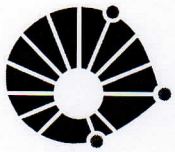
Arnoldo Rafael Teheran Herrera

Sobre curvas maximais não recobertas pela curva Hermitiana

CAMPINAS
2014



UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

ARNOLDO RAFAEL TEHERAN HERRERA

SOBRE CURVAS MAXIMAIS NÃO RECOBERTAS PELA CURVA HERMITIANA

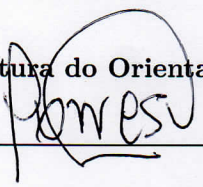
Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em matemática aplicada.

Orientador: Fernando Eduardo Torres Orihuela

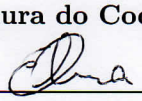
Coorientador: Ercílio Carvalho da Silva

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO ARNOLDO RAFAEL TEHERAN HERRERA, E ORIENTADA PELO PROF. DR. FERNANDO EDUARDO TORRES ORIHUELA.

Assinatura do Orientador



Assinatura do Coorientador



CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

T233s

Teheran Herrera, Arnoldo Rafael, 1968-
Sobre curvas maximais não recobertas pela curva hermitiana / Arnoldo Rafael Teheran Herrera. – Campinas, SP : [s.n.], 2014.

Orientador: Fernando Eduardo Torres Orihuela.
Coorientador: Ercílio Carvalho da Silva.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

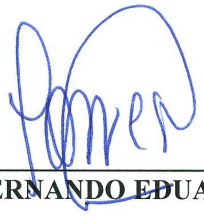
1. Curva maximal. 2. Curva hermitiana. I. Torres Orihuela, Fernando Eduardo,1961-. II. Silva, Ercílio Carvalho da. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Over maximal curves cannot be covered by the hermitian curve
Palavras-chave em inglês:
Maximal curve
Hermitian curve
Área de concentração: Matemática Aplicada
Titulação: Doutor em Matemática Aplicada
Banca examinadora:
Fernando Eduardo Torres Orihuela [Orientador]
Herivelto Martins Borges Filho
José Gilvan de Oliveira
Alonso Sepúlveda Castellanos
Luciane Quoos Conte
Data de defesa: 06-08-2014
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 06 de agosto de 2014 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.



Prof(a). Dr(a). FERNANDO EDUARDO TORRES ORIHUELA

Prof(a). Dr(a). HERIVELTO MARTINS BORGES FILHO

Prof(a). Dr(a). JOSÉ GILVAN DE OLIVEIRA

Prof(a). Dr(a). ALONSO SEPÚLVEDA CASTELLANOS

Prof(a). Dr(a). LUCIANE QUOOS CONTE

Abstract

In this thesis we work out exemples of maximal curve wich are not covered by the corresponding Hermitian curve. These exemples arise as covered curves of the called GK curve. We also construct exemples of maximal array which cannot be Galois covered by the corresponding Hermitian curve. Finally we stay some applications to coding theory.

Keywords: maximal curve, Hermitian curve, GK curve, GGS curve.

Resumo

Apresentamos nesta tese exemplos de curvas maximais que são obtidos usando recobrimentos da curva GK definida por Giulietti e Korchmáros. Demonstraremos que em alguns casos estas curvas generalizam uma propriedade fundamental da curva GK, ou seja, que elas não são recobertas pela curva Hermitiana correspondente; em outros casos também mostraremos exemplos de curvas que não podem ser Galois recobertas pela curva Hermitiana. Adicionalmente também apresentamos algumas aplicações, especialmente usaremos as curvas construídas para calcular alguns AG códigos num ponto racional; estes serão construídos usando certo semigrupo telescópico no ponto racional da curva correspondente. Finalmente compararemos os parâmetros obtidos de nossos exemplos, com os parâmetros dos códigos existentes na literatura.

Palavras-chave: curva maximal, curva Hermitiana, curva GK, curva GK generalizada.

Sumário

Em memória de minha filha Lina Maria....
Para minhas filhas Arleth Patricia e Maria Juliana....
Para minha esposa Mercaluz....

Agradecimentos

Agradeço primeiramente a Deus, por estar sempre presente na minha vida, por ter me dado saúde, força e esperança nos momentos difíceis desta caminhada, permitindo conquistar mais este objetivo.

Ao meu amigo e orientador Fernando Torres, por seu tempo, paciência, compreensão e dedicação na orientação desta tese. A Ercílio Carvalho da Silva pela coorientação desta tese.

Também agradeço ao professor Saeed Tafazolian, seus magníficos comentários foram fundamentais no desenvolvimento deste trabalho. Aos professores da banca examinadora Herivelto Borges, Gilvan de Oliveira, Alonso Sepúlveda e Luciane Qoous por todas suas sugestões e contribuições com o intuito de melhorar este estudo. Aos colegas do seminário de curvas algébricas, Steve Vicentim, Paulo César de Oliveira, Nazar Arakelian, Matheus Bernardini de Souza e Wanderson Tenório, por seu tempo para me escutar, por seus valiosos comentários sobre o trabalho e a sincera amizade. Aos creadores de *Magma Computational Algebra System* e à professora Beatriz Motta por me falar desta ferramenta computacional. Ao professor Massimo Giulietti pela revisão dos primeiros resultados deste trabalho.

A minha família pelo constante apoio e incentivo para seguir sempre em frente e conquistar meu sonho . Especialmente para Mercaluz pelo amor, carinho e companheirismo, por estar sempre presente em todo momento. A Maria Juliana e Arleth Patricia meus dois amores e motivações nesta vitória. A minha mãe, irmãos e sobrinhos.

Às colegas Sonia Sabogal, Adriana Alexandra Albarracín, a meu mestre Álvaro Garzón, e meu sogro José Hernandez, pela confiança depositada nesta aventura, sem eles esta conquista tinha sido impossível. Á universidade Industrial de Santander em Colômbia pela financiação deste doutorado.

Aos amigos na qual tive a oportunidade de conhecer nesta etapa de minha vida, especialmente a Gina Paola Vera Rizzo e Jeffrey León Pulido por me receber na chegada a Campinas. À família Cristovão Matesco por todos os momentos compartilhados. A Jairo Ayala e Angela Franco por sua ajuda e amizade. A Juan Gabriel Galeano, Blas Meléndez Caraballo, Kelly Madrid Cadena, Julián Acuña Collazos, John Alexander Perez Sepúlveda e sua família, Adrián Ricardo Gómez Plata e sua família, Miller Ceron Gómez e sua família, Abel Alvarez, Margui Romero, Denis Cajas Guaca, Daniel Núñez Alarcón e Diana Marcela Serrano, Maicon Benvenutti, Samuel Rocha, Marcus Vinicius Silva, Felipo Bacani, Valter Soares De Camargo, Lino Silva, Adson Mota Rocha, Tatiana Rocha, Ramom Santana, Cicero Silva, Porfirio Suñagua, Pedro Cárdena e Raphael Vilamiu. Para Jesus Niño Zambrano um grande e incondicional amigo na cidade de Bucaramanga. Finalmente a todos aqueles mencionados ou não sou eternamente grato

Introdução

Atualmente, o estudo das curvas algébricas sobre corpos finitos tem sido um tema de muito interesse em certas áreas da matemática, e tal tema tem sido amplamente estudado, especialmente por sua relação com a teoria da informação via a teoria de códigos e geometrias finitas.

Em 1940, A. Weil prova a hipótese de Riemann para curvas sobre corpos finitos. Como um corolário, é obtida uma cota superior para o número de pontos racionais de uma curva algébrica $\mathcal{C}$ geometricamente irredutível, não singular, de gênero g definida sobre o corpo finito com q elementos $\mathbb{F}_q$, a saber

$$\#\mathcal{C}\left(\mathbb{F}_q\right) \leq q + 1 + 2gq^{1/2},$$

onde $\#\mathcal{C}\left(\mathbb{F}_q\right)$ denota o número de pontos racionais da curva $\mathcal{C}$.

Alguns trabalhos tiveram como seu principal objetivo melhorar a cota acima (veja por exemplo, [16], [24]), outros determinar curvas onde $\#\mathcal{C}\left(\mathbb{F}_q\right)$ é o maior possível. Assim, foi obtidas uma grande variedade de curvas com esta propriedade, [28]. Além disso, foram encontradas curvas que atingiam esta cota, que na literatura são chamadas *curvas maximais*. Também foi determinada uma curva maximal de gênero maximal, chamada *curva Hermitiana*.

Com o trabalho de Goppa em 1980 (veja [13]) o estudo das curvas algébricas tornou-se importante, em consequência foi retomado novamente seu estudo; pois códigos induzidos por estas curvas tem bons parâmetros na medida que seu número de pontos racionais estava perto da cota de Hasse-Weil acima.

No ano 1987, Serre observou que toda curva recoberta por uma curva maximal era ainda maximal, [21]; uma prova deste fato é apresentada em [17]. Na literatura, todas as curvas maximais encontradas eram sempre recobertas pela curva Hermitiana (por exemplo veja [3], [11], entre outras). Uma questão que surgiu naturalmente foi se toda curva maximal estava sempre recoberta pela curva Hermitiana. Nesse aspecto, alguns trabalhos foram encaminhados a provar ou refutar esta afirmação. Em 2006, Garcia e Stichtenoth apresentam um primeiro exemplo de uma curva que não era Galois recoberta pela curva Hermitiana (veja [10]). Só em 2009 Giulietti e Korchmáros conseguiram resolver este problema, apresentando uma família de curvas maximais que não era recoberta pela curva Hermitiana, que ficaram conhecidas como as curvas GK, [12]. Uma generalização foi apresentada por Garcia, Güneri e Stichtenoth com uma curva que denotaremos por GGS. Até agora, a única informação para esta curva é que ela não é Galois recoberta pela curva Hermitiana, [4], [9].

Nosso objetivo principal nesta tese é construir exemplos de curvas maximais que não sejam

recobertas ou Galois recoberta pela curva Hermitiana, i.e, apresentar outras soluções ao problema resolvido por Giulietti e Korchmáros, e para isto usaremos recobrimentos da curva GGS, provaremos que algumas curvas obtidas com esta técnica tem tal propriedade (veja [27]).

Dividiremos este trabalho em 4 capítulos brevemente descritos a seguir:

O capítulo 1 tem como objetivo descrever alguns resultados sobre curvas maximais que serão usados adiante. Iniciamos apresentando a relação entre a função Zeta de uma curva e a cota de Hasse-Weil, e usaremos esta relação para determinar algumas propriedades das curvas maximais. A seguir apresentamos a equação fundamental de uma curva maximal, os principais resultados sobre recobrimentos e algumas relações com as curvas maximais também são estudadas. Finalizamos o capítulo com alguns aspectos sobre os semigrupos de Weierstrass associados a uma curva e a relação entre as curvas maximais e as variedades Hermitianas.

No capítulo 2 estudamos os principais fatos das curvas GK e GGS, e provaremos alguns destes resultados.

No capítulo 3 apresentamos a construção de duas famílias de curvas maximais. Para isto usaremos recobrimentos da curva GGS e depois provaremos que elas não são recobertas ou Galois recobertas pela curva Hermitiana.

Finalizamos este texto apresentando algumas aplicações. Em especial, usaremos as curvas apresentadas no capítulo 3 para calcular alguns códigos algébricos geométricos num ponto racional e compararemos os parâmetros obtidos com os parâmetros dos códigos existentes na literatura.

Capítulo 1

Preliminares

Neste capítulo descreveremos alguns resultados e conceitos que consideramos necessários para o desenvolvimento desta tese e que usaremos frequentemente; destacamos especialmente as curvas maximais e recobrimentos de curvas.

1.1 Curvas maximais

Apresentamos nesta seção alguns aspectos das curvas maximais e sua relação com um tipo especial de função Zeta de Riemman. Estudaremos as propriedades destas curvas; seu sistema linear e sua equação fundamental. Finalizamos a seção com alguns resultados sobre semigrupos de Weierstrass.

1.1.1 Curvas, divisores, a função Zeta e curvas maximais

Definição 1.1.1. *Seja q uma potência de um primo p. Denotaremos por $\mathbb{F}_q$ o corpo finito com q elementos; por uma **curva** sobre $\mathbb{F}_q$ entenderemos uma variedade algébrica projetiva $\mathcal{C} \subseteq \mathbb{P}^r\left(\overline{\mathbb{F}}_q\right)$ de dimensão 1, não singular e geometricamente irredutível sobre $\mathbb{F}_q$.*

Dada uma curva $\mathcal{C}$ sobre $\mathbb{F}_q$, os pontos P do espaço projetivo $\mathbb{P}^r\left(\overline{\mathbb{F}}_q\right)$ que satisfazem as equações que definem a curva são chamados **pontos** da curva $\mathcal{C}$ e escreveremos isto como $P \in \mathcal{C}$.

Um **divisor** de $\mathcal{C}$ é uma serie formal

$$D = \sum_{P \in \mathcal{C}} n_P P; \tag{1.1.1}$$

onde $n_P \in \mathbb{Z}$ e $n_P = 0$, exceto para um número finito de $P \in \mathcal{C}$. Denotaremos por por $Div\left(\mathcal{C}\right)$ o conjunto dos divisores de $\mathcal{C}$,

A **multiplicidade** de D em $P \in \mathcal{C}$ é definida como

$$v_P\left(D\right) := n_P;$$

onde v_P denota a valorização no ponto P.

O **suporte** de D é o conjunto

$$Sup\,(D) := \{P \in \mathcal{C} : n_P \neq 0\};$$

e seu **grau** é

$$grau\,(D) := \sum_{P \in Sup(D)} v_P\,(D)\,.n_P.$$

Naturalmente $Div\,(\mathcal{C})$ é um grupo abeliano com a soma definida como segue, para $D' = \sum_{P \in \mathcal{C}} m_P P$ e D como em (1.1.1),

$$D + D' = \sum_{P \in \mathcal{C}} (n_P + m_P)\,P.$$

O divisor D definido em (1.1.1) é chamado de **positivo ou efetivo** se para cada $P \in \mathcal{C}$, $n_P \geq 0$; neste caso escrevemos isto como $D \geq 0$. Se D, $E \in Div\,(\mathcal{C})$, dizemos que $D \geq E$ se $D - E \geq 0$.

Denotemos por $\mathbb{F}_q\,(\mathcal{C})$ o corpo de funções associado à curva $\mathcal{C}$, i.e., funções racionais definidas nos pontos de $\mathcal{C}$. Para cada $f \in \mathbb{F}_q\,(\mathcal{C}) \setminus \{0\}$ temos o **divisor principal** de f em $\mathcal{C}$, definido por

$$\mathrm{div}\,(f) = \sum_{P \in \mathcal{C}} v_P\,(f)\,P,$$

com v_P definida como acima, i.e., a valorização no ponto P.

Para cada $D \in Div\,(\mathcal{C})$ definimos o **espaço de Riemman-Roch**

$$\mathcal{L}\,(D) = \{f \in \mathbb{F}_q\,(\mathcal{C}) \setminus \{0\} : D + \mathrm{div}\,(f) \geq 0\} \cup \{0\};$$

temos que $\mathcal{L}\,(D)$ é um $\mathbb{F}_q-$ espaço vetorial de dimensão finita e

$$dim_{\mathbb{F}_q}\,(\mathcal{L}\,(D)) := \ell\,(D);$$

denota a **dimensão do divisor** D (veja [25], Proposição 1.4.9).

Definição 1.1.2. *Seja $\mathcal{C}$ uma curva sobre $\mathbb{F}_q$, existe um inteiro não negativo g chamado o **gênero** de $\mathcal{C}$, tal que*

$$\ell\,(D) = grau\,(D) + 1 - g, \tag{1.1.2}$$

para cada $D \in Div\,(\mathcal{C})$ com $grau\,(D) \geq 2g - 1$, (veja [25], Teorema 1.5.17)

Dois divisores $D, E \in Div\,(\mathcal{C})$ são chamados **linearmente equivalentes**, e escrevemos isto como $D \sim E$, se existe $f \in \mathbb{F}_q\,(\mathcal{C}) \setminus \{0\}$ tal que

$$D = E + \mathrm{div}\,(f)\,.$$

A relação $\sim$ é uma relação de equivalência; denotaremos por $[D]$ a classe de equivalência de $D \in Div\,(\mathcal{C})$. Como divisores equivalentes têm o mesmo grau e a mesma dimensão (veja [25], Corolário 1.4.12), definimos

$$grau\,[D] := grau\,(D)\,, \quad \text{e} \quad \ell\,([D]) := \ell\,(D)\,.$$

Denotaremos

$$Cl\left(\mathcal{C}\right)=\left\{[D]:D\in Div\left(\mathcal{C}\right)\right\}$$

e também

$$Cl^{0}\left(\mathcal{C}\right)=\left\{[D]\in Cl\left(\mathcal{C}\right):grau\left(D\right)=0\right\};\tag{1.1.3}$$

temos que $Cl^{0}\left(\mathcal{C}\right)$ é um subgrupo finito de $Cl\left(\mathcal{C}\right)$ (veja [25], Proposição 5.1.3).

Definimos para cada $n\in\mathbb{N}_{0}:=\mathbb{N}\cup\{0\}$:

$$A_{n}:=\#\left\{A\in Div\left(\mathcal{C}\right):A\geq 0\text{ e }grau\left(A\right)=n\right\}.$$

Por [25], Lema 5.1.1, cada A_n é um número finito. Em particular A_1 é chamado o número de $\mathbb{F}_q-$ **pontos racionais** da curva $\mathcal{C}$; denotaremos isto por

$$A_{1}:=\#\mathcal{C}\left(\mathbb{F}_{q}\right).$$

Definição 1.1.3. *A série de potências*

$$Z\left(t\right)=\sum_{n=0}^{\infty}A_{n}t^{n}\in\mathbb{C}\left[\left[t\right]\right]$$

é chamada a função ***Zeta*** *da curva* $\mathcal{C}$.

As principais propriedades desta função são descritas no seguinte teorema.

Teorema 1.1.4. *Seja* $\mathcal{C}$ *uma curva sobre* $\mathbb{F}_q$ *com gênero* $g\geq 0$ *então,*

1. *A função* $Z\left(t\right)$ *de* $\mathcal{C}$ *é convergente para* $|t|<q^{-1}$, *além disso:*

1.1. *Se* $g=0$ *então*

$$Z\left(t\right)=\frac{1}{\left(1-q\right)\left(1-qt\right)}.$$

1.2 *Se* $g\geq 1$ *então* $Z\left(t\right)=F\left(t\right)+G\left(t\right)$, *onde*

$$F\left(t\right)=\frac{1}{q-1}\sum_{[D]\in T}q^{\ell([D])}t^{grau([D])}\ \ e\ \ G\left(t\right)=\frac{\#Cl^{0}\left(\mathcal{C}\right)}{q-1}\left(q^{g}t^{2g-1}-\frac{1}{t}\right);$$

onde $T=\{[D]\in Cl\left(\mathcal{C}\right):0\leq grau\left([D]\right)\leq 2g-2\}$.

2. $Z\left(t\right)$ *satisfaz a equação funcional*

$$Z\left(t\right)=q^{g-1}t^{2g-2}Z\left(\frac{1}{qt}\right).$$

3. *O $L-$ polinômio de $\mathcal{C}$ sobre $\mathbb{F}_q$ é definido por*

$$L(t) = (1-q)(1-qt)Z(t);$$

então $L(t)$ é um polinômio com coeficientes em $\mathbb{Z}$, de grau $2g$.

Além disso temos,

3.1. *Se $L(t) = a_0 + a_1 t + ... + a_{2g} t^{2g}$, então $a_0 = 1$ e $a_{2g} = q^g$.*

3.2. *$a_{2g-i} = q^{g-i} a_i$, para $0 \leq i \leq g$.*

3.3. *$a_1 = \#\mathcal{C}(\mathbb{F}_q) - (q+1)$, onde $\#\mathcal{C}(\mathbb{F}_q)$ denota o número de $\mathbb{F}_q-$ pontos racionais de $\mathcal{C}$.*

3.4. *$L(t)$ se fatora em $\mathbb{C}[t]$ como*

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t); \tag{1.1.4}$$

onde $\alpha_1, ..., \alpha_{2g}$ são números complexos inteiros algébricos, arranjados tais que $\alpha_i \alpha_{i+g} = q$, com $i = 1, ..., g$.

Note-se que os α_i são inversos multiplicativos dos zeros de $L(t)$.

4. *Para $r \geq 1$, seja $Z_r(t)$ a função Zeta da curva $\mathcal{C}$ sobre $\mathbb{F}_{q^r}$, então seu $L-$ polinômio é*

$$L_r(t) = (1-q)(1-q^r t) Z_r(t);$$

e pode-se fatorar como

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t);$$

onde $\alpha_1, ..., \alpha_{2g}$ satisfazem (1.1.4).

