = v^{q+1}$ e $v^{q^2} - v = w^{\frac{q^n+1}{q+1}}$.

Defina-se o morfismo da curva GGS em $\mathbb{P}^3$:

$$\begin{array}{cccc} \varphi : & \mathcal{C}_n & \longrightarrow & \mathbb{P}^3 \\ & (u,v,w,1) & \longmapsto & \left(cu - (cu)^{p^b}, v, w^s, 1\right) \end{array}$$

e Seja $\chi_{a,b,n,s} := \chi$ o modelo não singular de $\varphi(\mathcal{C}_n)$ sobre $\mathbb{F}_{q^{2n}}$.

$$\chi : \begin{cases} cy^{q+1} & = & t(x) \\ z^M & = & y^{q^2} - y \end{cases}$$

Teorema

A curva χ é $\mathbb{F}_{q^{2n}}-$ maximal, com gênero

$$g(\chi) = \frac{q^{n+2} - p^b q^n - sq^3 + q^2 + (s-1)p^b}{2sp^b}$$

Definição e maximalidade

Dem. χ é $\mathbb{F}_{q^{2n}}-$ birracionalmente equivalente como a curva plana

$$\gamma : cz^{\frac{q^n+1}{s}} = t(x)\left(t(x)^{q-1}+1\right)^{q+1},$$

γ é um recobrimento de Kummer de $\mathbb{P}^1$, de grau $\frac{q^n+1}{s} = (q+1)M$

$F = \mathbb{F}_{q^{2n}}(\gamma) = \mathbb{F}_{q^{2n}}(x, z)$

$K = \mathbb{F}_{q^{2n}}(x)$

$t(x) = tr_{\mathbb{F}_q/\mathbb{F}_{p^b}}(x)$

$u := t(x)\left(t(x)^{q-1}+1\right)^{q+1}$

Definição e maximalidade

Para $\mathcal{P} \in \mathbb{P}_K$:

$$v_{\mathcal{P}}(u) = \begin{cases} 1 & \text{se} \quad \mathcal{P} = \mathcal{P}_\alpha \text{ com } \alpha \text{ zero de } t(x) \\ q+1 & \text{se} \quad \mathcal{P} = \mathcal{P}_\beta \text{ com } \beta \text{ zero de } t(x)^{q-1} + 1 \\ -\frac{q^3}{p^b} & \text{se} \quad \mathcal{P} = \mathcal{P}_\infty \text{ o polo de } x \text{ em } K \\ 0 & \text{se} \quad \mathcal{P} \neq \mathcal{P}_\alpha, \mathcal{P}_\beta, \mathcal{P}_\infty \end{cases}$$

$$r_{\mathcal{P}}(u) = \begin{cases} 1 & \text{se} \quad \mathcal{P} = \mathcal{P}_\alpha \text{ com } \alpha \text{ zero de } t(x) \\ q+1 & \text{se} \quad \mathcal{P} = \mathcal{P}_\beta \text{ com } \beta \text{ zero de } t(x)^{q-1} + 1 \\ 1 & \text{se} \quad \mathcal{P} = \mathcal{P}_\infty \text{ o polo de } x \text{ em } K \\ [F:K] & \text{se} \quad \mathcal{P} \neq \mathcal{P}_\alpha, \mathcal{P}_\beta, \mathcal{P}_\infty \end{cases}$$

Formula do gênero de Riemman - Hurwitz:

$$2g(F) - 2 = [F:K](2g(K) - 2) + \sum_{\mathcal{P} \in \mathbb{P}_K} ([F:K] - r_{\mathcal{P}}),$$

Definição e maximalidade

$g(K) = 0$

$[F : K] = \frac{q^n+1}{s} = (q+1) M$

$g(F) = g(\chi)$

$$g(\chi) = \frac{q^{n+2} - p^b q^n - sq^3 + q^2 + (s-1) p^b}{2sp^b}$$

■

χ não é recoberta pela Hermitiana

Teorema

Se $n = 3$, $s = 1$, $a \geq 3$ e $q > p^b + p^{2b}$, a curva χ não é $\mathbb{F}_{q^6}-$ recoberta pela curva Hermitana.

Dem.

$$g(\chi) = \frac{1}{2sp^b}\left(q^{n+2} - p^b q^n - sq^3 + q^2 + (s-1)\,p^b\right),$$

$$\#\chi\left(\mathbb{F}_{q^{2n}}\right) = \frac{q^{2n+2} + p^b(s-1)q^{2n} - sq^{n+3} + q^{n+2} + (s-1)p^b q^n + sp^b}{sp^b},$$

$$g\left(\mathcal{H}_{q^n}\right) = \frac{1}{2}\left(q^{2n} - q^n\right),$$

$$\#\mathcal{H}_{q^n}\left(\mathbb{F}_{q^{2n}}\right) = q^{3n} + 1.$$

Supor $\phi : \mathcal{H}_{q^n} \longrightarrow \chi$ um $\mathbb{F}_{q^{2n}}-$ recobrimento de grau d.