5. *Para $r \geq 1$:*

$$\#\mathcal{C}(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r. \tag{1.1.5}$$

Dem. [14], seção 9.1; [25], seção 5.1. ■

Teorema 1.1.5. *(**Teorema de Hasse-Weil**) Seja $\mathcal{C}$ uma curva definida sobre $\mathbb{F}_q$ de gênero g e $\alpha_1, ..., \alpha_{2g}$ os inversos multiplicativos dos zeros de seu $L-$ polinômio, então para $i = 1, ..., 2g$:*

$$|\alpha_i| = q^{1/2}.$$

Dem. [14], seção 9.19; [25], Teorema 5.2.1. ■

Teorema 1.1.6. *(**Cota de Hasse-Weil**) Dada uma curva $\mathcal{C}$ sobre $\mathbb{F}_q$ de gênero g, seu número de $\mathbb{F}_q-$ pontos racionais $\#\mathcal{C}(\mathbb{F}_q)$ satisfaz*

$$|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq 2gq^{1/2}.$$

Dem. Sejam $\alpha_1, ..., \alpha_{2g}$ os inversos multiplicativos dos zeros do $L-$ polinômio da curva $\mathcal{C}$, da parte (5) do Teorema 1.1.4 com $r = 1$ temos

$$\#\mathcal{C}\left(\mathbb{F}_q\right) = q + 1 - \sum_{i=1}^{2g} \alpha_i;$$

e pelo Teorema 1.1.5, segue-se que

$$\left|\#\mathcal{C}\left(\mathbb{F}_q\right) - (q+1)\right| \leq \sum_{i=1}^{2g} |\alpha_i| = 2gq^{1/2}. \blacksquare$$

Definição 1.1.7. *Dizemos que uma curva $\mathcal{C}$ de gênero g é $\mathbb{F}_\ell-$**maximal** se seu número de $\mathbb{F}_\ell-$ pontos racionais atinge a cota superior de Hasse-Weil, i.e,*

$$\#\mathcal{C}\left(\mathbb{F}_\ell\right) = \ell + 1 + 2g\sqrt{\ell}.$$

Neste caso observamos que para $g > 0$, necessariamente ℓ tem que ser um quadrado. No que segue neste capítulo, sempre consideraremos curvas $\mathbb{F}_\ell$ maximais de gênero $g > 0$, onde $\ell = q^2$. As curvas maximais podem se caracterizar como segue.

Teorema 1.1.8. *Seja $\mathcal{C}$ uma curva definida sobre $\mathbb{F}_{q^2}$ de gênero g e sejam $\alpha_1, ..., \alpha_{2g}$ os inversos multiplicativos dos zeros do seu $L-$ polinômio, então as seguintes afirmações são equivalentes:*

1. *$\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal.*

2. *Para $i = 1, ..., 2g : \alpha_i = -q$.*

3. *$L\left(t\right) = \left(t + q\right)^{2g}$.*

Dem. $(1) \Longrightarrow (2)$: Se $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal, então

$$1 + q^2 + 2gq = 1 + q^2 - \sum_{i=1}^{2g} \alpha_i;$$

portanto, $2g = \sum\limits_{i=1}^{2g} -\frac{\alpha_i}{q}$ e pelo Teorema de Hasse-Weil $|\alpha_i| = q$, em consequência $-\frac{\alpha_i}{q} = 1$.

$(2) \Longrightarrow (3)$: Se $\alpha_i = -q$ para cada $i = 1, ..., 2g$, temos

$$L\left(t\right) = \left(t - \alpha_i\right)^{2g} = \left(t + q\right)^{2g}.$$

$(3) \Longrightarrow (1)$: Se $L\left(t\right) = \left(t + q\right)^{2g}$, então para $i = 1, ..., 2g$ temos $\alpha_i = -q$, em consequência

$$\#\mathcal{C}\left(\mathbb{F}_{q^2}\right) = 1 + q^2 - \sum_{i=1}^{2g} \alpha_i = 1 + q^2 + 2gq;$$

i.e, $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal. $\blacksquare$

Teorema 1.1.9. *Se $\mathcal{C}$ é uma curva $\mathbb{F}_{q^2}-$ maximal e $m \in \mathbb{N}$ é ímpar, então $\mathcal{C}$ é $\mathbb{F}_{q^{2m}}-$ maximal.*

Dem. Se $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal então pelo Teorema 1.1.8, para $i = 1, ..., 2g$ temos $\alpha_i = -q$, e como m é ímpar temos

$$\#\mathcal{C}\left(\mathbb{F}_{q^{2m}}\right) = 1 + q^{2m} - \sum_{i=1}^{2g} \alpha_i^m = 1 + q^{2m} + 2gq^m;$$

i.e, $\mathcal{C}$ é $\mathbb{F}_{q^{2m}}-$ maximal. ■

Teorema 1.1.10. ***(Ihara)*** *Seja $\mathcal{C}$ uma curva $\mathbb{F}_{q^2}-$ maximal com gênero g então*

$$g \leq q\left(q-1\right)/2.$$

Dem. Sejam $\alpha_1, ..., \alpha_{2g}$ os inversos multiplicativos dos zeros do $L-$ polinômio da curva $\mathcal{C}$; como $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal, pelo Teorema 1.1.8, para $i = 1, ..., 2g$ temos $\alpha_i = -q$. Agora, pelo Teorema 1.1.4 temos

$$\#\mathcal{C}\left(\mathbb{F}_{q^4}\right) = 1 + q^4 - \sum_{i=1}^{2g} \alpha_i^2 = 1 + q^4 - 2gq^2.$$

Como $\mathcal{C}\left(\mathbb{F}_{q^2}\right) \subseteq \mathcal{C}\left(\mathbb{F}_{q^4}\right)$, temos $1 + q^2 + 2gq \leq 1 + q^4 - 2gq^2$ e portanto $g \leq q\left(q-1\right)/2$. ■

Do Teorema 1.1.10, o inteiro $q\left(q-1\right)/2$ é uma cota superior para os gêneros de curvas $\mathbb{F}_{q^2}-$ maximais. Além disso existe uma curva $\mathbb{F}_{q^2}-$ maximal cujo gênero atinge esta cota, como descrevemos a seguir.

Teorema 1.1.11. *A curva Hermitiana sobre $\mathbb{F}_{q^2}$ é definida pela equação afim*

$$\mathcal{H}_q : x^q + x = y^{q+1};$$

então,

1. $g\left(\mathcal{H}_q\right) = \frac{q(q-1)}{2}$.

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

3. $\mathcal{H}_q$ *é* $\mathbb{F}_{q^2}-$ *maximal.*

4. *Salvo isomorfismo, $\mathcal{H}_q$ é a única curva $\mathbb{F}_{q^2}-$ maximal com gênero*

$$g = \frac{q\left(q-1\right)}{2}.$$

Dem. [14], [25], [26]. ■

1.1.2 Sistemas lineares de uma curva, equação fundamental

Seja $\mathcal{C}$ uma curva definida sobre $\mathbb{F}_q$. Para cada divisor $E \in Div(\mathcal{C})$ definimos

$$|E| = \{D' \in Div(\mathcal{C}) : D' \geq 0 \text{ e } D' \sim E\}.$$

Notemos que, $|E| = \varphi(\mathcal{L}(E) \setminus \{0\})$, onde

$$\begin{array}{rccc} \varphi: & \mathcal{L}(E) \setminus \{0\} & \longrightarrow & |E| \\ & f & \longmapsto & E + \operatorname{div}(f). \end{array}$$

Para $f, g \in \mathbb{F}_q(\mathcal{C}) \setminus \{0\}$ temos que $\operatorname{div}(f) = \operatorname{div}(g)$ se somente se existe $\lambda \in \mathbb{F}_q \setminus \{0\}$ tal que $f = \lambda g$.

Segue-se da aplicação

$$\begin{array}{rcc} |E| & \longrightarrow & \mathbb{P}(\mathcal{L}(E)) \\ E + \operatorname{div}(f) & \longmapsto & [f]; \end{array}$$

que $|E|$ pode-se equipar da estrutura de espaço projetivo, i.e, $|E| \simeq \mathbb{P}(\mathcal{L}(E))$.

Definição 1.1.12. *Um **sistema linear** $\mathcal{D}$ sobre a curva $\mathcal{C}$ é um subconjunto de $|E|$ do tipo*

$$\{E + \operatorname{div}(f) : f \in S \setminus \{0\}\},$$

*onde S é um subespaço $\mathbb{F}_q-$ linear de $\mathcal{L}(E)$. Dizemos que o sistema linear $\mathcal{D}$ é **completo** se $\mathcal{D} = |E|$.*

Definimos os parâmetros

$$d = grau(\mathcal{D}) := grau(E) \quad \text{e} \quad r = \dim(\mathcal{D}) := \dim(S) - 1;$$

que são chamados respectivamente o **grau** e a **dimensão** (projetiva) de $\mathcal{D}$; neste caso dizemos que $\mathcal{D}$ é um g^r_d sistema em $\mathcal{C}$ e escrevemos

$$g^r_d := \mathcal{D}$$

para denotar isto.

Para curvas maximais existe um tipo especial de sistema linear que estudaremos a seguir.

Consideremos o **automorfismo de Frobenius** de $\overline{\mathbb{F}}_q$

$$\begin{array}{rccc} \Phi: & \overline{\mathbb{F}}_q & \longrightarrow & \overline{\mathbb{F}}_q \\ & t & \longmapsto & t^q. \end{array}$$

A **colinealização de Frobenius** de $\mathbb{P}^r\left(\overline{\mathbb{F}}_{q^2}\right)$ associada a este automorfismo é definida por

$$\begin{array}{rccc} \Phi: & \mathbb{P}^r\left(\overline{\mathbb{F}}_q\right) & \longrightarrow & \mathbb{P}^r\left(\overline{\mathbb{F}}_q\right) \\ & X = (x_0 : x_1 : ... : x_r) & \longmapsto & X^q := (x_0^q : x_1^q : ... : x_r^q). \end{array}$$

Se $D = \sum_{P \in \mathcal{C}} n_P P \in Div(\mathcal{C})$ definimos

$$\Phi(D) := \sum_{P \in \mathcal{C}} n_P \Phi(P).$$

Notemos que, para cada $P \in \mathcal{C}(\mathbb{F}_q)$, $\Phi(P) = P$.

Para $P_0 \in \mathcal{C}(\mathbb{F}_{q^2})$ definamos

$$\begin{array}{rccc} \varphi_{P_0}: & \mathcal{C}(\mathbb{F}_{q^2}) & \longrightarrow & Cl^0(\mathcal{C}) \\ & P & \longmapsto & [P - P_0], \end{array}$$

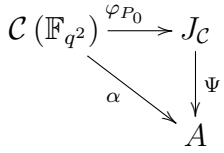
com $Cl^0(\mathcal{C})$ definido em (1.1.3). Notemos que $grau(P - P_0) = 0$, portanto φ_{P_0} está bem definida.

Seja $J_{\mathcal{C}}$ a **variedade Jacobiana** de $\mathcal{C}$, i.e, $J_{\mathcal{C}}$ é uma variedade abeliana caracterizada pela seguinte propriedade universal:

S*e A é uma variedade abeliana e $\alpha : \mathcal{C} \longrightarrow A$ é um morfismo que envia P_0 em $0 \in A$, então existe um único homomorfismo de variedades abelianas*[1] $\Psi : J_{\mathcal{C}} \longrightarrow A$ *tal que*

$$\Psi \circ \varphi_{P_0} = \alpha,$$

i.e., o seguinte diagrama comuta:



Teorema 1.1.13. *Seja $\mathcal{C}$ uma curva $\mathbb{F}_{q^2}-$ maximal contida em $\mathbb{P}^r\left(\overline{\mathbb{F}}_{q^2}\right)$. Se $P_0 \in \mathcal{C}(\mathbb{F}_{q^2})$ então o sistema linear de Frobenius $|(q+1)P_0|$ tem equação fundamental*

$$qP + \Phi(P) \sim (q+1)P_0, \tag{1.1.6}$$

satisfeita para cada $P \in \mathcal{C}$, onde Φ denota a colinealização de Frobenius de $\mathbb{P}^r\left(\overline{\mathbb{F}}_{q^2}\right)$ definida acima, e $\sim$ denota a equivalência linear entre divisores da curva $\mathcal{C}$.

Em particular, para cada par P_0, $P \in \mathcal{C}(\mathbb{F}_{q^2})$:

$$(q+1)P_0 \sim (q+1)P. \tag{1.1.7}$$

Dem. Definamos

$$\alpha = \varphi_{P_0} \circ \Phi : \mathcal{C}(\mathbb{F}_{q^2}) \longrightarrow Cl^0(\mathcal{C}) = A;$$

como

$$\alpha(P_0) = (\varphi_{P_0} \circ \Phi)(P_0) = [\Phi(P_0) - P_0] = [0];$$

[1]Variedades abelianas sao grupos grupos algébricos, ou seja, têm uma leis de grupos que podem ser definidos pelas funções regulares.

pela propriedade universal acima, existe $\Phi_{\mathcal{C}} : J_{\mathcal{C}} \longrightarrow Cl^0(\mathcal{C})$ tal que

$$\varphi_{P_0} \circ \Phi = \alpha = \Phi_{\mathcal{C}} \circ \varphi_{P_0}. \tag{1.1.8}$$

$\Phi_{\mathcal{C}}$ é chamada a **aplicação de Frobenius na variedade Jacobiana** $J_{\mathcal{C}}$. Notemos que $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal se somente se a aplicação de Frobenius $\Phi_{\mathcal{C}}$ na variedade Jacobiana $J_{\mathcal{C}}$ de $\mathcal{C}$ age sobre $J_{\mathcal{C}}$ multiplicando por $-q$, (veja [26], Lema 1).

De (1.1.8), para cada $P \in \mathcal{C}$

$$\begin{aligned}
[\Phi(P) - P_0] &= (\varphi_{P_0} \circ \Phi)(P) \\
&= (\Phi_{\mathcal{C}} \circ \varphi_{P_0})(P) \\
&= [-q(P - P_0)] \\
&= [qP_0 - qP],
\end{aligned}$$

portanto

$$\Phi(P) - P_0 \sim qP_0 - qP,$$

de onde obtemos (1.1.6).

Se em (1.1.6) $P \in \mathcal{C}(\mathbb{F}_{q^2})$ e portanto $\Phi(P) = P$, obtemos (1.1.7). ■

Se $\mathcal{C}$ é uma curva $\mathbb{F}_{q^2}-$ maximal então o sistema linear

$$\mathcal{D} = g^r_{q+1} = |(q+1)P_0|;$$

com $P_0 \in \mathcal{C}(\mathbb{F}_{q^2})$ é um $\mathbb{F}_{q^2}-$ invariante da curva $\mathcal{C}$. A dimensão r é independente $P_0 \in \mathcal{C}(\mathbb{F}_{q^2})$ e é chamada a **dimensão de Frobenius** de $\mathcal{C}$.

1.1.3 Semigrupos de Weierstrass de uma curva

Como é usual, denotaremos por $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ o conjunto dos números inteiros não negativos.

Definição 1.1.14. *Por um* ***semigrupo numérico*** *entendemos um subconjunto $S \subseteq \mathbb{N}_0$ tal que:*

- $0 \in S$;
- *S é fechado com respeito a adição, i.e, $s_1 + s_2 \in S$, para cada par $s_1, s_2 \in S$;*
- *$\mathbb{N}_0 \setminus S$ é finito.*

Se S é um semigrupo numérico então o número $g := \#(\mathbb{N}_0 \setminus S)$ é chamado o **gênero** de S; se existe

$$cond(S) = \min\{\lambda : \lambda + s \in S, \quad \forall s \in \mathbb{N}\};$$

então ele é chamado o **condutor** de S.

Se S é definido por

$$S = \{0 = s_0 < s_1 < ...\}$$

então cada s_i é chamada **não lacuna** de S; s_1 é a multiplicidade de S.

Os elementos do conjunto

$$Gap\,(S) := \mathbb{N}_0 \setminus S = \{\ell_1 < \ell_2 < ... < \ell_g\}$$

são chamados **lacunas**, onde ℓ_g a maior lacuna é chamada **número de Frobenius** de S e a denotamos por $Frob\,(S)$. Notemos que $\ell_g \leq 2g-1$. Dizemos que S é **simétrico** se $\ell_g = 2g-1$. Em geral $\ell_g + 1 = cond\,(S)$.

Denotaremos por $\langle s_1, ..., s_r\rangle$ o semigrupo numérico gerado pelas combinações lineares de $s_1, ..., s_r \in \mathbb{N}$, com coeficientes em $\mathbb{N}_0$.

Definição 1.1.15. *Seja $(a_1, ..., a_r)$ uma sequência finita em $\mathbb{N}$, com $mdc\,(a_1, ..., a_r) = 1$, para $i = 1, ..., r$, seja $d_i = mdc\,(a_1, ..., a_i)$ e defina*

$$S_i = \left\langle \frac{a_1}{d_i}, ..., \frac{a_i}{d_i} \right\rangle;$$

o semigrupo numérico gerado por $\frac{a_1}{d_i}, ..., \frac{a_i}{d_i}$.

- *Dizemos que $(a_1, ..., a_r)$ é uma **sequência telescópica** se para cada $i = 2, .., r : \frac{a_i}{d_i} \in S_{i-1}$.*
- *Um semigrupo numérico é chamado de **semigrupo telescópico** se é gerado por uma sequência telescópica.*

Podemos calcular o gênero de um semigrupo telescópico da seguinte forma:

Teorema 1.1.16. *Seja $A = (a_1, ..., a_r)$ é uma sequência telescópica e $S = \langle a_1, .., a_r\rangle$ o semigrupo telescópico gerado por A; então S tem gênero*

$$g\,(S) = \frac{1}{2}\left(1 + \sum_{i=1}^{r}\left(\frac{d_{i-1}}{d_i} - 1\right)a_i\right);$$

onde $d_0 = 0$ e para cada $i \geq 1 : d_i = mdc\,(a_1, ..., a_i)$.

Dem. [15], proposição 5.35. ■

Observação 1.1.17. *Como uma consequência direta da fórmula acima temos a conhecida fórmula do gênero de um semigrupo gerado por dois elementos, i.e., se $p, q \in \mathbb{N}$, com $mdc\,(p, q) = 1$, então o semigrupo $S = \langle p, q\rangle$ é um semigrupo numérico telescópico e*

$$g\,(S) = \frac{(p-1)\,(q-1)}{2}.$$

Seja $\mathcal{C}$ uma curva definida sobre $\mathbb{F}_q$ e denotaremos por $\mathbb{F}_q\,(\mathcal{C})$ o corpo de funções racionais definido sobre $\mathcal{C}$. Para $f \in \mathbb{F}_q\,(\mathcal{C}) \setminus \{0\}$, seja $\mathcal{N}_f = \{P \in \mathcal{C} : v_P\,(f) < 0\}$ o conjunto dos polos de f; denotemos por

$$\mathrm{div}_\infty(f) = \sum_{P \in \mathcal{N}_f} -v_P(f)\, P$$

o **divisor dos polo** de f.

Se $P \in \mathcal{C}(\mathbb{F}_q)$, dizemos que $k \in \mathbb{N}_0$ é um **número de polo** de P se existe $f \in \mathbb{F}_q(\mathcal{C}) \setminus \{0\}$ tal que $\mathrm{div}_\infty(f) = kP$.

Definamos

$$H(P) = \{k \in \mathbb{N}_0 : \mathrm{div}_\infty(f) = kP, \text{ para alguma } f \in \mathbb{F}_q(\mathcal{C}) \setminus \{0\}\}.$$

Se f é uma função constante não nula definida em $\mathcal{C}$ então $\mathrm{div}_\infty(f) = 0P$. Sejam $k_1,\ k_2 \in H(P)$, então existem $f_1, f_2 \in \mathbb{F}_q(\mathcal{C}) \setminus \{0\}$ tais que $\mathrm{div}_\infty(f_1) = k_1 P$ e $\mathrm{div}_\infty(f_2) = k_2 P$, portanto

$$\mathrm{div}_\infty(f_1.f_2) = \mathrm{div}_\infty(f_1) + \mathrm{div}_\infty(f_2) = (k_1 + k_2)\, P;$$

em consequência $H(P)$ é um semigrupo numérico; este semigrupo é conhecido como o **semigrupo de Weierstrass de $\mathcal{C}$ no ponto** P. Os números $k \in \mathbb{N}_0 \setminus H(P)$ são chamados **lacunas de Weierstrass** de P, e denotamos

$$G(P) = \{k \in \mathbb{N}_0 : k \text{ é lacuna de Weierstrass de } P\};$$

e os elementos de $H(P)$ também são chamados de **não lacunas** de P.

Teorema 1.1.18. *Seja $\mathcal{C}$ uma curva definida sobre $\mathbb{F}_q$ de gênero g e $P \in \mathcal{C}(\mathbb{F}_q)$, então:*

1. $\#G(P) = g$.

Em particular se $g > 0$, P tem exatamente g lacunas

$$1 = j_1 < j_2 < ... < j_g \leq 2g - 1;$$

portanto, se $k > 2g - 1$ então $k \in H(P)$, i.e,

$$\{2g,\ 2g+1,\ 2g+2, ...\} \subseteq H(P).$$

2. *Se $k \in \mathbb{N}_0$ então as seguintes afirmações são equivalentes:*

2.1 $k \in H(P)$.

2.2 *Existe $f \in \mathcal{L}(kP)$ tal que $v_P(f) = -k$.*

2.3 *Existe $f \in \mathbb{F}_q(\mathcal{C}) \setminus \{0\}$ tal que $(f)_\infty = kP$.*

2.4 $\ell(kP) = \ell((k-1)P) + 1$.

Dem. [14], Teoremas 6.88, 6.89; [25], Teorema 1.6.8. ■

Existe uma relação entre os sistemas lineares e os números não lacunas em curvas maximais, que apresentamos a seguir.

Teorema 1.1.19. *Seja $\mathcal{C}$ uma curva $\mathbb{F}_{q^2}-$ maximal e g^r_{q+1} um sistema linear sobre $\mathcal{C}$. Se $P \in \mathcal{C}(\mathbb{F}_{q^2})$ então existe uma sequência crescente em $H(P)$:*

$$0 < m_1(P) < m_2(P) < ... < m_r(P) = q+1.$$

Dem. [14], Teoremas 10.6. ■

Finalmente, de (1.1.7) temos que $q+1 \in H(P_0)$, i.e., $q+1$ é uma não lacuna de $\mathcal{C}$ em cada $P_0 \in \mathcal{C}(\mathbb{F}_{q^2})$, e o teorema acima vai garantir que de fato sempre $m_r(P) = q+1$, para cada $P \in \mathcal{C}(\mathbb{F}_{q^2})$.

Teorema 1.1.20. *Se $\mathcal{C}$ é uma curva definida sobre $\mathbb{F}_q$, $P \in \mathcal{C}(\mathbb{F}_q)$ e $H(P) = \{0 = s_0 < s_1 < s_2 < ...\}$ é o semigrupo de Weierstrass de $\mathcal{C}$ no ponto P, onde s_1 é a multiplicidade de $H(P)$, então*

$$\#\mathcal{C}(\mathbb{F}_q) \leq s_1 q^{1/2} + 1.$$

Dem. [22]. ■

Definição 1.1.21. ***(Cota de Lewittes)*** *Dada uma curva $\mathcal{C}$ sobre $\mathbb{F}_{q^2}$, $P \in \mathcal{C}(\mathbb{F}_q)$ e s_1 a multiplicidade de $H(P)$. Dizemos que C é* ***curva de Castle*** *em P se*

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = s_1 q + 1.$$

1.2 Recobrimentos de curvas

Nesta seção estudaremos os recobrimentos entre curvas, especialmente estamos interessados na relação entre os recobrimentos e as curvas maximais. No final da seção apresentamos uma relação entre as curvas maximais e as variedades Hermitianas.

1.2.1 Definição e propriedades

Da maneira mais simples entendemos por um morfismo entre duas curvas uma aplicação racional entre elas, i.e., se $\mathcal{C}_1$ e $\mathcal{C}_2$ são curvas sobre $\mathbb{F}_q$, com $\mathcal{C}_1 \subset \mathbb{P}^n$ e $\mathcal{C}_2 \subset \mathbb{P}^m$, supor que existem polinômios homogêneos $g_0, g_1, ..., g_m \in \mathbb{F}_q(\mathcal{C}_1)$ tais que para cada $P \in \mathcal{C}_1$ temos que

$$(g_0(P) : g_1(P) : ... : g_m(P)) \in \mathcal{C}_2;$$

um $\mathbb{F}_q-$ **morfismo** de $\mathcal{C}_1$ em $\mathcal{C}_2$ é uma função $\varphi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ definida por

$$\varphi(P) = (g_0(P) : g_1(P) : ... : g_m(P));$$

e escrevemos isto como $(g_0 : g_1 : ... : g_m)$ e as funções g_i são chamadas coordenadas (homogêneas) de φ. Neste caso, $\mathbb{F}_q(\varphi(\mathcal{C}_1)) = \mathbb{F}_q(g_0, g_1, ..., g_m)$. Para cada $Q \in \varphi(\mathcal{C}_1)$, os pontos de $\varphi^{-1}(Q)$ são chamados as ramificações de $\varphi(\mathcal{C}_1)$ em Q. O grau de φ é $grau(\varphi) := [\mathbb{F}_q(\mathcal{C}_1) : \mathbb{F}_q(\varphi(\mathcal{C}_1))]$.

Naturalmente, todo morfismo entre duas curvas afins, pode-se estender para um morfismo entre suas respectivas curvas homogêneas. Com a linguagem acima temos.

Definição 1.2.1. *Sejam $\mathcal{C}_1$, $\mathcal{C}_2$ curvas sobre $\mathbb{F}_q$, um morfismo sobrejetivo $\varphi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ é chamado um $\mathbb{F}_q-$* ***recobrimento****, neste caso dizemos que $\mathcal{C}_1$ recobre à curva $\mathcal{C}_2$ e também $\mathcal{C}_2$ é recoberta por $\mathcal{C}_1$.*

Em termos dos corpos de funções associados às curvas, isto significa que $\mathbb{F}_q(\mathcal{C}_2) \subseteq \mathbb{F}_q(\mathcal{C}_1)$. Assim,

- *φ é chamado* ***recobrimento de Galois*** *se $\mathbb{F}_q(\mathcal{C}_1)/\mathbb{F}_q(\mathcal{C}_2)$ é extensão de Galois.*
- *Dizemos φ é recobrimento de* ***grau*** *d se $[\mathbb{F}_q(\mathcal{C}_1) : \mathbb{F}_q(\mathcal{C}_2)] = d$.*

Recobrimentos e curvas maximais estão relacionadas como segue.

Teorema 1.2.2. *(**Serre**, [21]) Seja $\mathcal{C}$ curva $\mathbb{F}_{q^2}-$ recoberta por uma curva $\mathbb{F}_{q^2}-$ maximal, então $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal.*

Dem. Uma prova deste resultado foi apresentada por Kazemifard-Naghipour-Tafazolian (veja [17], Proposição 2.3) usando o fato que uma curva $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal se somente se a aplicação de Frobenius $\Phi_{\mathcal{C}}$ na variedade Jacobiana $J_{\mathcal{C}}$ de $\mathcal{C}$ age sobre $J_{\mathcal{C}}$ multiplicando por $-q$, (veja [26], Lema 1). A ideia da prova é que se $\varphi : \mathcal{D} \longrightarrow \mathcal{C}$ é um $\mathbb{F}_{q^2}-$ recobrimento, então φ induz um homomorfismo $\varphi^* : J_{\mathcal{C}} \longrightarrow J_{\mathcal{D}}$ sobre as variedades jacobianas e $J_{\mathcal{C}}$ é isogena a uma subvariedade de $J_{\mathcal{D}}$. Agora se $\mathcal{D}$ é $\mathbb{F}_{q^2}-$ maximal então $\Phi_{\mathcal{D}}$ age sobre $J_{\mathcal{D}}$ multiplicando por $-q$, portanto $\Phi_{\mathcal{C}}$ age sobre $J_{\mathcal{C}}$ multiplicando por $-q$, em consequência $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal. ■

Em particular toda curva $\mathbb{F}_{q^2}-$ recoberta pela curva Hermitiana $\mathcal{H}_q$ é $\mathbb{F}_{q^2}-$ maximal. Neste caso temos cotas para o grau do recobrimento.

Teorema 1.2.3. *Seja $\mathcal{C}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ e $\mathcal{H}_q$ a curva Hermitiana correspondente em $\mathbb{F}_{q^2}$, se existe um recobrimento $\varphi : \mathcal{H}_q \longrightarrow \mathcal{C}$ de grau d então*

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

Dem. Da fórmula do gênero de Riemman-Hurwitz temos

$$\begin{aligned} 2g(\mathcal{H}_q)-2 &= d(2g(\mathcal{C})-2) + grau(Diff(\mathbb{F}_{q^2}(\mathcal{H}_q)/\mathbb{F}_{q^2}(\mathcal{C}))) \\ &\geq d(2g(\mathcal{C})-2). \end{aligned}$$

Para cada $Q \in \mathcal{H}_q(\mathbb{F}_{q^2})$ existe $P \in \mathcal{C}(\mathbb{F}_{q^2})$ tal que Q cai sobre P. Além disso existem no máximo d de tais pontos P com a propriedade anterior, portanto $\#\mathcal{H}_q(\mathbb{F}_{q^2}) \leq d.\#\mathcal{C}(\mathbb{F}_{q^2})$. ■

Também foi obtida uma condição sobre os gêneros de curvas maximais tais que elas sejam recobertas pela curva Hermitiana, a seguir.

Teorema 1.2.4. *(Korchmáros-Torres) Se $\mathcal{C}$ é uma curva $\mathbb{F}_{q^2}-$ maximal, com gênero*

$$g > \frac{q^2-q+4}{6};$$

então $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ recoberta pela curva Hermitiana $\mathcal{H}_q$.

Dem. [20], Corolario 3.3. ■

Note-se que do Teorema 1.2.4, se $\mathcal{C}$ é uma curva $\mathbb{F}_{q^2}-$ maximal com gênero g, para que $\mathcal{C}$ não seja $\mathbb{F}_{q^2}-$ recoberta pela curva Hermitiana correspondente é necessário que

$$\frac{q^2-q+4}{6} \geq g.$$

1.2.2 Curvas maximais e variedades Hermitianas

Seja F um corpo. Um automorfismo $\phi : F \longrightarrow F$ é chamado de **involução** se $\phi \neq i_F$ e $\phi^2 = i_F$, onde i_F denota o automorfismo identidade sobre F. Facilmente podemos provar que a única involução sobre $\mathbb{F}_{q^2}$ é definida por

$$\phi(t) = t^q.$$

Como no caso do corpo dos números complexos dizemos que uma matriz $A = (a_{ij})$ quadrada com entradas em $\mathbb{F}_{q^2}$ é $\mathbb{F}_{q^2}-$ **Hermitiana** se $A = A^H$, onde naturalmente A^H denota a transposta hermitiana de A, i.e.,

$$A^H = (\phi(a_{ji})) = \left(a_{ji}^q\right).$$

Dizemos que uma variedade V sobre o corpo $\mathbb{F}_{q^2}$ é **variedade Hermitiana** se é gerada por uma matriz $\mathbb{F}_{q^2}-$ **Hermitiana**, i.e.,

$$V = \left\{X : XAX^H = 0\right\} \subset P^n\left(\overline{\mathbb{F}}_{q^2}\right),$$

com A uma matriz $\mathbb{F}_{q^2}-$ Hermitiana de ordem n.

Temos uma relação entre as curvas $\mathbb{F}_{q^2}-$ maximais e as variedades $\mathbb{F}_{q^2}-$ Hermitianas que descrevemos a seguir:

Seja $\mathcal{C}$ uma curva $\mathbb{F}_{q^2}-$ maximal, seja $P_0 \in \mathcal{C}(\mathbb{F}_{q^2})$ e consideremos o sistema linear

$$g_{q+1}^r = |(q+1)P_0|;$$

de dimensão r, pelo teorema 1.1.19, existe uma sequência crescente em $H(P_0)$:

$$0 < m_1(P_0) < m_2(P_0) < ... < m_r(P_0) = q+1.$$

Agora, para cada $i = 1, ..., r$ existe $f_i \in \mathbb{F}_q(\mathcal{C}) \setminus \{0\}$ tal que $\mathrm{div}_\infty(f_i) = m_i(P)P$, e associado à curva $\mathcal{C}$ temos o morfismo

$$\begin{array}{rccc} \pi: & \mathcal{C} & \longrightarrow & \mathbb{P}^{r-1}\left(\overline{\mathbb{F}}_{q^2}\right) \subset \mathbb{P}^r\left(\overline{\mathbb{F}}_{q^2}\right) \\ & Q & \longmapsto & (f_1(Q) : ... : f_r(Q)). \end{array}$$

Teorema 1.2.5. *Para o morfismos acima temos,*

- $\mathcal{C}$ *é* $\mathbb{F}_{q^2}-$ *isomorfa à curva* $\pi(\mathcal{C})$*;*

- *Se* $P \in \mathcal{C}$ *e* $\pi(P) \in \mathbb{P}^r(\mathbb{F}_{q^2})$ *então* $P \in \mathcal{C}(\mathbb{F}_{q^2})$*;*
- *A curva* $\mathcal{C}$ *esta contida em uma* $\mathbb{F}_{q^2}-$ *variedade Hermitiana de* $\mathbb{P}^r\left(\overline{\mathbb{F}}_{q^2}\right)$.

Dem. [8], Lema 1.9; [19], Lema 2.4, Teoremas 2.5, 3.4. ■

Reciprocamente temos:

Teorema 1.2.6. *Seja* $\mathcal{C}$ *uma curva projetiva não singular e geometricamente irredutível sobre* $\mathbb{F}_{q^2}$*, equipada com um* $\mathbb{F}_{q^2}-$ *morfismo birracional não degenerado*

$$\begin{array}{rccc} \pi: & \mathcal{C} & \longrightarrow & \mathbb{P}^N\left(\overline{\mathbb{F}}_{q^2}\right) \\ & Q & \longmapsto & (f_0(Q) : ... : f_N(Q)); \end{array}$$

tal que $\mathcal{Y} := \pi(\mathcal{C})$*, esta contida em una* $\mathbb{F}_{q^2}-$ *variedade Hermitiana não degenerada de* $\mathbb{P}^r\left(\overline{\mathbb{F}}_{q^2}\right)$*, então* $\mathcal{C}$ *é* $\mathbb{F}_{q^2}-$ *maximal.*

Dem. [19], Teorema 4.1. ■

Observação 1.2.7. *Os dois teoremas acima determinam uma relação entre as curvas maximais e as variedades Hermitianas descrita explicitamente como segue: toda curva* $\mathbb{F}_{q^2}-$ *maximal está contida numa variedade Hermitiana sobre* $\mathbb{F}_{q^2}$*. Além disso se* $\mathcal{C}$ *é uma curva contida numa* $\mathbb{F}_{q^2}-$ *variedade Hermitiana, então* $\mathcal{C}$ *é* $\mathbb{F}_{q^2}-$ *maximal.*

Capítulo 2

As curvas GK e GGS

Apresentamos agora duas famílias de curvas que em essência são a chave de nosso trabalho. Do Teorema 1.2.2, temos que em particular, se $\mathcal{C}$ é uma curva $\mathbb{F}_{q^2}-$ recoberta pela curva Hermitiana $\mathcal{H}_q$ então $\mathcal{C}$ é $\mathbb{F}_{q^2}-$ maximal. Uma questão de interesse é a recíproca desta afirmação, i.e, se toda curva $\mathbb{F}_{q^2}-$ maximal é $\mathbb{F}_{q^2}-$ recoberta pela curva curva Hermitiana $\mathcal{H}_q$. Na literatura, diversas curvas maximais foram obtidas como sendo recobertas pela curva Hermitiana (veja [3], [11]). Garcia e Stichtenoth encontraram o primeiro exemplo de uma que não era Galois recoberta pela curva Hermitiana (veja [10]). As curvas que estudaremos neste capítulo dão uma resposta mais ampla para esta questão, a maior parte dos resultados aparecem provados em [4], [9], [12].

2.1 A curva GK

Seja p um número primo, q uma potência de p. Em $\mathbb{P}^3\left(\overline{\mathbb{F}}_{q^6}\right)$ definimos a curva GK como a intersecção das superfícies com equações afins

$$y^{q+1} = x^q + x \quad \text{e} \quad z^{\frac{q^3+1}{q+1}} = yh\left(x\right); \tag{2.1.1}$$

onde $h\left(x\right)$ é o polinômio em $\mathbb{F}_{q^6}\left[x\right]$ definido por $h\left(x\right) = \sum_{i=0}^{q}\left(-1\right)^{i+1} x^{i(q-1)}$, portanto

$$h\left(x\right) = \frac{x^{q^2} - x}{x^q + x}.$$

(Veja [12], Lema 1).

As principais propriedades destas curvas são descritas a seguir.

Teorema 2.1.1. *A curva GK está contida na variedade $\mathbb{F}_{q^6}-$ Hermitiana com equação afim*

$$\mathcal{H} : X^{q^3} + X = Y^{q^3+1} + Z^{q^3+1}; \tag{2.1.2}$$

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

Dem. Primeiro notemos que a curva GK tem um único ponto no infinito $X_\infty = (1:0:0:0)$, que corresponde ao eixo x. De fato, $h(x)$ tem grau q^2-q, portanto $z^{\frac{q^3+1}{q+1}} - yh(x)$ é um polinômio homogêneo de grau q^2-q+1. Temos as equações homogenizadas de GK

$$Y^{q+1} = WX^q + W^qX \quad \text{e} \quad Z^{\frac{q^3+1}{q+1}} = Yh(X);$$

nas variáveis (X,Y,Z,W).

Notemos que se $W=0$, de $Y^{q+1} = WX^q + W^qX$, obtemos $Y=0$, portanto $Z^{\frac{q^3+1}{q+1}} = Yh(X) = 0$, i.e, $Z=0$ em consequência, $X_\infty = (1:0:0:0)$ é o único ponto no infinito de $\mathbb{P}^3\left(\overline{\mathbb{F}}_{q^6}\right)$ com $X_\infty \in GK$.

Agora homogeneizando $\mathcal{H}$ obtemos

$$\mathcal{H} : WX^{q^3} + W^{q^3}X = Y^{q^3+1} + Z^{q^3+1};$$

também nas variáveis (X,Y,Z,W).

Notemos que

$$(X,Y,Z,W)\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} X^{q^3} \\ Y^{q^3} \\ Z^{q^3} \\ W^{q^3} \end{pmatrix} = WX^{q^3} + W^{q^3}X - \left(Y^{q^3+1} + Z^{q^3+1}\right);$$

portanto $\mathcal{H}$ é uma variedade $\mathbb{F}_{q^6}-$ Hermitiana; além disso, é X_∞ o único ponto no infinito da curva GK cai em $\mathcal{H}$.

Para os pontos afins $(x,y,z,1)$ de GK

$$\begin{aligned} z^{q^3+1} &= y^{q+1}h(x)^{q+1} \\ &= (x^q+x)\left(\frac{x^{q^2}-x}{x^q+x}\right)^{q+1} \\ &= \frac{x^{q^3+q^2} - x^{q^3+1} - x^{q^2+q} + x^{q+1}}{(x^q+x)^q}; \end{aligned}$$

também temos

$$\begin{aligned} y^{q^3+1} &= (x^q+x)^{q^2-q+1} \\ &= \frac{x^{q^3+q} + x^{q^3+1} + x^{q^2+q} + x^{q^2+1}}{(x^q+x)^q}; \end{aligned}$$

daí obtemos

$$z^{q^3+1} + y^{q^3+1} = x^{q^3} + x.$$

■

Observação 2.1.2. *([23], Teorema 2.19) Se $\mathcal{X}$ é uma variedade afim em $\mathbb{A}^r\left(\overline{\mathbb{F}}_q\right)$ e $f_1,..,f_t \in \overline{\mathbb{F}}_q[X_1,...,X_r]$ são polinômios geradores de $\mathcal{X}$, então $\mathcal{X}$ é não singular em $P \in \mathcal{X}$ se somente se a matriz $\left(\frac{\partial f_i}{\partial X_j}(P)\right)$ tem posto $r - \dim(\mathcal{X})$.*

Teorema 2.1.3. *A curva GK é absolutamente irredutível e não singular.*

Dem. Pela Observação 2.1.2, $P_0 = (0,0,0)$ é um ponto não singular de GK. Seja $\mathcal{Y}$ uma componente irredutível de GK que contém o ponto P_0; como $\mathcal{Y} \subset \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^6}\right)$, temos um $\mathbb{F}_{q^6}-$ morfismo $\varphi = (x,y,z,w) : \mathcal{Y} \longrightarrow \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^6}\right)$, onde $x,y,z,w \in \mathbb{F}_{q^6}(\mathcal{Y})$ e estas funções coordenadas de φ são determinadas de maneira única por um fator de proporcionalidade em $\mathbb{F}_{q^6}(\mathcal{Y}) \setminus \{0\}$. Podemos supor $w = 1$; como $\mathcal{Y} \subset GK$ e portanto $\mathcal{Y}$ cai na variedade Hermitiana $\mathcal{H}$ definida acima, temos

$$z^{q^3+1} + y^{q^3+1} = x^{q^3} + x. \tag{2.1.3}$$

Como P_0 é um zero de x, y, z, então

$$\begin{aligned} q^3+1 &\leq v_{P_0}\left(z^{q^3+1} + y^{q^3+1}\right) \\ &= v_{P_0}\left(x^{q^3} + x\right) \\ &= \min\left\{q^3 v_{P_0}(x),\ v_{P_0}(x)\right\} \\ &= v_{P_0}(x). \end{aligned}$$

Seja π_0 o plano com equação $X = 0$, então o número de intersecção $I(P,\ \mathcal{Y} \cap \pi_0)$ é pelo menos q^3+1, portanto, se $GK \neq \mathcal{Y}$, então $\mathcal{Y}$ cai em π_0, mas isto é impossível, pois $GK \cap \pi_0 = \{P_0, X_\infty\}$, em consequência $GK = \mathcal{Y}$, isto é, GK é absolutamente irredutível. Finalmente, usando o fato que GK é absolutamente irredutível, e por [14], Teorema 10.17, temos que GK é não singular. ■

Teorema 2.1.4. *A curva GK tem gênero*

$$g = \frac{q^5 - 2q^3 + q^2}{2}.$$

Dem. [12], Teorema 2. ■

Com o argumento que descreveremos no capítulo 3, temos.