χ não é recoberta pela Hermitiana

$$\frac{\#\mathcal{H}_{q^n}\left(\mathbb{F}_{q^{2n}}\right)}{\#\chi\left(\mathbb{F}_{q^{2n}}\right)} \leq d \leq \frac{2g\left(\mathcal{H}_{q^n}\right)-2}{2g\left(\chi\right)-2}$$

Se $n = 3$, $s = 1$:

$$\frac{\#\mathcal{H}_{q^n}\left(\mathbb{F}_{q^{2n}}\right)}{\#\chi\left(\mathbb{F}_{q^{2n}}\right)} = p^b q + u$$

$$\frac{2g\left(\mathcal{H}_{q^n}\right)-2}{2g(\chi)-2} = p^b q + v$$

$$u = \frac{p^b q^7 - p^b q^6 - p^{2b} q + p^b}{q^8 - q^6 + q^5 + p^b} \qquad \text{e} \qquad v = \frac{p^{2b} q^4 + p^b q^4 - 2p^b q^3 + 2p^{2b} q - 2p^b}{q^5 - p^b q^3 - q^3 + q^2 - 2p^b}$$

Se $q > p^b + p^{2b}$ e $a \geq 3$:

$u > 0$ e $v < 1$, contradição. ■

χ não é Galois recoberta pela Hermitiana

Teorema

Seja γ *uma curva* $\mathbb{F}_{q^{2n}}-$ *maximal, suponha que existem* $A, B \in \mathbb{Z}^+$, $k \in \mathbb{R}^+$ *tais que*

- $2g(\gamma) - 2 = A(q^n + 1) - B$,
- $1 \leq B \leq q^n + 1$,
- $k(A + 1) < B$,
- $A + 2 < B$.

Se existe um $\mathbb{F}_{q^{2n}}-$ *recobrimento de Galois* $\phi : \mathcal{H}_{q^n} \longrightarrow \gamma$, *então*

$$grau(\phi)\, B \geq (k + 1)(q^n + 1).$$

Dem. Ver [3], Duursma, Mak, Proposição 5.1.■

Teorema

Se $n > 3$, $s = 1$ *a curva* χ *não é* $\mathbb{F}_{q^{2n}}-$ *Galois recoberta pela curva Hemitana* $\mathcal{H}_{q^n}$.

χ não é Galois recoberta pela Hermitiana

Dem.

$2g(\chi) - 2 = A(q^n + 1) - B,$

$A = \frac{1}{p^b}\left(q^2 - p^b\right),$

$B = \frac{1}{p^b}\left(q^3 + p^b\right),$

$A + 2 = \frac{1}{p^b}\left(q^2 + p^b\right) < \frac{1}{p^b}\left(q^3 + p^b\right) = B,$

para cada $n \geq 3 : 1 \leq B \leq q^n + 1,$

$k = q :$

$k(A + 1) < B.$

Supor $\phi : \mathcal{H}_{q^n} \longrightarrow \chi$ um $\mathbb{F}_{q^{2n}}-$ recobrimento de Galois de grau d

χ não é Galois recoberta pela Hermitiana

$$d \geq \frac{(k+1)(q^n+1)}{B} = p^b q^{n-2} + u$$

$$d \leq \frac{2g\left(\mathcal{H}_{q^n}\right)-2}{2g(\chi)-2} = p^b q^{n-2} + v$$

$$u = \frac{p^b q^n - p^{2b} q^{n-2} + p^b q + p^b}{q^3 + p^b}$$

$$v = \frac{p^{2b} q^{2n-2} + p^b q^{n+1} - 2p^b q^n + 2p^{2b} q^{n-2} - 2p^b}{q^{n+2} - p^b q^n - q^3 + q^2 - 2p^b}$$

$$u \leq v$$

$$q^{2n+2} + 2q^{n+3} + 2q^{n+2} + 2q^3 + q^2 \leq p^b q^{2n+1} + 2p^b q^{2n} + q^{n+4} + 3p^b q^{n+1} + 2p^b q^n + q^4 + 2p^b$$

que é falso para $n > 3$. ■

Bibliografia: I

- M. Abdón J. Bezerra, L. Quoos; *Further examples of maximal curves*, Journal of Pure and Applied Algebra, pp. 1192 - 1196, 2009.
- A. Cossidente, G. Korchmáros, F. Torres; *On curves covered by the Hermitian curve*, J. Algebra 216, 56–76, 1999.
- I. Duursma, K. Mak; *On maximal curves which are not Galois subcovers of the Hermitian curve*, Bulletin of the Brazilian Mathematical Society, New Series 43, 453–465, 2012.
- A. Garcia, H. Stichtenoth; *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bull Braz Math Soc, New Series 37, 139–152, 2006.
- A. Garcia, C. Güneri, H. Stichtenoth; *A generalization of the Giulietti-Korchmaros maximal curve*, Adv. Geom, 10, 427–434, 2010.
- A. Garcia, F. Torres; *On unramified coverings of maximal curves*, Séminaires et Congrés SMF, 2009, v. 21, p. 35-42
- M. Giulietti, G. Korchmáros; *A new family of maximal curves over a finite field*, Math. Ann 343, 229–245, 2009.

Bibliografia: II

G. Lachaud; *Sommes d'Eisenstein et Nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris 305, Serie I, 729–732, 1987.

H. Ruck, H. Stichtenoth; *A Characterization of Hermitian Function Fields over Finite Fields*, J. Reine Angew. Math 457, 185–188, 1994.

H. Stichtenoth; *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

G. Korchmaros, F. Torres *Embedding of a maximal curve in a Hermitian variety*, Compositio Math. 128 (2001), no. 1, 95-113.