Teorema 2.1.5. *Para $q > 2$ a curva GK não é $\mathbb{F}_{q^6}-$ recoberta pela curva Hermitiana $\mathcal{H}_{q^3}$.*

Dem. [12], Teorema 5. ■

No capítulo 3 descreveremos em detalhe o argumento usando na demonstração do Teorema 2.1.5. Até agora a curva GK é o único exemplo existente na literatura de uma curva que não é recoberta pela curva Hermitiana. No caso $q = 2$, temos que a curva GK é Galois recoberta pela curva Hermitiana $\mathcal{H}_{q^3}$, (veja [12]). Finalmente, alguns aspectos teóricos como códigos, grupos de automorfismo e quocientes da curva GK são considerados em [5] e [6].

2.2 A curva GGS

Sejam q uma potência de um primo p e $m \in \mathbb{N}$ ímpar com $m \geq 3$. Em $\mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$ definimos a curva GGS como a intersecção das superfícies com equações afins

$$y^{q+1} = x^q + x \quad e \quad z^{\frac{q^m+1}{q+1}} = y^{q^2} - y. \tag{2.2.1}$$

Esta curva generaliza a curva GK definida em (2.1.1) como veremos a seguir.

Lema 2.2.1. *Para $m = 3$ a curva GGS é $\mathbb{F}_{q^6}-$ isomorfa à curva GK.*

Dem. Seja $h(x)$ definido como na curva GK, i.e

$$h(x) = \frac{x^{q^2} - x}{x^q + x}.$$

Para $(x, y, z) \in GGS$ temos

$$y^{q^2-1} = (x^q + x)^{q-1} = \frac{x^{q^2} + x^q}{x^q + x} = \frac{\left(x^{q^2} - x\right) + (x^q + x)}{x^q + x} = h(x) + 1;$$

de onde obtemos

$$y^{q^2} - y = y\left(y^{q^2-1} - 1\right) = yh(x).\blacksquare$$

Com esta generalização gostaríamos de saber que propriedades da curva GK são herdadas pela curva GGS.

Analogamente como no caso da curva GK, a curva GGS tem um único ponto no infinito $X_\infty = (1 : 0 : 0 : 0)$, que corresponde ao eixo x. Agora, se $(x, y, z, 1)$ é um ponto do espaço afim sobre a curva GGS temos

$$\begin{aligned} z^{q^m+1} &= \left(y^{q^2} - y\right)^{q+1} = \left(y^{q^2} - y\right)^q \left(y^{q^2} - y\right) \\ &= (x^q + x)^{q^2} - y^{q^3+1} - (x^q + x)^q + (x^q + x) \\ &= x^{q^3} + x - y^{q^3+1}; \end{aligned}$$

i.e, $z^{q^m+1} + y^{q^3+1} = x^{q^3} + x$.

Definamos a variedade

$$\mathcal{H}_m : Z^{q^m+1} + Y^{q^3+1} = X^{q^3} + X. \tag{2.2.2}$$

Facilmente podemos provar que $X_\infty \in \mathcal{H}_m$, em consequência a curva GGS esta contida nesta variedade $\mathcal{H}_m$; note-se que se $m = 3$, a variedade $\mathcal{H}_m$ coincide com a variedade Hermitiana definida em (2.1.2), e note-se também que para $m > 3$, $\mathcal{H}_m$ não e uma variedade Hermitiana, portanto não podemos obter diretamente a maximalidade da curva GGS de $\mathcal{H}_m$, mas podemos aproveitar (2.2.2) para provar o seguinte.

Teorema 2.2.2. *A curva GGS é absolutamente irredutível e não singular.*

Dem. Exceto por algumas mudanças apropriadas a demonstração é a mesma do Teorema 2.1.3, a seguir. Novamente pela observação 2.1.2, $P_0 = (0,0,0)$ é um ponto não singular de GGS. Seja $\mathcal{Y}$ uma componente irredutível de GGS que contem o ponto P_0; como $\mathcal{Y} \subset \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$, temos um $\mathbb{F}_{q^{2m}}-$ morfismo $\varphi = (x,y,z,w) : \mathcal{Y} \longrightarrow \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$, onde $x,y,z,w \in \mathbb{F}_{q^{2m}}(\mathcal{Y})$ e estas funções coordenadas de φ então determinadas de maneira única por um fator de proporcionalidade em $\mathbb{F}_{q^{2m}}(\mathcal{Y}) \setminus \{0\}$. Podemos supor $w = 1$; como $\mathcal{Y} \subset GGS$ e portanto $\mathcal{Y}$ cai na variedade Hermitiana $\mathcal{H}_m$ definida acima, temos

$$z^{q^m+1} + y^{q^3+1} = x^{q^3} + x.$$

P_0 é um zero de x, y, z e

$$v_{P_0}\left(z^{q^m+1} + y^{q^3+1}\right) \geq \min\left\{v_{P_0}\left(z^{q^m+1}\right), v_{P_0}\left(y^{q^3+1}\right)\right\}.$$

Se $\min\left\{v_{P_0}\left(z^{q^m+1}\right), v_{P_0}\left(y^{q^3+1}\right)\right\} = v_{P_0}\left(z^{q^m+1}\right)$, então

$$\min\left\{v_{P_0}\left(z^{q^m+1}\right), v_{P_0}\left(y^{q^3+1}\right)\right\} \geq q^m + 1 \geq q^3 + 1.$$

Se $\min\left\{v_{P_0}\left(z^{q^m+1}\right), v_{P_0}\left(y^{q^3+1}\right)\right\} = v_{P_0}\left(y^{q^3+1}\right)$, então

$$\min\left\{v_{P_0}\left(z^{q^m+1}\right), v_{P_0}\left(y^{q^3+1}\right)\right\} \geq q^3 + 1;$$

portanto

$$\begin{aligned} q^3 + 1 &\leq v_{P_0}\left(z^{q^m+1} + y^{q^3+1}\right) \\ &= v_{P_0}\left(x^{q^3} + x\right) \\ &= \min\left\{q^3 v_{P_0}(x),\ v_{P_0}(x)\right\} \\ &= v_{P_0}(x). \end{aligned}$$

Seja π_0 o plano com equação $X = 0$, então o número de intersecção $I(P,\ \mathcal{Y} \cap \pi_0)$ é pelo menos q^3+1, portanto, se $GGS \neq \mathcal{Y}$, então $\mathcal{Y}$ cai em π_0, mais isto é impossível, pois $GGS \cap \pi_0 = \{P_0, X_\infty\}$, em consequência $GGS = \mathcal{Y}$, isto é, GGS é absolutamente irredutível. Finalmente, usando o fato que GGS é absolutamente irredutível, e por [14], Teorema 10.17, temos que GK é não singular.■

Demonstraremos agora a maximalidade da curva GGS, para isto usaremos a notação

$$\mathcal{X}_m : z^{\frac{q^m+1}{q+1}} = y^{q^2} - y;$$

e consideremos os recobrimentos das curvas

$$GGS \longrightarrow \mathcal{X}_m \longrightarrow \mathbb{P}^1; \tag{2.2.3}$$

onde $\mathbb{P}^1$ denota a reta projetiva.

Lema 2.2.3. *(**Abdón-Bezerra-Quoos**) A curva $\mathcal{X}_m$ é $\mathbb{F}_{q^{2m}}-$ maximal com gênero*

$$g\left(\mathcal{X}_m\right) = \frac{\left(q-1\right)\left(q^m-q\right)}{2}.$$

Dem. [1]. ■

Temos agora.

Teorema 2.2.4. *A curva GGS é $\mathbb{F}_{q^{2m}}-$ maximal, com gênero*

$$g\left(GGS\right) = \frac{\left(q-1\right)\left(q^{m+1}+q^m-q^2\right)}{2}. \tag{2.2.4}$$

Dem. Para o cálculo do gênero, de (2.2.3) podemos olhar GGS como um recobrimento do tipo Artin-Scherier de $\mathcal{X}_m$, além disso, de [25], Lema 3.7.7 e Proposição 3.7.8 temos que o único ponto do recobrimento $\mathcal{X}_m \longrightarrow \mathbb{P}^1$ que é totalmente ramificado em GGS é o polo P_∞ de y, que de fato é o mesmo polo de z. Agora, para $u = y^{q+1}$, temos

$$\begin{aligned} m_{P_\infty}\left(u\right) &= -\left(q+1\right)v_{P_\infty}\left(y\right) \\ &= -\left(q+1\right)\left(-grau\left(\mathcal{X}_m\right)\right) \\ &= -\left(q+1\right)\left(-\frac{q^m+1}{q+1}\right) \\ &= q^m+1; \end{aligned}$$

portanto o expoente da diferente neste ponto é

$$\begin{aligned} d_{P_\infty}\left(u\right) &= \left(q-1\right)\left(m_{P_\infty}\left(u\right)+1\right) \\ &= \left(q-1\right)\left(q^m+2\right); \end{aligned}$$

e pela fórmula do gênero de Riemann-Hurwitz

$$\begin{aligned} 2g\left(GGS\right)-2 &= q\left(2g\left(\mathcal{X}_m\right)-2\right)+\left(q-1\right)\left(q^m+2\right) \\ &= q\left(\left(q-1\right)\left(q^m-q\right)-2\right)+\left(q-1\right)\left(q^m+2\right); \end{aligned}$$

de onde obtemos (2.2.4).

Para calcular o número de $\mathbb{F}_{q^{2m}}-$ pontos racionais da curva GGS, note-se que $\mathcal{X}_m$ é $\mathbb{F}_{q^{2m}}-$ maximal, em consequência

$$\#\mathcal{X}_m\left(\mathbb{F}_{q^{2m}}\right) = q^{2m}+1+\left(q-1\right)\left(q^m-q\right)q^m = q^{2m+1}-q^{m+2}+q^{m+1}+1.$$

Agora, pelas identidades polinomiais apresentadas em [9], Lema 2.5, temos que cada $\mathbb{F}_{q^{2m}}-$ ponto racional afim de $\mathcal{X}_m$ é totalmente ramificado em GGS, além disso, o único ponto no infinito de $\mathcal{X}_m$ é totalmente ramificado em GGS e como $GGS \longrightarrow \mathcal{X}_m$ é um recobrimento de grau q temos

$$\#GGS\left(\mathbb{F}_{q^{2m}}\right) = q\left(\#\mathcal{X}_m\left(\mathbb{F}_{q^{2m}}\right)-1\right)+1 = q^{2m}+1+2g\left(GGS\right)q^m;$$

e GGS é $\mathbb{F}_{q^{2m}}-$ maximal. ■

Para $m = 3$, pelo Lema 2.2.1, a curva GGS é $\mathbb{F}_{q^6}-$ isomorfa à curva GK portanto

$$g(GGS) = \frac{(q-1)(q^{3+1}+q^3-q^2)}{2} = \frac{q^5-2q^3+q^2}{2};$$

e temos o Teorema 2.1.4. Também temos que a curva GGS não é $\mathbb{F}_{q^6}-$ recoberta pela curva Hermitiana $\mathcal{H}_{q^3}$. Para $m > 3$ a melhor informação obtida é apresentada no seguinte teorema.

Teorema 2.2.5. *Para $m > 3$ e $q > 2$, a curva GGS não é $\mathbb{F}_{q^{2m}}-$ Galois recoberta pela curva Hermitiana $\mathcal{H}_{q^m}$.*

Dem. Consequência direta de [4], Proposição 5.1. ■

Observação 2.2.6. *Finalmente, notemos que:*

- *Pelo Lema 2.2.3 a curva $\mathcal{X}_m$ é $\mathbb{F}_{q^{2m}}-$ maximal.*
- *Em particular quando $m = q = 3$ temos que*

  $$\mathcal{X}_3 : y^9 - y = z^7;$$

  é $\mathbb{F}_{27^2}-$ maximal com gênero $g = 24$ e não é $\mathbb{F}_{27^2}-$ Galois recoberta pela curva Hermitiana $\mathcal{H}_{27}$ (veja [10]); não é conhecido um resultado análogo para $(m, q) \neq (3, 3)$; de fato este foi o primeiro resultado apresentado na teoria que tentava garantir que nem toda curva maximal estava recoberta pela curva Hermitiana correspondente.
- *A curva,*

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

  é a curva Hermitiana sobre $\mathbb{F}_{q^2}$, (veja Teorema 1.1.11), que é $\mathbb{F}_{q^2}-$ maximal e pelo Teorema 1.1.9 é $\mathbb{F}_{q^{2m}}-$ maximal para cada m ímpar.
- *Temos duas superfícies (com equações que definem curvas $\mathbb{F}_{q^{2m}}-$ maximais) cuja interseção é uma curva $\mathbb{F}_{q^{2m}}-$ maximal. Em geral isto não ocorre sempre, por exemplo, para q ímpar, seja*

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

  Notemos que a curva $x^q + x = y^{(q+1)/2}$ é $\mathbb{F}_{q^{2m}}-$ recoberta pela curva Hermitiana sobre $\mathcal{H}_q$ portanto é $\mathbb{F}_{q^{2m}}-$ maximal, onde m é ímpar. Para $q = m = 3$, obtemos $g(\mathcal{C}) = 85$ e $\#\mathcal{C}(\mathbb{F}_{27^2}) = 2296$ [2], e uma curva $\mathbb{F}_{27^2}-$ maximal com gênero 85 deve ter 5320 $\mathbb{F}_{27^2}-$ pontos racionais.

[2] Magma Computational Algebra System

Capítulo 3

Exemplos

Neste capítulo vamos definir duas famílias de curvas que são maximais. De fato estas são construídas via recobrimentos da curva GK generalizada ou curva GGS definida em (2.2.1). Além disso, estudaremos a possibilidade que estas sejam recobertas ou Galois recobertas pela curva Hermitiana correspondente.

3.1 A curva $\mathcal{X}_{a,b,m,s}$

3.1.1 Definição e maximalidade de $\mathcal{X}_{a,b,m,s}$

Sejam $a, b, s \in \mathbb{N}$, $m \geq 3$, $q = p^a$, com p primo, suponhamos que:

- m é ímpar;
- b é um divisor de a;
- s é um divisor de $\frac{q^m+1}{q+1}$.

Consideremos o morfismo

$$\begin{array}{rccl} \varphi_{a,b,m,s}: & \mathcal{C}_m & \longrightarrow & \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right) \\ & (u,v,w,1) & \longmapsto & (x:y:z:1) := \left(\lambda u - (\lambda u)^{p^b} : v : w^s : 1\right); \end{array} \tag{3.1.1}$$

onde $\mathcal{C}_m$ é a curva GGS definida em (2.2.1), e $\lambda \in \mathbb{F}_{q^2}$ é tal que $\lambda^{q-1} = -1$.

Definição 3.1.1. *A curva $\mathcal{X}_{a,b,m,s}$ é definida como o modelo não singular de $\varphi_{a,b,m,s}(\mathcal{C}_m) \subseteq \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$.*

Explicitamente temos.

Lema 3.1.2. *A curva $\varphi_{a,b,m,s}(\mathcal{C}_m)$ tem equações afins*

$$\lambda y^{q+1} = t(x) := \sum_{i=0}^{d-1} x^{p^{bi}} \quad e \quad z^M = y^{q^2} - y; \tag{3.1.2}$$

onde $d = \frac{a}{b}$, $M = \frac{q^m+1}{s(q+1)}$.

Dem. Para $(u,v,w,1) \in \mathcal{C}_m$, i.e,

$$u^q + u = v^{q+1} \quad \text{e} \quad w^{\frac{q^m+1}{q+1}} = v^{q^2} - v;$$

sejam

$$\begin{cases} x &= \lambda u - (\lambda u)^{p^b}, \\ y &= v, \\ z &= w^s; \end{cases}$$

então

$$\begin{aligned} t(x) &= \sum_{i=0}^{d-1} \left((\lambda u)^{p^{bi}} - (\lambda u)^{p^{b(i+1)}} \right) \\ &= \lambda u - (\lambda u)^q \\ &= \lambda (u^q + u) \\ &= \lambda v^{q+1}; \end{aligned}$$

e

$$z^M = (w^s)^{\frac{q^m+1}{s(q+1)}} = w^{\frac{q^m+1}{q+1}} = v^{q^2} - v.$$

Portanto, os pontos de $\varphi_{a,b,m,s}(\mathcal{C}_m)$ satisfazem (3.1.2). Reciprocamente, se $(x,y,z,1)$ satisfaz (3.1.2), seja u uma raiz do polinômio $\lambda T - (\lambda T)^{p^b} - x \in \mathbb{F}_{q^{2m}}(x)[T]$, e w uma raiz de $T^s - z \in \mathbb{F}_{q^{2m}}(z)[T]$, i.e,

$$x = \lambda u - (\lambda u)^{p^b} \quad \text{e} \quad z = w^s;$$

defina agora, $v = y$; de (3.1.2) temos $(x,y,z,1) \in \mathcal{C}_m$, pois de fato

$$\begin{aligned} \lambda v^{q+1} &= \lambda y^{q+1} \\ &= t(x) \\ &= t\left(\lambda u - (\lambda u)^{p^b} \right) \\ &= \lambda u - (\lambda u)^q \\ &= \lambda (u + u^q); \end{aligned}$$

e

$$w^{\frac{q^m+1}{q+1}} = (w^s)^M = z^M = y^{q^2} - y = v^{q^2} - v;$$

além disso, $(x,y,z,1) = \varphi_{a,b,m,s}(u,v,w,1)$. ■

Notemos que a curva definida por (3.1.2) pode ser singular, portanto $\mathcal{X}_{a,b,m,s}$ é definida como o modelo não singular definido por (3.1.2). No que segue neste capítulo denotaremos

$$\mathcal{X}_{a,b,m,s} := \mathcal{X}.$$

Lema 3.1.3. *A curva $\mathcal{X}$ é $\mathbb{F}_{q^{2m}}-$ birracionalmente equivalente a curva*

$$\mathcal{C}_{\mathcal{X}} : \lambda z^{\frac{q^m+1}{s}} = t(x) \left(t(x)^{q-1} + 1 \right)^{q+1}; \tag{3.1.3}$$

i.e, $\mathbb{F}_{q^{2m}}(\mathcal{X}) = \mathbb{F}_{q^{2m}}(\mathcal{C}_{\mathcal{X}})$.

Dem. De (3.1.2) temos

$$\begin{aligned} z^M &= y^{q^2} - y \\ &= y\left(y^{q^2-1} - 1\right) \\ &= y\left(\left(y^{q+1}\right)^{q-1} - 1\right); \end{aligned}$$

e como $M = \frac{q^m+1}{s(q+1)}$ e $\lambda y^{q+1} = t(x)$, e usando o fato que $\lambda \neq 0$ e $\lambda^q + \lambda = 0$, obtemos

$$\begin{aligned} z^{\frac{q^m+1}{s}} &= y^{q+1}\left(\left(y^{q+1}\right)^{q-1} - 1\right)^{q+1} \\ &= \frac{t(x)}{\lambda}\left(\left(\frac{t(x)}{\lambda}\right)^{q-1} - 1\right)^{q+1} \\ &= t(x)\left(t(x)^{q-1} + 1\right)^{q+1}. \end{aligned}$$

Portanto, $\mathbb{F}_{q^{2m}}(\mathcal{X}) = \mathbb{F}_{q^{2m}}(x, y, z) \supseteq \mathbb{F}_{q^{2m}}(x, z) = \mathbb{F}_{q^{2m}}(\mathcal{C}_{\mathcal{X}})$.

Note que

$$y = \frac{z^M}{y^{q^2-1} - 1} = \frac{z^M}{\left(\frac{t(x)}{\lambda}\right)^{q-1} - 1} \in \mathbb{F}_{q^{2m}}(x, z);$$

em consequência, $\mathbb{F}_{q^{2m}}(\mathcal{X}) = \mathbb{F}_{q^{2m}}(\mathcal{C}_{\mathcal{X}})$. ■

Teorema 3.1.4. *A curva $\mathcal{X}$ é $\mathbb{F}_{q^{2m}}-$ maximal com gênero*

$$g(\mathcal{X}) = \frac{q^{m+2} - p^b q^m - sq^3 + q^2 + (s-1)p^b}{2sp^b}. \tag{3.1.4}$$

Dem. A maximalidade de $\mathcal{X}$ é consequência dos Teoremas 1.2.2, 2.2.4 e da definição 3.1.1.

Para o cálculo do gênero, como $mdc\left(\frac{q^m+1}{s}, p\right) = 1$, então $\mathcal{C}_{\mathcal{X}_{a,b,m,s}}$ definida em (3.1.3) é um recobrimento do tipo Kummer de $\mathbb{P}^1$ de grau $\frac{q^m+1}{s}$. Notemos que $t(x)$ é o traço $tr_{\mathbb{F}_q/\mathbb{F}_{p^b}}(x)$ de $\mathbb{F}_q$ sobre $\mathbb{F}_{p^b}$, portanto é separável com todos seus $\frac{q}{p^b}$ zeros em $\mathbb{F}_q \subseteq \mathbb{F}_{q^{2m}}$. Além disso $t(x)^{q-1} + 1$ também é separavél e

$$\begin{aligned} tr_{\mathbb{F}_{q^2}/\mathbb{F}_{p^b}}(x) &= tr_{\mathbb{F}_{q^2}/\mathbb{F}_p}\left(tr_{\mathbb{F}_q/\mathbb{F}_{p^b}}(x)\right) \\ &= t(x)^q + t(x) \\ &= t(x)\left(t(x)^{q-1} + 1\right). \end{aligned}$$

Concluímos que cada um dos $\frac{q}{p^b}(q-1)$ zeros de $t(x)^{q-1} + 1$ está em $\mathbb{F}_{q^2} \subseteq \mathbb{F}_{q^{2m}}$.

Seja α um zero de $t(x)$. Denotemos por $\mathcal{P}_\alpha$ o lugar de $x - \alpha$, $\mathcal{P}_\infty$ é o polo de x em $\mathbb{F}_{q^{2m}}(x)$ e $f(x) := t(x)\left(t(x)^{q-1} + 1\right)^{q+1}$. Como $grau(f(x)) = \frac{q^3}{p^b}$, temos

$$v_{\mathcal{P}_\beta}(f(x)) = \begin{cases} 1 & \text{se} \quad \beta \text{ é zero de } t(x), \\ q+1 & \text{se} \quad \beta \text{ é zero de } t(x)^{q-1} + 1, \\ \frac{q^3}{p^b} & \text{se} \quad \beta = \infty, \\ 0 & \text{em} \quad \text{outro caso.} \end{cases}$$

Segue-se que

$$r_{\mathcal{P}_\beta}(f(x)) = mdc\left(\frac{q^m+1}{s}, v_{\mathcal{P}_\beta}(f(x))\right) = \begin{cases} 1 & \text{se} \quad \beta \text{ é zero de } t(x), \\ q+1 & \text{se} \quad \beta \text{ é zero de } t(x)^{q-1}+1, \\ 1 & \text{se} \quad \beta = \infty, \\ \frac{q^m+1}{s} & \text{em} \quad \text{outro caso.} \end{cases}$$

Da fórmula do gênero de Riemman Hurwitz e por Corolário 3.7.4 em [25] obtemos

$$\begin{aligned} 2g(\mathcal{X}) - 2 &= \frac{q^m+1}{s}(2g(\mathbb{F}_{q^{2m}}(x)) - 2) + \sum_{\mathcal{P}_\beta}\left(\frac{q^m+1}{s} - r_{\mathcal{P}_\beta}(f(x))\right) \\ &= \frac{q^m+1}{s}\left(\frac{q^2}{p^b} - 1\right) - \left(\frac{q^3}{p^b} + 1\right); \end{aligned}$$

de onde obtemos (3.1.4). ■

Observação 3.1.5. *Na construção da curva $\mathcal{X}$ os maiores valores para b e s são $b = a$ e $s = \frac{q^m+1}{q+1}$. Neste caso substituindo temos*

$$g(\mathcal{X}) = \frac{q^{m+2} - p^b q^m - sq^3 + q^2 + (s-1)p^b}{2sp^b} = 0.$$

Reciprocamente se $g(\mathcal{X}) = 0$, então $q^{m+2} - p^b q^m - sq^3 + q^2 + (s-1)p^b = 0$, ou equivalentemente

$$s = \frac{q^{m+2} - p^b q^m + q^2 - p^b}{q^3 - p^b}.$$

Portanto

$$\begin{aligned} s = \tfrac{q^m+1}{q+1} &\iff (q+1)\left(q^{m+2} - p^b q^m + q^2 - p^b\right) = \left(q^3 - p^b\right)(q^m+1) \\ &\iff q(q^m+1)\left(q - p^b\right) = 0 \\ &\iff q = p^b \\ &\iff a = b. \end{aligned}$$

Quando $a = b$ e $s = \frac{q^m+1}{(q+1)}$ e portanto $g(\mathcal{X}) = 0$, então $\mathbb{F}_{q^{2m}}(\mathcal{X}) = \mathbb{F}_{q^{2m}}(x, y, z)$ é o corpo de funções racionais (Veja [25], Teorema 1.6.3).

3.1.2 Possibilidades de recobrimento pela curva Hermitiana

Teorema 3.1.6. *Seja $q = p^a$ uma potência de um número primo p, seja b um divisor de a e suponha que $q > p^b + p^{2b}$ ou equivalentemente $a \geq 2b+1$, então para $s = 1$ e $m = 3$ a curva $\mathcal{X}$ não é $\mathbb{F}_{q^6}-$ recoberta pela curva Hermitiana $\mathcal{H}_{q^3}$.*

Dem. A prova é similar a prova do Teorema 9 em [12]. Primeiro note que de (3.1.4), como $\mathcal{X}$ é $\mathbb{F}_{q^{2m}}-$ maximal, então

$$\begin{aligned}\#\mathcal{X}\left(\mathbb{F}_{q^{2m}}\right) &= 1+q^{2m}+2q^{m}g\left(\mathcal{X}\right)\\ &= \frac{q^{2m+2}+p^{b}\left(s-1\right)q^{2m}-sq^{m+3}+q^{m+2}+\left(s-1\right)p^{b}q^{m}+sp^{b}}{sp^{b}}.\end{aligned}$$

Agora, pelo Teorema 1.1.11,

$$g\left(\mathcal{H}_{q^{m}}\right)=\frac{q^{2m}-q^{m}}{2}\quad e\quad \#\mathcal{H}_{q^{m}}\left(\mathbb{F}_{q^{2m}}\right)=q^{3m}+1.$$

Suponhamos que exista um recobrimento $\phi:\mathcal{H}_{q^{m}}\longrightarrow\mathcal{X}$ de grau d, pelo Teorema, 1.2.3

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

Notemos que

$$\begin{aligned}\frac{\#\mathcal{H}_{q^{m}}\left(\mathbb{F}_{q^{2m}}\right)}{\#\mathcal{X}\left(\mathbb{F}_{q^{2m}}\right)} &= \frac{q^{3m}+1}{\frac{q^{2m+2}+p^{b}\left(s-1\right)q^{2m}-sq^{m+3}+q^{m+2}+\left(s-1\right)p^{b}q^{m}+sp^{b}}{sp^{b}}}\\ &= \frac{sp^{b}q^{3m}+sp^{b}}{q^{2m+2}+p^{b}\left(s-1\right)q^{2m}-sq^{m+3}+q^{m+2}+\left(s-1\right)p^{b}q^{m}+sp^{b}}\\ &= sp^{b}q^{m-2}+\frac{h}{q^{2m+2}+p^{b}\left(s-1\right)q^{2m}-sq^{m+3}+q^{m+2}+\left(s-1\right)p^{b}q^{m}+sp^{b}};\end{aligned}$$

onde

$$h=-s\left(s-1\right)p^{2b}q^{3m-2}+s^{2}p^{b}q^{2m+1}-sp^{b}q^{2m}-s\left(s-1\right)p^{2b}q^{2m-2}-s^{2}p^{2b}q^{m-2}+sp^{b}.$$

Também temos

$$\begin{aligned}\frac{2g\left(\mathcal{H}_{q^{m}}\right)-2}{2g\left(\mathcal{X}\right)-2} &= \frac{q^{2m}-q^{m}-2}{\frac{q^{m+2}-p^{b}q^{m}-sq^{3}+q^{2}+\left(s-1\right)p^{b}}{sp^{b}}-2}\\ &= \frac{sp^{b}q^{2m}-sp^{b}q^{m}-2sp^{b}}{q^{m+2}-p^{b}q^{m}-sq^{3}+q^{2}-\left(s+1\right)p^{b}}\\ &= sp^{b}q^{m-2}+\frac{sp^{2b}q^{2m-2}+s^{2}p^{b}q^{m+1}-2sp^{b}q^{m}+s\left(s+1\right)p^{2b}q^{m-2}-2sp^{b}}{q^{m+2}-p^{b}q^{m}-sq^{3}+q^{2}-\left(s+1\right)p^{b}}.\end{aligned}$$

Se $m=3$ e $s=1$ então

$$\frac{\#\mathcal{H}_{q^{3}}\left(\mathbb{F}_{q^{6}}\right)}{\#\mathcal{X}\left(\mathbb{F}_{q^{6}}\right)}=p^{b}q+v;$$

e

$$\frac{2g\left(\mathcal{H}_{q^{3}}\right)-2}{2g\left(\mathcal{X}_{a,b,3,1}\right)-2}=p^{b}q+u;$$

onde

$$v = \frac{p^b q^7 - p^b q^6 - p^{2b} q + p^b}{q^8 - q^6 + q^5 + p^b} \quad \text{e} \quad u = \frac{\left(p^{2b} + p^b\right) q^4 - 2p^b q^3 + 2p^{2b} q - 2p^b}{q^5 - p^b q^3 - q^3 + q^2 - 2p^b}.$$

Como $p^b q^7 - p^b q^6 - p^{2b} q + p^b > 0$ e $q^8 - q^6 + q^5 + p^b > 0$, temos que $v > 0$.

Para u, note que $\left(p^b + 1\right) q^4 + 2p^b q > 2\left(q^3 + 1\right)$, em consequência

$$\left(p^{2b} + p^b\right) q^4 - 2p^b q^3 + 2p^{2b} q - 2p^b > 0.$$

Agora, como $q > p^b + p^{2b} > 2$ temos $q^5 + q^2 > \left(p^b + 1\right) q^3 + 2p^b$, de onde obtemos $q^5 - p^b q^3 - q^3 + q^2 - 2p^b > 0$. Novamente usando a condição $q > p^b + p^{2b}$ temos $\left(p^{2b} + p^b\right) q^4 + q^3 + 2p^{2b} q < q^5 + p^b q^3 + q^2$, ou equivalentemente $u < 1$. Segue-se que

$$p^b q < p^b q + v \leq d \leq p^b q + u < p^b q + 1;$$

que é uma contradição, pois $d = grau\left(\phi\right) \in \mathbb{N}$. ■

O seguinte teorema é uma ferramenta que permite obter informação adicional sobre a possibilidade de recobrimento de Galois da curva $\mathcal{X}$ pela curva Hermitiana para outros parâmetros. De fato completa a melhor informação que podemos obter até agora para $\mathcal{X}$ com relação a recobrimentos pela curva Hermitiana.

Teorema 3.1.7. *Seja $\mathcal{Y}$ uma curva $\mathbb{F}_{q^{2m}}-$ maximal. Suponha que existem A, $B \in \mathbb{N}$, $k \in \mathbb{R}^+$ tais que*

$$2g\left(\mathcal{Y}\right) - 2 = A\left(q^m + 1\right) - B;$$

com $1 \leq B \leq q^m + 1$, $k\left(A + 1\right) < B$ e $A + 2 < B$. Se existe $\phi : \mathcal{H}_{q^m} \longrightarrow \mathcal{Y}$ um $\mathbb{F}_{q^{2m}}-$ recobrimento de Galois de grau d onde $\mathcal{H}_{q^m}$ é a curva Hermitiana sobre $\mathbb{F}_{q^{2m}}$, então $dB \geq \left(k + 1\right)\left(q^m + 1\right)$.

Dem. Ver [4], Proposição 5.1. ■

Teorema 3.1.8. *Se $a > b$, $m > 3$ e $s = 1$, então a curva $\mathcal{X}$ não é $\mathbb{F}_{q^{2m}}-$ Galois recoberta pela curva Hermitiana $\mathcal{H}_{q^m}$.*

Dem. Para $s = 1$ temos

$$g\left(\mathcal{X}\right) = \frac{q^{m+2} - p^b q^m - q^3 + q^2}{2p^b}.$$

Agora

$$\begin{aligned} 2g\left(\mathcal{X}\right) - 2 &= \frac{q^{m+2} - p^b q^m - q^3 + q^2 - 2p^b}{p^b} \\ &= \frac{\left(q^m + 1\right)\left(q^2 - p^b\right) - \left(q^3 + p^b\right)}{p^b} \\ &= A\left(q^m + 1\right) - B; \end{aligned}$$

com $A = \frac{q^2-p^b}{p^b}$, $B = \frac{q^3+p^b}{p^b}$, note-se que A, $B \in \mathbb{N}$.

Como

$$A + 2 = \frac{q^2 + p^b}{p^b} < \frac{q^3 + p^b}{p^b} = B;$$

$$1 \leq B = \frac{q^3}{p^b} + 1 \leq q^m + 1;$$

para cada $m \geq 3$.

Além disso, para $k = q$

$$k\,(A+1) = \frac{q^3}{p^b} < \frac{q^3}{p^b} + 1 = B.$$

Se existe $\phi : \mathcal{H}_{q^m} \longrightarrow \mathcal{X}$ um $\mathbb{F}_{q^{2m}}-$ recobrimento de Galois de grau d, por o Teorema 3.1.7

$$\begin{aligned} d &\geq \frac{(k+1)\,(q^m+1)}{B} \\ &= \frac{p^b q^{m+1} + p^b q^m + p^b q + p^b}{q^3 + p^b} \\ &= p^b q^{m-2} + \frac{p^b q^m - p^{2b} q^{m-2} + p^b q + p^b}{q^3 + p^b} \end{aligned}$$

Do Teorema 1.2.3 também

$$\begin{aligned} d &\leq \frac{2g\,(\mathcal{H}_{q^3}) - 2}{2g\,(\mathcal{X}) - 2} \\ &= p^b q^{m-2} + \frac{p^{2b} q^{2m-2} + p^b q^{m+1} - 2p^b q^m + 2p^{2b} q^{m-2} - 2p^b}{q^{m+2} - p^b q^m - q^3 + q^2 - 2p^b}; \end{aligned}$$

segue-se que

$$\frac{p^b q^m - p^{2b} q^{m-2} + p^b q + p^b}{q^3 + p^b} \leq \frac{p^{2b} q^{2m-2} + p^b q^{m+1} - 2p^b q^m + 2p^{2b} q^{m-2} - 2p^b}{q^{m+2} - p^b q^m - q^3 + q^2 - 2p^b};$$

ou equivalentemente

$$q^{2m+2} + 2q^{m+3} + 2q^{m+2} + 2q^3 + q^2 \leq p^b q^{2m+1} + 2p^b q^{2m} + q^{m+4} + 3p^b q^{m+1} + 2p^b q^m + q^4 + 2p^b q. \quad (3.1.5)$$

Note que para $m > 3$ e $a > b$

$$q^{2m+2} \geq p^b q^{2m+1} + 2p^b q^{2m} + q^{m+4};$$

pois $q^2 - p^b - 2p^b \geq 1$ e $2m \geq m + 4$.

Também $2q^{m+3} > 3p^b q^{m+1}$, $2q^3 + q^2 > 2p^b q$ e

$$2q^{m+2} = q^{m+2} + q^{m+2} > 2p^b q^m + q^4;$$

portanto (3.1.5) é falsa, i.e, $\mathcal{X}$ não é $\mathbb{F}_{q^{2m}}-$ Galois recoberta pela curva Hermitana $\mathcal{H}_{q^m}$. ■

3.2 A curva $\mathcal{Y}_{m,s}$

Apresentamos agora outra curva com propriedades muito similares à curva definida na seção anterior. As provas de alguns resultados são parecidas com as provas feitas para a curva $\mathcal{X}$.

3.2.1 Definição e maximalidade de $\mathcal{Y}_{m,s}$

Consideremos os seguintes parâmetros:

- $m \geq 3$ ímpar;
- q uma potência de um primo p;
- $s \geq 1$ um divisor de $\frac{q^m+1}{q+1}$.

Definamos o morfismo

$$\begin{array}{rccl} \varphi_{m,s}: & \mathcal{C}_m & \longrightarrow & \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right) \\ & (u,v,w,1) & \longmapsto & (x:y:z:1) := (u:v:w^s:1)\,; \end{array} \tag{3.2.1}$$

onde novamente $\mathcal{C}_m$ é a curva GGS definida em (2.2.1).

Definição 3.2.1. *A curva $\mathcal{Y}_{m,s}$ é definida como o modelo não singular de $\varphi_{m,s}(\mathcal{C}_m) \subseteq \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$.*

Explicitamente.

Lema 3.2.2. *A curva $\varphi_{m,s}(\mathcal{C}_m)$ tem equações afins*

$$y^{q+1} = x^q + x \quad e \quad z^M = y^{q^2} - y; \tag{3.2.2}$$

onde $M = \frac{q^m+1}{s(q+1)}$ como na seção anterior.

Dem. Para $(u,v,w,1) \in \mathcal{C}_m$, i.e,

$$u^q + u = v^{q+1} \quad \text{e} \quad w^{\frac{q^m+1}{q+1}} = v^{q^2} - v.$$

Seja

$$\left\{ \begin{array}{rcl} x & = & u, \\ y & = & v, \\ z & = & w^s; \end{array} \right.$$

então

$$y^{q+1} = v^{q+1} = u^q + u = x^q + x;$$

e

$$z^M = \left(w^s\right)^{\frac{q^m+1}{s(q+1)}} = w^{\frac{q^m+1}{q+1}} = v^{q^2} - v;$$

portanto, os pontos de $\varphi_{m,s}(\mathcal{C}_m)$ satisfazem (3.2.2).

Reciprocamente, se $(x,y,z,1)$ satisfaz (3.2.2), seja w uma raiz de $T^s - z \in \mathbb{F}_{q^{2m}}(z)[T]$, i.e $z = w^s$ e defina $u = x$ e $y = v$, note-se que de (3.2.2) temos trivialmente que $(u,v,w,1) \in \mathcal{C}_m$, e $(x,y,z,1) = \varphi_{m,s}(u,v,w,1)$. ■

Notemos que a curva definida por (3.2.2) pode ser singular, portanto $\mathcal{Y}_{m,s}$ deve-se definir como o modelo não singular da curva determinado por (3.2.2). No que segue neste capítulo denotaremos

$$\mathcal{Y}_{m,s} := \mathcal{Y}.$$

Lema 3.2.3. *A curva $\mathcal{Y}$ é $\mathbb{F}_{q^{2m}}-$ birracionalmente equivalente à curva*

$$\mathcal{C}_{\mathcal{Y}} : z^{\frac{q^m+1}{s}} = (x^q + x)\left((x^q + x)^{q-1} + 1\right)^{q+1}; \tag{3.2.3}$$

i.e, $\mathbb{F}_{q^{2m}}(\mathcal{Y}) = \mathbb{F}_{q^{2m}}(\mathcal{C}_{\mathcal{Y}})$.

Dem. Análoga à demonstração De 3.1.3, só mudando $cy^{q+1} = t(x)$ por $y^{q+1} = x^q + x$. ■

Teorema 3.2.4. *A curva $\mathcal{Y}$ é $\mathbb{F}_{q^{2m}}-$ maximal, com gênero*

$$g(\mathcal{Y}) = \frac{q^{m+2} - q^m - sq^3 + q^2 + (s-1)}{2s}. \tag{3.2.4}$$

Dem. Novamente a maximalidade de $\mathcal{Y}$ é consequência dos Teoremas 1.2.2, 2.2.1 e da definição 3.2.1.

Para o cálculo do gênero, como $mdc\left(\frac{q^m+1}{s}, p\right) = 1$, então $\mathcal{C}_{\mathcal{Y}}$ definida em (3.1.3) é um recobrimento do tipo Kummer de $\mathbb{P}^1$ de grau $\frac{q^m+1}{s}$.

Seja

$$t(x) := x^q + x = tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x).$$

Note que $t(x)$ é separável e tem todos seus q zeros em $\mathbb{F}_{q^2} \subseteq \mathbb{F}_{q^{2m}}$. Além disso

$$\begin{aligned} t(x)\left(t(x)^{q-1} + 1\right) &= t(x)^q + t(x) \\ &= tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(t(x)) \\ &= tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}\left(tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x)\right), \end{aligned}$$

portanto cada uns dos $q(q-1)$ zeros de $t(x)^{q-1} + 1$ estão ém $\mathbb{F}_{q^2}$. Com a mesma notação da demonstração do Teorema 3.1.4,

Seja α um zero de $t(x)$. Denotemos por $\mathcal{P}_\alpha$ o lugar de $x - \alpha$, $\mathcal{P}_\infty$ é o polo de x em $\mathbb{F}_{q^{2m}}(x)$ e $f(x) := t(x)\left(t(x)^{q-1} + 1\right)^{q+1}$. Como $grau(f(x)) = q^3$, temos

$$v_{\mathcal{P}_\beta}(f(x)) = \begin{cases} 1 & \text{se} \quad \beta \text{ é zero de } t(x), \\ q+1 & \text{se} \quad \beta \text{ é zero de } t(x)^{q-1} + 1, \\ q^3 & \text{se} \quad \beta = \infty, \\ 0 & \text{em} \quad \text{outro caso;} \end{cases}$$

portanto

$$r_{\mathcal{P}_\beta}(f(x)) = mdc\left(\frac{q^m+1}{s},\ v_{\mathcal{P}_\beta}(f(x))\right) = \begin{cases} 1 & \text{se} \quad \beta \text{ é zero de } t(x), \\ q+1 & \text{se} \quad \beta \text{ é zero de } t(x)^{q-1}+1, \\ 1 & \text{se} \quad \beta = \infty, \\ \frac{q^m+1}{s} & \text{em} \quad \text{outro caso.} \end{cases}$$

Pela fórmula do gênero de Riemman Hurwitz e por Corolário 3.7.4 em [25]

$$\begin{aligned} 2g(\mathcal{Y}) - 2 &= \frac{q^m+1}{s}\left(2g\left(\mathbb{F}_{q^{2m}}(x)\right) - 2\right) + \sum_{\mathcal{P}_\beta}\left(\frac{q^m+1}{s} - r_{\mathcal{P}_\beta}(f(x))\right) \\ &= \frac{q^m+1}{s}\left(q^2-1\right) - \left(q^3+1\right); \end{aligned}$$

de onde obtemos (3.2.4). ■

Observação 3.2.5. *Notemos que por cálculos simples*

$$\begin{aligned} g(\mathcal{Y}) = \frac{q(q-1)}{2} &\iff (q^m+1)(q^2-1) = s(q+1)(q^2-1) \\ &\iff s = \frac{q^m+1}{q+1}. \end{aligned}$$

3.2.2 Possibilidades de recobrimento pela curva Hermitiana

Teorema 3.2.6. *Seja q uma potência de um primo e s um divisor de q^2-q+1 tal que $q > s(s+1)$. Então a curva $\mathcal{Y}_{3,s}$ não é $\mathbb{F}_{q^6}-$ recoberta pela curva Hermitiana $\mathcal{H}_{q^3}$.*

Dem. Como $\mathcal{Y}$ é $\mathbb{F}_{q^{2m}}-$ maximal então por (3.2.4), temos

$$\begin{aligned} \#\mathcal{Y}\left(\mathbb{F}_{q^{2m}}\right) &= 1 + q^{2m} + 2q^m g(\mathcal{Y}) \\ &= \frac{q^{2m+2} + (s-1)q^{2m} - sq^{m+3} + q^{m+2} + (s-1)q^m + s}{s}. \end{aligned}$$

Vamos supor que existe um recobrimento $\phi : \mathcal{H}_{q^m} \longrightarrow \mathcal{Y}$ de grau d. Pelo Lema 1.2.3 temos

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

Agora

$$\begin{aligned} \frac{\#\mathcal{H}_{q^m}\left(\mathbb{F}_{q^{2m}}\right)}{\#\mathcal{Y}\left(\mathbb{F}_{q^{2m}}\right)} &= \frac{q^{3m}+1}{\frac{q^{2m+2} + (s-1)q^{2m} - sq^{m+3} + q^{m+2} + (s-1)q^m + s}{s}} \\ &= \frac{sq^{3m}+s}{q^{2m+2} + (s-1)q^{2m} - sq^{m+3} + q^{m+2} + (s-1)q^m + s} \\ &= sq^{m-2} + \frac{-(s-1)sq^{3m-2} + s^2q^{2m+1} - sq^{2m} - (s-1)sq^{2m-2} - s^2q^{m-2} + s}{q^{2m+2} + (s-1)q^{2m} - sq^{m+3} + q^{m+2} + (s-1)q^m + s}, \end{aligned}$$

e

$$\begin{aligned}\frac{2g\left(\mathcal{H}_{q^m}\right)-2}{2g\left(\mathcal{Y}\right)-2} &= \frac{q^{2m}-q^m-2}{\dfrac{q^{m+2}-q^m-sq^3+q^2+(s-1)}{s}-2} \\ &= \frac{sq^{2m}-sq^m-2s}{q^{m+2}-q^m-sq^3+q^2-(s+1)} \\ &= sq^{m-2}+\frac{sq^{2m-2}+s^2q^{m+1}-2sq^m+s\left(s+1\right)q^{m-2}-2s}{q^{m+2}-q^m-sq^3+q^2-(s+1)}.\end{aligned}$$

Para $m=3$ temos

$$\frac{\#\mathcal{H}_{q^3}\left(\mathbb{F}_{q^6}\right)}{\#\mathcal{Y}\left(\mathbb{F}_{q^6}\right)} = sq+\frac{sq^7-sq^6-\left(s-1\right)sq^4-s^2q+s}{q^8-q^6+q^5+\left(s-1\right)q^3+s}; \tag{3.2.5}$$

e

$$\frac{2g\left(\mathcal{H}_{q^3}\right)-2}{2g\left(\mathcal{Y}\right)-2} = sq+\frac{s\left(s+1\right)q^4-2sq^3+s\left(s+1\right)q-2s}{q^5-\left(s+1\right)q^3+q^2-(s+1)}. \tag{3.2.6}$$

Em (3.2.5) temos

$$sq^7-sq^6-\left(s-1\right)sq^4-s^2q+s>0 \iff q^7+q^4+1>q^6+sq^4+sq;$$

como $q>s\left(s+1\right)$, portanto $q>s$, temos $q^7+q^4+1>q^6+sq^4+sq$.

Agora

$$q^8-q^6+q^5+\left(s-1\right)q^3+s>0;$$

e trivialmente verdadeiro. Segue-se que

$$\frac{sq^7-sq^6-\left(s-1\right)sq^4-s^2q+s}{q^8-q^6+q^5+\left(s-1\right)q^3+s}>0.$$

Para (3.2.6), note que

$$s\left(s+1\right)q^4-2sq^3+s\left(s+1\right)q-2s>0 \iff \left(s+1\right)q^4+\left(s+1\right)q>2q^3+s;$$

é trivialmente temos que $\left(s+1\right)q^4+\left(s+1\right)q>2q^3+s$ é verdadeiro.

Também

$$q^5-\left(s+1\right)q^3+q^2-(s+1)>0;$$

pois $q>s\left(s+1\right)\geq s+1$. Consequentemente em (3.2.6) a fração tem numerador e denominador positivo, portanto

$$\frac{s\left(s+1\right)q^4-2sq^3+s\left(s+1\right)q-2s}{q^5-\left(s+1\right)q^3+q^2-(s+1)}<1 \iff s\left(s+1\right)q^4+s\left(s+1\right)q<q^5+\left(s-1\right)q^3+q^2+\left(s-1\right),$$

e esta última desigualdade é verdadeira para $q>s\left(s+1\right)\geq s+1$.

Obtemos assim

$$sq<\frac{\#\mathcal{H}_{q^3}\left(\mathbb{F}_{q^6}\right)}{\#\mathcal{Y}\left(\mathbb{F}_{q^6}\right)}\leq d\leq\frac{2g\left(\mathcal{H}_{q^3}\right)-2}{2g\left(\mathcal{Y}\right)-2}<sq+1;$$

que de fato é uma contradição. ■

Capítulo 4

Alguns AG códigos associados

Nosso objetivo neste capítulo é apresentar algumas aplicações dos resultados obtidos com relação as curvas $\mathcal{X}_{a,b,m,s}$ e $\mathcal{Y}_{m,s}$. Estamos interessados especialmente em calcular alguns AG códigos num ponto racional destas curvas, e comparar os parâmetros obtidos com os parâmetros dos códigos existentes na teoria. Iniciamos este capítulo com uma descrição geral dos AG códigos e códigos unipontuais, depois calcularemos alguns exemplos deles para nossas curvas.

4.1 AG códigos e codigos unipontuais

Nesta seção apresentamos alguns resultados básicos sobre códigos algébricos, a maior parte provados no capitulo 2 de [25].

Seja $\mathcal{C}$ uma curva definida sobre $\mathbb{F}_q$ de gênero g e consideremos $P_1, P_2, ..., P_n \in \mathcal{C}(\mathbb{F}_q)$, e defina o divisor $D = P_1 + P_2 + ... + P_n$. Seja G algum outro divisor tal que $Sup(D) \cap Sup(G) = \varnothing$. O **código algébrico** (AG **código**) ou **código de Goppa** $C(D,G)$ de **comprimento** n sobre $\mathbb{F}_q$ é a imagem da função

$$\begin{array}{rccc} \Omega: & \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & (f(P_1), f(P_2), ..., f(P_n)). \end{array} \tag{4.1.1}$$

$\mathbb{F}_q$ é chamado o o **alfabeto** de $C(D,G)$, e a dimensão do subespaço $C(D,G)$ que denotaremos por

$$k := \dim_{\mathbb{F}_q}(C(D,G))$$

é chamada **dimensão** do código $C(D,G)$. A **distancia mínima** de $C(D,G)$ é definida como

$$d = d(C(D,G)) := \min\{d(a,b) : a, b \in C(D,G)\},$$

onde para $a = (a_1, .., a_n)$, $b = (b_1, .., b_n) \in C(D,G) : d(a,b) = \#\{i : a_i \neq b_i\}$.

O código acima de comprimento n, dimensão k e distancia mínima d é chamado um $[n,k,d]$ código. Neste caso

$$k + d \leq n + 1 \tag{4.1.2}$$

que chamaremos a **cota singleton**.

A função Ω é $\mathbb{F}_q-$ linear com $\ker(\Omega) = \mathcal{L}(G-D)$, portanto

$$k = \ell(G) - \ell(G-D) \quad \text{e} \quad d \geq n - grau(G). \tag{4.1.3}$$

De (4.1.2) e (4.1.3) temos

$$n - grau(G) \leq d \leq n + 1 - k. \tag{4.1.4}$$

Se $grau(G-D) < 0$, i.e., $grau(G) < n$, por [25], Lema 1.4.7, $\mathcal{L}(G-D) = \{0\}$ e portanto $\ell(G-D) = 0$, em consequência $k = \ell(G)$. Novamente por [25], Lema 1.5.15 existe um divisor canônico W, i.e., $grau(W) = 2g-2$ e $\ell(W) = g$, tal que

$$k = \ell(G) = grau(G) + 1 - g + \ell(W-G). \tag{4.1.5}$$

Novamente por [25], Lema 1.4.7 se $2g-2 = grau(W) < grau(G) < n$ então

$$k = grau(G) + 1 - g. \tag{4.1.6}$$

A **matriz geradora** de $C(D,G)$ é

$$M = \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & & \vdots \\ f_k(P_1) & \dots & f_k(P_n) \end{pmatrix};$$

onde $f_1, .., f_k$ é uma base de $\mathcal{L}(G)$ sobre $\mathbb{F}_q$.

Para $a = (a_1, .., a_n)$, $b = (b_1, .., b_n) \in \mathbb{F}_q^n$ definimos:

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i.$$

$\langle , \rangle$ é o produto interno canônico em $\mathbb{F}_q^n$, portanto o $[n,k,d]$ código $C(D,G)$ tem um complemento ortogonal que denotaremos por $C^{\perp}(D,G)$, que chamaremos o **código dual** de $C(D,G)$. Temos que $C^{\perp}(D,G)$ é um $\left[n, k^{\perp}, d^{\perp}\right]$ onde

$$k^{\perp} = \dim_{\mathbb{F}_{q^2}}\left(C^{\perp}(D,G)\right) = n - k \tag{4.1.7}$$

e

$$d^{\perp} \geq grau(G) - (2g-2). \tag{4.1.8}$$

Como também temos $k^{\perp} + d^{\perp} \leq n+1$, obtemos

$$grau(G) - (2g-2) \leq d^{\perp} \leq k+1. \tag{4.1.9}$$

Analogamente se $2g-2 < grau(G) < n$:

$$k^{\perp} = n + g - 1 - grau(G).$$

Em particular se $G = hP$ para algum $P \in \mathcal{C}(\mathbb{F}_{q^2})$ e $h \in \mathbb{N}$, os AG códigos $C(D,G)$ e $C^{\perp}(D,G)$ são chamados AG **códigos unipontuais**.

4.2 AG códigos e códigos das curvas $\mathcal{X}_{a,b,m,s}$ e $\mathcal{Y}_{m,s}$

No que segue neste capítulo fixaremos a seguinte notação:

- $a, b, s \in \mathbb{N}$; $q = p^a$, com p primo.
- Quando é necessário b é um divisor de a e $d = \frac{a}{b}$.
- m ímpar ≥ 3.
- $s \geq 1$ um divisor de $\frac{q^m+1}{q+1}$ e $M = \frac{q^m+1}{s(q+1)}$.
- $\mathcal{C} = \mathcal{X}_{a,b,m,s} := \mathcal{X}$ ou $\mathcal{C} = \mathcal{Y}_{m,s} := \mathcal{Y}$, definidas como em (3.1.2) e (3.2.2).
- $g = g(\mathcal{C})$ o gênero de $\mathcal{C}$.
- $\varphi := \varphi_{a,b,m,s}$ ou $\varphi_{m,s} : \mathcal{C}_m \longrightarrow \mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$ os morfismos definidos em (3.1.1) e (3.2.1). Notemos que
$$grau(\varphi) = \begin{cases} sp^m & \text{se } \mathcal{C} = \mathcal{X}, \\ s & \text{se } \mathcal{C} = \mathcal{Y}. \end{cases}$$

4.2.1 Semigrupos de Weierstrass em um ponto das curvas $\mathcal{X}_{a,b,m,s}$ e $\mathcal{Y}_{m,s}$

Lema 4.2.1. *A curva $\mathcal{C}$ tem um único ponto no infinito $P_0 \in \mathcal{C}(\mathbb{F}_{q^{2m}})$, que de fato é o único polo comum de x, y, z, i.e, $\#\varphi^{-1}(P_0) = 1$. Além disso:*

- *Para $\mathcal{C} = \mathcal{X}_{a,b,m,s}$:*
$$\begin{aligned} \mathrm{div}_\infty(x) &= (q+1)MP_0; \\ \mathrm{div}_\infty(y) &= \frac{q}{p^b}MP_0; \\ \mathrm{div}_\infty(z) &= \frac{q^3}{p^b}P_0. \end{aligned}$$
- $\mathcal{C} = \mathcal{Y}_{m,s}$:
$$\begin{aligned} \mathrm{div}_\infty(x) &= (q+1)MP_0; \\ \mathrm{div}_\infty(y) &= qMP_0; \\ \mathrm{div}_\infty(z) &= q^3P_0. \end{aligned}$$

Dem. Para $\mathcal{C} = \mathcal{X}$:

Homogeneizando $\mathcal{X}$ temos

$$\widetilde{\mathcal{X}} : \lambda Y^{q+1} = W^{q+1}t\left(\frac{X}{W}\right) \quad \text{e} \quad Z^M = W^{M-q^2}Y^{q^2} - W^{M-1}Y.$$

Se $W=0$, das equações acima temos $Y=Z=0$, portanto $X_\infty=(1:0:0:0)$ é o único no infinito de $\mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$ tal que $X_\infty\in\mathcal{X}$. Defina $P_0:=X_\infty\in\mathcal{X}\left(\mathbb{F}_{q^{2m}}\right)$.

Consideremos os corpos de funções $K=\mathbb{F}_{q^{2m}}(x)$ e

$$\begin{aligned} F &= \mathbb{F}_{q^{2m}}(x,y):\lambda y^{q+1}=t(x); \\ \widetilde{F} &= \mathbb{F}_{q^{2m}}(x,y,z):z^M=y^{q^2}-y; \end{aligned}$$

i.e, temos a torre de corpos de funções algébricas $K\subset F\subset\widetilde{F}$ e cada uma das extensões $\widetilde{F}/F$ e F/K é do tipo Kummer.

A prova é consequência direta das duas afirmações seguintes.

Afirmação 4.2.2. *O polo $\mathcal{P}_\infty$ de x em K é totalmente ramificado em F; se $\mathcal{Q}_\infty$ denota o único lugar em F tal que $\mathcal{Q}_\infty/\mathcal{P}_\infty$ então*

- $e\left(\mathcal{Q}_\infty/\mathcal{P}_\infty\right)=q+1$;
- $v_{\mathcal{Q}_\infty}(x)=-(q+1)$;
- $v_{\mathcal{Q}_\infty}(y)=-\frac{q}{p^b}$.
- *Se $\mathcal{Q}$ é um lugar em F tal que $v_{\mathcal{Q}}(x)<0$ ou $v_{\mathcal{Q}}(y)<0$, então $\mathcal{Q}=\mathcal{Q}_\infty$, i.e, x e y tem o mesmo polo $\mathcal{Q}_\infty$ em F.*

De fato $v_{\mathcal{P}_\infty}(t(x))=-\frac{q}{p^b}$, pois $grau(t(x))=\frac{q}{p^b}$ e $\mathcal{P}_\infty$ é o polo de x em K, além disso $[F:K]=q+1$, portanto

$$r_{\mathcal{P}_\infty}=mdc\left([F:K],\ v_{\mathcal{P}_\infty}(t(x))\right)=1;$$

em consequência $\mathcal{P}_\infty$ é totalmente ramificado em F, (veja [25], Proposição 3.7.3).

Seja $\mathcal{Q}_\infty$ o único lugar em F tal que $\mathcal{Q}_\infty/\mathcal{P}_\infty$, então $e\left(\mathcal{Q}_\infty/\mathcal{P}_\infty\right)=[F:K]$; agora

$$\begin{aligned} v_{\mathcal{Q}_\infty}(x) &= e\left(\mathcal{Q}_\infty/\mathcal{P}_\infty\right)v_{\mathcal{P}_\infty}(x) \\ &= -(q+1). \end{aligned}$$

Como

$$\begin{aligned} (q+1)\,v_{\mathcal{Q}_\infty}(y) &= v_{\mathcal{Q}_\infty}\left(\lambda y^{q+1}\right) \\ &= v_{\mathcal{Q}_\infty}(t(x)) \\ &= e\left(\mathcal{Q}_\infty/\mathcal{P}_\infty\right)v_{\mathcal{P}_\infty}(t(x)); \end{aligned}$$

então $v_{\mathcal{Q}_\infty}(y)=-\frac{q}{p^b}$.

Note-se que $\mathcal{P}\in\mathbb{P}_K$ e $\mathcal{P}\neq\mathcal{P}_\infty$ então $v_{\mathcal{P}}(t(x))\geq 0$. Seja $\mathcal{Q}$ um lugar em F e $\mathcal{P}$ um lugar em K tal que $\mathcal{Q}/\mathcal{P}$, como $v_{\mathcal{Q}}(x)=e\left(\mathcal{Q}/\mathcal{P}\right)v_{\mathcal{P}}(x)$; se $v_{\mathcal{Q}}(x)<0$ então, $\mathcal{P}=\mathcal{P}_\infty$ e assim, $\mathcal{Q}=\mathcal{Q}_\infty$. Se $v_{\mathcal{Q}}(y)<0$, então $v_{\mathcal{P}}(t(x))<0$ e portanto $\mathcal{P}=\mathcal{P}_\infty$, em consequência $\mathcal{Q}=\mathcal{Q}_\infty$.

Afirmação 4.2.3. *O polo comum $\mathcal{Q}_\infty$ de x e y em F é totalmente ramificado em $\widetilde{F}$; se $\widetilde{\mathcal{Q}}_\infty$ denota o único lugar em $\widetilde{F}$ tal que $\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty$ então*

- $e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right) = M$;
- $v_{\widetilde{\mathcal{Q}}_\infty}(x) = -(q+1)M$;
- $v_{\widetilde{\mathcal{Q}}_\infty}(y) = -\frac{q}{p^b}M$;
- $v_{\widetilde{\mathcal{Q}}_\infty}(z) = -\frac{q^3}{p^b}$;
- *Se $\widetilde{\mathcal{Q}}$ é um lugar em F tal que $v_{\widetilde{\mathcal{Q}}}(x) < 0$ ou $v_{\widetilde{\mathcal{Q}}}(y) < 0$ ou $v_{\widetilde{\mathcal{Q}}}(z) < 0$, então $\widetilde{\mathcal{Q}} = \widetilde{\mathcal{Q}}_\infty$. i.e, x, y, z têm o mesmo polo $\widetilde{\mathcal{Q}}_\infty$ em $\widetilde{F}$.*

Seja $u = y^{q^2} - y$; como $v_{\mathcal{Q}_\infty}(y) = -\frac{q}{p^b}$ então

$$\begin{aligned} v_{\mathcal{Q}_\infty}(u) &= \min\left\{v_{\mathcal{Q}_\infty}(y),\ v_{\mathcal{Q}_\infty}\left(y^{q^2}\right)\right\} \\ &= -\frac{q^3}{p^b}. \end{aligned}$$

Como, $\left[\widetilde{F}:F\right] = M$ e $r_{\mathcal{Q}_\infty}(u) = mdc\left(\left[\widetilde{F}:F\right],\ v_{\mathcal{Q}_\infty}(u)\right) = 1$, portanto $\mathcal{Q}_\infty$ é totalmente ramificado em $\widetilde{F}$; se $\widetilde{\mathcal{Q}}_\infty$ é o único lugar em $\widetilde{F}$ tal que $\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty$ então

$$e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right) = \left[\widetilde{F}:F\right] = M.$$

Agora

$$\begin{aligned} v_{\widetilde{\mathcal{Q}}_\infty}(x) &= e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right) e\left(\mathcal{Q}_\infty/\mathcal{P}_\infty\right) v_{\mathcal{P}_\infty}(x) \\ &= -(q+1)M. \end{aligned}$$

Também

$$\begin{aligned} v_{\widetilde{\mathcal{Q}}_\infty}(y) &= e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right) v_{\mathcal{Q}_\infty}(y) \\ &= -\frac{q}{p^b}M. \end{aligned}$$

Da condição $z^M = y^{q^2} - y$ temos

$$\begin{aligned} M v_{\widetilde{\mathcal{Q}}_\infty}(z) &= v_{\widetilde{\mathcal{Q}}_\infty}\left(y^{q^2} - y\right) \\ &= e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right) v_{\mathcal{Q}_\infty}\left(y^{q^2} - y\right) \\ &= -\frac{q^3}{p^b}M. \end{aligned}$$

Finalmente, seja $\widetilde{\mathcal{Q}}$ um lugar de $\widetilde{F}$ e suponhamos que $\mathcal{Q} \in \mathbb{P}_F$ e $\mathcal{P} \in \mathbb{P}_K$ tal que $\widetilde{\mathcal{Q}}/\mathcal{Q}$ e $\mathcal{Q}/\mathcal{P}$, usando os fatos

$$\begin{aligned} v_{\widetilde{\mathcal{Q}}}(x) &= e\left(\widetilde{\mathcal{Q}}/\mathcal{Q}\right) e\left(\mathcal{Q}/\mathcal{P}\right) v_{\mathcal{P}}(x); \\ v_{\widetilde{\mathcal{Q}}}(y) &= e\left(\widetilde{\mathcal{Q}}/\mathcal{Q}\right) v_{\mathcal{Q}}(y); \end{aligned}$$

se $v_{\widetilde{\mathcal{Q}}}(x) < 0$, então $v_{\mathcal{P}}(x) < 0$, portanto $\mathcal{P} = \mathcal{P}_\infty$, segue-se que $\mathcal{Q} = \mathcal{Q}_\infty$ e $\widetilde{\mathcal{Q}} = \widetilde{\mathcal{Q}}_\infty$. Se $v_{\widetilde{\mathcal{Q}}}(y) < 0$, então $v_{\mathcal{Q}}(y) < 0$, e pela última parte da afirmação anterior temos $\mathcal{Q} = \mathcal{Q}_\infty$, portanto $\widetilde{\mathcal{Q}} = \widetilde{\mathcal{Q}}_\infty$.

Para $v_{\widetilde{\mathcal{Q}}}(z)$, como $Mv_{\widetilde{\mathcal{Q}}}(z) = e\left(\widetilde{\mathcal{Q}}/\mathcal{Q}\right) v_{\mathcal{Q}}\left(y^{q^2} - y\right)$, é suficiente provar que $v_{\mathcal{Q}}\left(y^{q^2} - y\right) \geq 0$, para cada $\mathcal{Q} \in \mathbb{P}_F$, com $\mathcal{Q} \neq \mathcal{Q}_\infty$. De fato se $\mathcal{P} \in \mathbb{P}_K$ com $\mathcal{Q}/\mathcal{P}$, então $\mathcal{P} \neq \mathcal{P}_\infty$, portanto $v_{\mathcal{P}}(x) \geq 0$, então $v_{\mathcal{Q}}(y) \geq 0$, segue-se que $v_{\mathcal{Q}}\left(y^{q^2} - y\right) \geq \min\left\{v_{\mathcal{Q}}(y), q^2 v_{\mathcal{Q}}(y)\right\} \geq 0$.

Dos cálculos acima, P_0 é único polo comum de x, y, z em $\mathcal{X}$, então

$$\begin{aligned} \mathrm{div}_\infty(x) &= (q+1)MP_0; \\ \mathrm{div}_\infty(y) &= \frac{q}{p^b} MP_0; \\ \mathrm{div}_\infty(z) &= \frac{q^3}{p^b} P_0. \end{aligned}$$

Para $\mathcal{C} = \mathcal{Y}$, com as mesmas ideais trocando $t(x)$ por $x^q + x$ obtemos os resultados análogos, de fato homogeneizando $\mathcal{Y}$ temos

$$\widetilde{\mathcal{Y}} : Y^{q+1} = W^q X^q + XW^q \quad \text{e} \quad Z^M = W^{M-q^2} Y^{q^2} - W^{M-1} Y.$$

Se $W = 0$, das equações acima temos $Y = Z = 0$, portanto $X_\infty = (1:0:0:0)$ é o único no infinito de $\mathbb{P}^3\left(\overline{\mathbb{F}}_{q^{2m}}\right)$ tal que $X_\infty \in \mathcal{X}$. Defina $P_0 := X_\infty \in \mathcal{X}\left(\mathbb{F}_{q^{2m}}\right)$.

Consideremos os corpos de funções $K = \mathbb{F}_{q^{2m}}(x)$ e

$$\begin{aligned} F &= \mathbb{F}_{q^{2m}}(x, y) : y^{q+1} = x^q + x \\ \widetilde{F} &= \mathbb{F}_{q^{2m}}(x, y, z) : z^M = y^{q^2} - y; \end{aligned}$$

i.e, temos a torre de corpos de funções algébricas $K \subset F \subset \widetilde{F}$ e cada uma das extensões $\widetilde{F}/F$ e F/K é do tipo Kummer.

Novamente a a prova é consequência direta das duas afirmações seguintes.

Afirmação 4.2.4. *O polo $\mathcal{P}_\infty$ de x em K é totalmente ramificado em F; se $\mathcal{Q}_\infty$ denota o único lugar em F tal que $\mathcal{Q}_\infty/\mathcal{P}_\infty$ então*

- $e\left(\mathcal{Q}_\infty/\mathcal{P}_\infty\right) = q+1$;
- $v_{\mathcal{Q}_\infty}(x) = -(q+1)$;
- $v_{\mathcal{Q}_\infty}(y) = -q$.

- *Se $\mathcal{Q}$ é um lugar em F tal que $v_{\mathcal{Q}}(x) < 0$ ou $v_{\mathcal{Q}}(y) < 0$, então $\mathcal{Q} = \mathcal{Q}_\infty$, i.e, x e y tem o mesmo polo $\mathcal{Q}_\infty$ em F.*

De fato $v_{\mathcal{P}_\infty}(x^q + x) = -q$, pois $grau(x^q + x) = q$ e $\mathcal{P}_\infty$ é o polo de x em K, além disso $[F : K] = q + 1$, portanto

$$r_{\mathcal{P}_\infty} = mdc([F : K],\ v_{\mathcal{P}_\infty}(x^q + x)) = 1;$$

em consequência $\mathcal{P}_\infty$ é totalmente ramificado em F, (veja [25], Proposição 3.7.3).

Seja $\mathcal{Q}_\infty$ o único lugar em F tal que $\mathcal{Q}_\infty/\mathcal{P}_\infty$, então $e(\mathcal{Q}_\infty/\mathcal{P}_\infty) = [F : K]$; agora

$$\begin{aligned} v_{\mathcal{Q}_\infty}(x) &= e(\mathcal{Q}_\infty/\mathcal{P}_\infty)\, v_{\mathcal{P}_\infty}(x) \\ &= -(q+1). \end{aligned}$$

Como

$$\begin{aligned} (q+1)\, v_{\mathcal{Q}_\infty}(y) &= v_{\mathcal{Q}_\infty}\left(y^{q+1}\right) \\ &= v_{\mathcal{Q}_\infty}(x^q + x) \\ &= e(\mathcal{Q}_\infty/\mathcal{P}_\infty)\, v_{\mathcal{P}_\infty}(x^q + x); \end{aligned}$$

então $v_{\mathcal{Q}_\infty}(y) = -q$.

Note-se que $\mathcal{P} \in \mathbb{P}_K$ e $\mathcal{P} \neq \mathcal{P}_\infty$ então $v_{\mathcal{P}}(x^q + x) \geq 0$. Seja $\mathcal{Q}$ um lugar em F e $\mathcal{P}$ um lugar em K tal que $\mathcal{Q}/\mathcal{P}$, como $v_{\mathcal{Q}}(x) = e(\mathcal{Q}/\mathcal{P})\, v_{\mathcal{P}}(x)$; se $v_{\mathcal{Q}}(x) < 0$ então, $\mathcal{P} = \mathcal{P}_\infty$ e assim, $\mathcal{Q} = \mathcal{Q}_\infty$. Se $v_{\mathcal{Q}}(y) < 0$, então $v_{\mathcal{P}}(x^q + x) < 0$ e portanto $\mathcal{P} = \mathcal{P}_\infty$, em consequência $\mathcal{Q} = \mathcal{Q}_\infty$.

Afirmação 4.2.5. *O polo comum $\mathcal{Q}_\infty$ de x e y em F é totalmente ramificado em $\widetilde{F}$; se $\widetilde{\mathcal{Q}}_\infty$ denota o único lugar em $\widetilde{F}$ tal que $\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty$ então*

- $e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right) = M$;
- $v_{\widetilde{\mathcal{Q}}_\infty}(x) = -(q+1)M$;
- $v_{\widetilde{\mathcal{Q}}_\infty}(y) = -qM$;
- $v_{\widetilde{\mathcal{Q}}_\infty}(z) = -q^3$;
- *Se $\widetilde{\mathcal{Q}}$ é um lugar em F tal que $v_{\widetilde{\mathcal{Q}}}(x) < 0$ ou $v_{\widetilde{\mathcal{Q}}}(y) < 0$ ou $v_{\widetilde{\mathcal{Q}}}(z) < 0$, então $\widetilde{\mathcal{Q}} = \widetilde{\mathcal{Q}}_\infty$. i.e, x, y, z têm o mesmo polo $\widetilde{\mathcal{Q}}_\infty$ em $\widetilde{F}$.*

Seja $u = y^{q^2} - y$; como $v_{\mathcal{Q}_\infty}(y) = -q$ então

$$\begin{aligned} v_{\mathcal{Q}_\infty}(u) &= \min\left\{v_{\mathcal{Q}_\infty}(y),\ v_{\mathcal{Q}_\infty}\left(y^{q^2}\right)\right\} \\ &= -q^3. \end{aligned}$$

Como, $\left[\widetilde{F}:F\right]=M$ e $r_{\mathcal{Q}_\infty}(u)=mdc\left(\left[\widetilde{F}:F\right],\ v_{\mathcal{Q}_\infty}(u)\right)=1$, portanto $\mathcal{Q}_\infty$ é totalmente ramificado em $\widetilde{F}$; se $\widetilde{\mathcal{Q}}_\infty$ é o único lugar em $\widetilde{F}$ tal que $\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty$ então

$$e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right)=\left[\widetilde{F}:F\right]=M.$$

Agora

$$\begin{aligned} v_{\widetilde{\mathcal{Q}}_\infty}(x) &= e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right)e\left(\mathcal{Q}_\infty/\mathcal{P}_\infty\right)v_{\mathcal{P}_\infty}(x)\\ &= -(q+1)M. \end{aligned}$$

Também

$$\begin{aligned} v_{\widetilde{\mathcal{Q}}_\infty}(y) &= e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right)v_{\mathcal{Q}_\infty}(y)\\ &= -qM. \end{aligned}$$

Da condição $z^M=y^{q^2}-y$ temos

$$\begin{aligned} Mv_{\widetilde{\mathcal{Q}}_\infty}(z) &= v_{\widetilde{\mathcal{Q}}_\infty}\left(y^{q^2}-y\right)\\ &= e\left(\widetilde{\mathcal{Q}}_\infty/\mathcal{Q}_\infty\right)v_{\mathcal{Q}_\infty}\left(y^{q^2}-y\right)\\ &= -q^3M. \end{aligned}$$

Finalmente, seja $\widetilde{\mathcal{Q}}$ um lugar de $\widetilde{F}$ e suponhamos que $\mathcal{Q}\in\mathbb{P}_F$ e $\mathcal{P}\in\mathbb{P}_K$ tal que $\widetilde{\mathcal{Q}}/\mathcal{Q}$ e $\mathcal{Q}/\mathcal{P}$, usando os fatos

$$\begin{aligned} v_{\widetilde{\mathcal{Q}}}(x) &= e\left(\widetilde{\mathcal{Q}}/\mathcal{Q}\right)e\left(\mathcal{Q}/\mathcal{P}\right)v_{\mathcal{P}}(x);\\ v_{\widetilde{\mathcal{Q}}}(y) &= e\left(\widetilde{\mathcal{Q}}/\mathcal{Q}\right)v_{\mathcal{Q}}(y); \end{aligned}$$

se $v_{\widetilde{\mathcal{Q}}}(x)<0$, então $v_{\mathcal{P}}(x)<0$, portanto $\mathcal{P}=\mathcal{P}_\infty$, segue-se que $\mathcal{Q}=\mathcal{Q}_\infty$ e $\widetilde{\mathcal{Q}}=\widetilde{\mathcal{Q}}_\infty$. Se $v_{\widetilde{\mathcal{Q}}}(y)<0$, então $v_{\mathcal{Q}}(y)<0$, e pela última parte da afirmação anterior temos $\mathcal{Q}=\mathcal{Q}_\infty$, portanto $\widetilde{\mathcal{Q}}=\widetilde{\mathcal{Q}}_\infty$.

Para $v_{\widetilde{\mathcal{Q}}}(z)$, como $Mv_{\widetilde{\mathcal{Q}}}(z)=e\left(\widetilde{\mathcal{Q}}/\mathcal{Q}\right)v_{\mathcal{Q}}\left(y^{q^2}-y\right)$, é suficiente provar que $v_{\mathcal{Q}}\left(y^{q^2}-y\right)\geq 0$, para cada $\mathcal{Q}\in\mathbb{P}_F$, com $\mathcal{Q}\neq\mathcal{Q}_\infty$. De fato se $\mathcal{P}\in\mathbb{P}_K$ com $\mathcal{Q}/\mathcal{P}$, então $\mathcal{P}\neq\mathcal{P}_\infty$, portanto $v_{\mathcal{P}}(x)\geq 0$, então $v_{\mathcal{Q}}(y)\geq 0$, segue-se que $v_{\mathcal{Q}}\left(y^{q^2}-y\right)\geq\min\left\{v_{\mathcal{Q}}(y),q^2v_{\mathcal{Q}}(y)\right\}\geq 0$.

Dos cálculos acima, P_0 é único polo comum de x,y,z em $\mathcal{X}$, então

$$\begin{aligned} \mathrm{div}_\infty(x) &= (q+1)MP_0;\\ \mathrm{div}_\infty(y) &= qMP_0;\\ \mathrm{div}_\infty(z) &= q^3P_0. \end{aligned}$$

■

Observação 4.2.6. *Com a notação acima:*

- *Temos as sequências de números polos ou não lacunas da curva $\mathcal{C}$ no ponto P_0 :*

$$(a_1, a_2, a_3) := \begin{cases} \left(\frac{q}{p^b}M, \frac{q^3}{p^b}, (q+1)\,M\right) & \mathcal{C} = \mathcal{X}, \\ (qM, q^3, (q+1)\,M) & \mathcal{C} = \mathcal{Y}. \end{cases} \tag{4.2.1}$$

- *Notemos que se esquecemos a origem de b como um divisor de a e simplesmente fazemos $b = 0$, então as sequências de $\mathcal{X}$ e $\mathcal{Y}$ em (4.2.1) são as mesmas. Neste caso, também, $g(\mathcal{X}) = g(\mathcal{Y})$, (veja, (3.1.4) e (3.2.4)).*

Calcularemos agora o semigrupo de Weierstrass $H(P_0)$ de $\mathcal{X}$ em P_0. Para isto primeiro note que

$$S = \langle a_1, a_2, a_3\rangle \subseteq H(P_0),$$

onde, como é usual, $\langle a_1, a_2, a_3\rangle$ denota o semigrupo gerado pela sequência (a_1, a_2, a_3).

Teorema 4.2.7. *O semigrupo S gerado por cada uma das sequências (a_1, a_2, a_3) em (4.2.1) é um semigrupo telescópico (veja definição 1.1.15) e*

$$g(S) = \begin{cases} \dfrac{q^{m+2} - p^b q^m - sq^3 + q^2 + (s-1)\,p^b}{2sp^b} & se \quad \mathcal{C} = \mathcal{X}, \\ \dfrac{q^{m+2} - q^m - sq^3 + q^2 + (s-1)}{2s} & se \quad \mathcal{C} = \mathcal{Y}. \end{cases}$$

portanto $S = \langle a_1, a_2, a_3\rangle = H(P_0)$.

Dem. Para $\mathcal{C} = \mathcal{X}$:

$$(a_1, a_2, a_3) = \left(\frac{q}{p^b}M, \frac{q^3}{p^b}, (q+1)\,M\right);$$

Note-se que $mdc(a_1, a_2, a_3) = 1$. Agora, $d_1 = mdc(a_1) = a_1$ e $S_1 = \left\langle \frac{a_1}{d_1}\right\rangle = \langle 1\rangle = \mathbb{N}_0$. Seja $d_2 = mdc(a_1, a_2)$, como $\frac{q}{p^b}$ é um divisor comum de a_1 e a_2, temos que $\frac{q}{p^b}$ é um divisor de d_2. Note que M e q^2 são coprimos, portanto existem inteiros α, β tais que $\alpha M + \beta q^2 = 1$, de onde é obtida a combinação linear $\alpha\frac{q}{p^b}M + \beta\frac{q^3}{p^b} = \frac{q}{p^b}$, e como d_2 é um divisor comum de a_1 e a_2, segue-se que d_2 é um divisor de $\frac{q}{p^b}$, i.e, $d_2 = \frac{q}{p^b}$. Agora, $S_2 = \left\langle \frac{a_1}{d_2}, \frac{a_2}{d_2}\right\rangle = \langle M, q^2\rangle$. Finalmente, $d_3 = mdc(a_1, a_2, a_3) = 1$, então $S_3 = \left\langle \frac{a_1}{d_3}, \frac{a_2}{d_3}, \frac{a_3}{d_3}\right\rangle = S$, e $\frac{a_3}{d_3} = (q+1)\,M \in S_2$, pois $M \in S_2$. Podemos concluir que (a_1, a_2, a_3) é uma sequência telescópica e portanto S é um semigrupo telescópico.

Pelo Teorema 1.1.16 temos

$$\begin{aligned} g(S) &= \frac{1}{2}\left(1 + \left(\frac{d_0}{d_1} - 1\right)a_1 + \left(\frac{d_1}{d_2} - 1\right)a_2 + \left(\frac{d_2}{d_3} - 1\right)a_3\right) \\ &= \frac{1}{2}\left(1 - \frac{q}{p^b}M + (M-1)\,\frac{q^3}{p^b} + \left(\frac{q}{p^b} - 1\right)(q+1)M\right) \\ &= \frac{1}{2sp^b}\left(q^{m+2} - p^b q^m - sq^3 + q^2 + (s-1)\,p^b\right). \end{aligned}$$

Finalmente, como $g(S) = g(\mathcal{X})$ (veja Teorema 3.1.4), i.e., $\#(\mathbb{N}_0 \setminus S) = \#(\mathbb{N}_0 \setminus H(P_0))$, e como estes conjuntos são finitos, além disso $S \subseteq H(P_0)$ então $S = H(P_0)$.

No caso $\mathcal{C} = \mathcal{Y}$, é suficiente fazer $b = 0$ em $\mathcal{C} = \mathcal{X}$. ■

Para a curva $\mathcal{Y}$, o semigrupo numérico $H(P_0)$, generaliza a proposição 1 em [12], e $\mathcal{Y}_{m,1}$ é a curva GGS definida em (2.2.1). Como $H(P_0)$ é telescópico, por [2], Teorema 4.1, $H(P_0)$ é simétrico. Notemos que $\mathcal{C}$ não é curva de Castle em P_0 (veja definição 1.1.21). De fato para $\mathcal{C} = \mathcal{X}$, como veremos depois por (4.2.5)

$$s_1 = \begin{cases} \frac{q}{p^b} M & \text{se } m = 3 \text{ e } p^b > s \\ \frac{q^3}{p^b} & \text{se } m > 3 \text{ e } p^b > s; \end{cases}$$

e para para $\mathcal{C} = \mathcal{Y}$, por (4.2.6), $s_1 = q^3$ para $q/2 > s$.

Se $\mathcal{C}$ for de Castle em P_0 então

$$1 + q^{2m} + 2gq^m = 1 + s_1 q^m,$$

ou equivalentemente $s_1 = q^m + 2g$, que é impossível.

4.2.2 Alguns exemplos

Consideremos $\mathcal{C} = \mathcal{X}$ ou $\mathcal{Y}$ as curvas definidas na seção anterior. Explicitamente vamos supor que

$$H(P_0) = \langle a_1, a_2, a_3 \rangle = \{0 = \rho_1 < \rho_2 < ...\}.$$

Para $\rho_h \in H(P_0)$, com $h \in \mathbb{N}_0$, seja C_h o $[n_h, k_h, d_h]$ código geométrico unipontual sobre a curva $\mathcal{C}$, definido pelos divisores

$$G_h := \rho_h P_0 \quad \text{e} \quad E := P_1 + \ldots + P_N;$$

onde $P_i \in \mathcal{C}(\mathbb{F}_{q^{2m}})$, com $P_i \neq P_j$ para $i \neq j$, P_0 é o polo comum de x, y, z em $\mathcal{C}$, e $N = \#\mathcal{C}(\mathbb{F}_{q^{2m}}) - 1$.

Notemos que

$$C_h = \{(f(P_1), f(P_2), ..., f(P_N)) : f \in \mathcal{L}(G_h)\} \subset \mathbb{F}_{q^{2m}}^N;$$

e por (4.1.3)

$$k_h = \ell(G_h) - \ell(G_h - E).$$

Como $H(P_0)$ é simétrico podemos calcular k_h, para isto usaremos o lema a seguir.

Lema 4.2.8. *Se $(a_1, ..., a_k)$ é uma sequência numérica telescópica (veja definição 1.1.15), defina para $i = 1, ..., k$: $d_i = mdc(a_1, ..., a_i)$. Então para cada $r \in S := \langle a_1, ..., a_k \rangle$, existem únicos $j_1, ..., j_k \in \mathbb{N}_0$, com $0 \leq j_i \leq d_{i-1}/d_i$ para $i = 2, ..., k$, tais que*

$$r = \sum_{i=1}^{r} j_i a_i.$$

Dem. [15], Lema 5.34.■

Agora $H(P_0) = \langle a_1, a_2, a_3 \rangle$ é semigrupo telescópico, pelo Teorema 4.2.8. Como $\rho_h \in H(P_0)$, existem únicos inteiros $0 \leq x_1$, $0 \leq x_2 < d_1/d_2$, $0 \leq x_3 < d_2/d_3 = d_2$, tais que

$$\rho_h = x_1 a_1 + x_2 a_2 + x_3 a_3.$$

Sejam $f_1, f_2, f_3 \in \mathbb{F}_{q^{2m}}(\mathcal{C})$ tais que $\mathrm{div}_\infty(f_i) = a_i P_0$, onde $i = 1, 2, 3$.

Lema 4.2.9. *Com a notação acima, o conjunto de funções racionais*

$$B = \{f_1^{\alpha_1} f_2^{\alpha_2} f_3^{\alpha_3} : \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 \leq \rho_h\,,\ \alpha_1 \geq 0\,,\ 0 \leq \alpha_2 < d_1/d_2, 0 \leq \alpha_3 < d_2\};$$

é uma $\mathbb{F}_{q^{2m}}-$ base do espaço de Riemann-Roch $\mathcal{L}(G_h)$.

Dem. Consequência direta da definição de B. ■

Notemos que $n_h = N$; e para $2g - 2 < grau\,(G_h) = \rho_h < N$, por (4.1.4), (4.1.6) e Lema 4.2.9 temos

$$k_h = \ell(G_h) = \#\{\rho \in H(P_0) : \rho \leq \rho_h\}; \tag{4.2.2}$$

e

$$N - \rho_h = n_h - grau(G_h) \leq d_h \leq N + 1 - k_h.$$

Seja agora $C_h^\perp$ o código dual de C_h; $C_h^\perp$ é um $\left[N, k_h^\perp, d_h^\perp\right]$ código e por (4.1.7) e (4.1.9)

$$k_h^\perp = N - k_h;$$

e

$$grau\,(G_h) - (2g-2) = \rho_h - (2g-2) \leq d_h^\perp \leq k_h + 1.$$

Notemos que $C_h^\perp$ e C_h tem comprimento de palavras N, e como $\mathcal{C}$ é $\mathbb{F}_{q^{2m}}-$ maximal, portanto N é muito maior que g, concluímos que $C_h^\perp$ e C_h são bons códigos.

Temos

$$d_h \geq N - \rho_h \quad \text{e} \quad d_h^\perp \geq d_G(h) := \rho_h - (2g-2). \tag{4.2.3}$$

A cota $d_G(h)$ em (4.2.3) pode ser melhorada usando o fato que $H\,(P_0)$ é telescópico, e alguns resultados com relação à cota d_{FR} de Feng-Rao definida em [7] e que lembraremos a seguir.

Para $\rho_h \in H(P_0)$ consideremos o conjunto

$$\nu_h := \#\left\{(i,j) \in \mathbb{N}^2 : \rho_i + \rho_j = \rho_{h+1}\right\};$$

e defina

$$d_{FR}\,(h) := \min\{\nu_m : h \leq m\};$$

que é chamada a **cota ordem de Feng-Rao** de $C_h^\perp$ (em P_0).

Lema 4.2.10. *A distância mínima $d_h^\perp$ de $C_h^\perp$ satisfaz*

$$d_h^\perp \geq d_{FR}\,(h)\,.$$

Dem. [15], Teorema 4.13. ■

Podemos calcular $d_{FR}(h)$, a seguir.

Lema 4.2.11. *Em geral*

$$d_{FR}(h) \geq h + 1 - g;$$

além disso, se $h \geq 2\lambda - g - 1$, *onde* $\lambda := \max\{m \in \mathbb{Z} : m - 1 \notin H(P_0)\}$, *i.e* $\lambda = cond(H(P_0))$ *o condutor de* $H(P_0)$; *então* $\nu_h = h + 1 - g$, *e portanto*

$$d_{FR}(h) = h + 1 - g.$$

Dem. [15], Teorema 5.24. ■

Também.

Teorema 4.2.12. *Seja* S *um semigrupo numérico de* $\mathbb{N}_0$ *gerado pela sequência telescópica* $(a_1, a_2, ..., a_k)$, *suponha que* $a_k = \max\{a_1, a_2, ..., a_k\}$ *e* $d_{k-1} = (a_1, a_2, ..., a_{k-1}) > 1$, *seja* (ρ_i) *a sequência de lacunas do* S.

- *Se* $g \leq h$ *e* $3g - 2 - (d_{k-1} - 1)a_k < h \leq 3g - 2$, *então*

$$d_{FR}(h) = \min\{\rho_m : \rho_m \geq h + 1 - g\}. \tag{4.2.4}$$

- *Se* $(j-1)a_k < \rho_{h+1} \leq ja_k \leq (d_{k-1} - 1)a_k$, *então*

$$d_{FR}(h) = j + 1.$$

Dem. [18], Teoremas 6.10, 6.11.■

Observação 4.2.13. *Seja* $\mathcal{C} = \mathcal{X}$ *ou* $\mathcal{Y}$, *as curvas* $\mathbb{F}_{q^{2m}}-$ *maximais definidas acima.*

- $H(P_0)$ *semigrupo de Weierstrass de* $\mathcal{C}$ *em* P_0, *é um semigrupo telescópico gerado pela sequência* (a_1, a_2, a_3), *onde se* $\mathcal{C} = \mathcal{X}$:

$$(a_1, a_2, a_3) := \begin{cases} (\frac{q}{p^b}M, \frac{q^3}{p^b}, (q+1)M) & se\ m = 3\ \ e\ p^b > s; \\ (\frac{q^3}{p^b}, \frac{q}{p^b}M, (q+1)M) & se\ m > 3\ \ e\ p^b > s, \end{cases} \tag{4.2.5}$$

  e se $\mathcal{C} = \mathcal{Y}$:

$$(a_1, a_2, a_3) := \ (q^3, qM, (q+1)M) \quad se\ q/2 > s; \tag{4.2.6}$$

  com $a_1 < a_2 < a_3$.

  Segue-se que $a_3 = \max\{a_1, a_2, a_3\} = (q+1)M$, *e*

$$d_2 = mdc(a_1, a_2) = \begin{cases} q/p^b & se\ \ \mathcal{C} = \mathcal{X}; \\ q & se\ \ \mathcal{C} = \mathcal{Y}, \end{cases}$$

  portanto $d_2 > 1$ *se* $b < a$, *e o Teorema 4.2.12 é verdadeiro para* $H(P_0)$.

- *Na sequência enumerável* $(\rho_k)_{k\in\mathbb{N}}$ *com* $\rho_1 = 0$ *e* $\rho_k < \rho_{k+1}$ *para cada* $k \in \mathbb{N}$. *Como* $g = g(H(P_0))$, *as* g *lacunas de* $H(P_0)$ *satisfazem*

$$1 = \ell_1 < \ell_2 < ... < \ell_g \leq 2g - 1;$$

usando o fato que $H(P_0)$ *é simétrico, então a maior lacuna* $\ell_g = 2g - 1$. *Em* $[0, 2g - 1]$ *existem exatamente* g *não lacunas,*

$$0 = \rho_1 < \rho_2 < ... < \rho_g = 2g - 2;$$

pois $2g - 1$ *é a maior lacuna; portanto*

$$0 = \rho_1 < \rho_2 < ... < \rho_g < \ell_g;$$

em consequência, as lacunas de $H(P_0)$ *estão explicitamente determinadas por*

$$1 = \ell_g - \rho_g < \ell_g - \rho_{g-1} < \ldots < \ell_g - \rho_2 < \ell_g = 2g - 1. \tag{4.2.7}$$

Teorema 4.2.14. *Seja* $\mathcal{C} = \mathcal{X}$ *ou* $\mathcal{Y}$, *as curvas* $\mathbb{F}_{q^{2m}}-$ *maximais definidas acima, supor que* u *é um inteiro tal que*

$$0 \leq u \leq \min\{2g - 2, (d_2 - 1)a_3 - 1\};$$

defina $h = 3g - 2 - u$; *se* $u \in \mathbb{N}_0 \setminus H(P_0)$, *então* $d_{FR}(h) = h + 1 - g$.

Dem. Notemos que se u é definido como na hipótese temos que h satisfaz $g < h$ e

$$3g - 2 - (d_2 - 1)a_3 < h \leq 3g - 2,$$

portanto, pela observação 4.2.13 e o Teorema 4.2.12, obtemos

$$d_{FR}(r) = \min\{\rho_t : \rho_t \geq h + 1 - g\}.$$

Note que

$$h + 1 - g = 2g - 1 - u = \ell_g - u;$$

além disso, $\ell_g - u \in H(P_0)$, pois se $\ell_g - u \notin H(P_0)$, por (4.2.7) $\ell_g - u = \ell_g - \rho_i$ para algum $i = 1, 2, ..., g$, i.e, $u = \rho_i \in H(P_0)$ que de fato é uma contradição. Em conclusão $h+1-g \in H(P_0)$ e por (4.2.4), obtemos

$$d_{FR}(h) = \min\{\rho_t : \rho_m \geq h + 1 - g\} = r + 1 - g.\blacksquare$$

Exemplo 4.2.15. *Em* $\mathcal{X}$ *consideremos os parâmetros* $p = 2$, $m = 3$ *e* $a = b = 1$, *portanto* $q = 2$ *e* $\frac{q^m+1}{q+1} = 3$, *para* $s = 1$ *e* $\lambda = 1 \in \mathbb{F}_{2^6}$ *obtemos a curva* $\mathbb{F}_{2^6}-$ *maximal com equações afins*

$$y^3 = x \quad e \quad z^3 = y^4 - y;$$

que tem gênero $g = 3$ *e* $\#\mathcal{X}(\mathbb{F}_{2^6}) = 113$.

Em [28] é apresentada a curva record $\mathbb{F}_{2^6}-$ maximal com gênero $g = 3$, com modelo plano afim

$$\mathcal{C} : u^4 + u^2 + u = v^3.$$

Uma questão natural é perguntar-se se as curvas $\mathcal{X}$ e $\mathcal{C}$ acima são $\mathbb{F}_{2^6}-$ isomorfas. Inicialmente note-se que $\mathcal{X}$ tem singularidades e $\mathcal{C}$ é não singular, portanto é suficiente perguntar-se o modelo não singular de $\mathcal{X}$ e $\mathcal{C}$ são $\mathbb{F}_{2^6}-$ birracionalmente equivalentes. De fato são, para provar isto notemos que $\mathcal{X}$ e $\mathcal{C}$ tem um único ponto no infinito P_0 e Q respectivamente, além disso

$$H(P_0) = \langle 3, 4, 9\rangle \quad e \quad H(Q) = \langle 3, 4\rangle.$$

En geral de [14], Teorema 10.43, se $\mathcal{Y}$ é uma curva $\mathbb{F}_{q^2}-$ maximal e se existe $P \in \mathcal{Y}(\mathbb{F}_{q^2})$ e uma não lacuna $m \in H(P)$ que divide $q+1$ então $\mathcal{Y}$ é $\mathbb{F}_{q^2}-$ birracionalmente equivalente com a curva $\mathbb{F}_{q^2}-$ maximal

$$X^q + X = Y^m.$$

Agora, $m = 3 \in H(P_0)$ e 3 divide a $2^3 + 1$, portanto temos a conclusão.

Para o calculo dos parâmetros dos AG códigos, com a notação definida acima, se P_0 é o polo comum de x, y, z em $\mathcal{X}$, então

$$\begin{aligned} H(P_0) &= \langle \frac{q}{p^b}M, \frac{q^3}{p^b}, (q+1)M\rangle \\ &= \langle 3, 4, 9\rangle \\ &= \{0 = \rho_1 < \rho_2 < ...\} \end{aligned}$$

Para o $[N, k_h, d_h]$ código geométrico unipuntual C_h sobre a curva $\mathcal{X}$,

$$G_h := \rho_h P_0 \quad e \quad E = P_1 + \ldots + P_N;$$

temos que

$$N = \#\mathcal{X}(\mathbb{F}_{2^6}) - 1 = 112.$$

Para $\rho_h < 112$

$$k_h = \ell(G_h) = \#\{\rho \in H(P_0) : \rho \leq \rho_h\},$$

e como

$$0 = \rho_1 \leq ... \leq \rho_{h-1} \leq \rho_h;$$

obtemos $k_h = h$. Além disso,

$$d_h \geq n_h - grau(G_h) = N - \rho_h.$$

Para mostrar em particular alguns parâmetros e além disso comparar com a cota de Feng-Rao devemos pensar no Lema 4.2.11, para isto note que como $H(P_0)$ é simétrico

$$\lambda = cond(H(P_0)) = 2g = 6;$$

em consequência para $h \geq 2\lambda - g - 1 = 8$*, temos* $d_{FR}(h) = h + 1 - g$*, i.e, a partir desta cota esta sequência é crescente. Temos a seguinte tabela para os primeiros 21 parâmetros* [3]*.*

h	ρ_h	N	k_h	$N - \rho_h$	$k_h^{\perp}$	${\nu_h}^3$	$d_{FR}(h)$
1	0	112	1	112	111	2	2
2	3	112	2	109	110	2	2
3	4	112	3	108	109	3	3
4	6	112	4	106	108	4	3
5	7	112	5	105	107	3	3
6	8	112	6	104	106	4	4
7	9	112	7	103	105	4	4
8	10	112	8	102	104	6	6
9	11	112	9	101	103	7	7
10	12	112	10	100	102	8	8
11	13	112	11	99	101	9	9
12	14	112	12	98	100	10	10
13	15	112	13	97	99	11	11
14	16	112	14	96	98	12	12
14	17	112	15	95	97	13	13
16	18	112	16	94	96	14	14
17	19	112	17	93	95	15	15
18	20	112	18	92	94	16	16
19	21	112	19	91	93	17	17
20	22	112	20	90	92	18	18
21	23	112	21	89	91	19	19

Para as dimensões $111, 110, 109, 105, 104, 103$ *são obtidos os melhores valores conhecidos para a distância minima. Para outras curvas o alfabeto é muito grande e não é possível fazer comparações.*

[3] Wolfram Research Mathematica

Referências Bibliográficas

[1] Miriam Abdón, Juscelino Bezerra, and Luciane Quoos. Further examples of maximal curves. *Journal of Pure and Applied Algebra*, 213(6):1192–1196, 2009.

[2] Scott T Chapman. *Arithmetical properties of commutative rings and monoids*. CRC Press, 2010.

[3] Antonio Cossidente, Gabor Korchmáros, and Fernando Torres. On curves covered by the hermitian curve. *Journal of Algebra*, 216(1):56–76, 1999.

[4] Iwan Duursma and Kit-Ho Mak. On maximal curves which are not galois subcovers of the hermitian curve. *Bulletin of the Brazilian Mathematical Society, New Series*, 43(3):453–465, 2012.

[5] Stefania Fanali and Massimo Giulietti. One-point ag codes on the gk maximal curves. *IEEE Transactions on Information Theory*, 56(1):202–210, 2010.

[6] Stefania Fanali and Massimo Giulietti. Quotient curves of the gk curve. *Adv. Geom*, 12:239–268, 2012.

[7] Gui-Liang Feng and Thammavarapu R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *Information Theory, IEEE Transactions on*, 40(4):1003–1012, 1994.

[8] Rainer Fuhrmann, Arnaldo Garcia, and Fernando Torres. On maximal curves. *Journal of Number Theory*, 67(1):29–51, 1997.

[9] Arnaldo Garcia, Cem Güneri, and Henning Stichtenoth. A generalization of the giulietti–korchmáros maximal curve. *Advances in Geometry*, 10(3):427–434, 2010.

[10] Arnaldo Garcia and Henning Stichtenoth. A maximal curve which is not a galois subcover of the hermitian curve. *Bull Braz Math Soc*, 37(1), 2006.

[11] Arnaldo Garcia, Henning Stichtenoth, and Chao-Ping Xing. On subfields of the hermitian function field. *Compositio Mathematica*, 120(2):137–170, 2000.

[12] Massimo Giulietti and Gábor Korchmáros. A new family of maximal curves over a finite field. *Mathematische Annalen*, 343(1):229–245, 2009.

[13] Valerii Denisovich Goppa. Codes on algebraic curves. In *Soviet Math. Dokl.*, volume 24, pages 170–172, 1981.

[14] James William Peter Hirschfeld, Gábor Korchmáros, and Fernando Torres. *Algebraic curves over a finite field*. Princeton University Press, 2013.

[15] Tom Høholdt, Jacobus Van Lint, and Ruud Pellikaan. Algebraic geometry codes. *Handbook of coding theory*, 1(Part 1):871–961, 1998.

[16] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724, 1981.

[17] Ahmad Kazemifard, Ali Reza Naghipour, and Saeed Tafazolian. A note on superspecial and maximal curves. *Bulletin of the Iranian Mathematical Society*, 39(3):405–413, 2013.

[18] Christoph Kirfel and Ruud Pellikaan. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Transactions on information theory*, 41(6):1720–1732, 1995.

[19] Gábor Korchmáros and Fernando Torres. Embedding of a maximal curve in a hermitian variety. *Compositio Mathematica*, 128(1):95–113, 2001.

[20] Gábor Korchmáros and Fernando Torres. On the genus of a maximal curve. *Mathematische Annalen*, 323(3):589–608, 2002.

[21] Gilles Lachaud. Sommes d'eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. *CR Acad. Sci. Paris*, 305:729–732, 1987.

[22] Joseph Lewittes. Places of degree one in function fields over finite fields. *Journal of Pure and Applied Algebra*, 69(2):177–183, 1990.

[23] Qing Liu and Reinie Erné. *Algebraic geometry and arithmetic curves*, volume 6. Oxford university press Oxford, 2002.

[24] Jean-Pierre Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *CR Acad. Sci. Paris*, 296(Série I):397–402, 1983.

[25] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer, 2009.

[26] Henning Stichtenoth and Hans-Georg Rück. A characterization of hermitian function fields over finite fields. *Journal für die reine und angewandte Mathematik*, 457:185–188, 1994.

[27] Saeed Tafazolian, Arnoldo Teheran Herrera, and Fernando Torres. Further examples of maximal curves which cannot be covered by the hermitian curve. *preprint*, 2014.

[28] Gerard Van Der Geer, Everett Howe, Kristin Lauter, and Christophe Ritzenthaler. Manypoints: A table of curves with many points. *Online webpage: http://www. manypoints. org*, 2011.