Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Tese de Doutorado

O arco associado a uma generalização da curva Hermitiana

por

Beatriz Casulari da Motta Ribeiro[†]

Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Fernando Eduardo Torres Orihuela

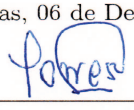
Coorientador: Prof. Dr. Herivelto Martins Borges Filho

[†]Este trabalho contou com apoio financeiro da CAPES, do CNPq e do PROQUALI.

O arco associado a uma generalização da curva Hermitiana

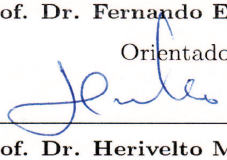
Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Beatriz Casulari da Motta Ribeiro** e aprovada pela comissão julgadora.

Campinas, 06 de Dezembro de 2011.



Prof. Dr. Fernando Eduardo Torres Orihuela

Orientador



Prof. Dr. Herivelto Martins Borges Filho

Coorientador

Banca examinadora:

1. Prof. Dr. Fernando Eduardo Torres Orihuela
2. Prof. Dr. Paulo Roberto Brumatti
3. Prof. Dr. Cícero Fernandes de Carvalho
4. Profa. Dra. Luciane Quoos Conte
5. Prof. Dr. José Gilvan Oliveira

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP como requisito parcial para obtenção do título de **Doutor em Matemática**.

FICHA CATALOGRÁFICA ELABORADA POR
MARIA FABIANA BEZERRA MÜLLER - CRB8/6162
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

R354a

Ribeiro, Beatriz Casulari da Motta, 1984-
O arco associado a uma generalização da curva hermitiana / Beatriz Casulari da Motta Ribeiro. - Campinas, SP : [s.n.], 2011.

Orientador: Fernando Eduardo Torres Orihuela.
Coorientador: Herivelto Martins Borges Filho.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Curvas algébricas. 2. Soma exponencial. 3. Geometria finita. 4. Corpos finitos (Algébra). I. Torres Orihuela, Fernando Eduardo, 1961-. II. Borges Filho, Herivelto Martins. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

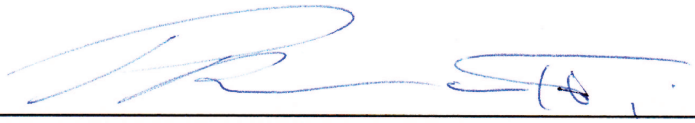
Informações para Biblioteca Digital

Título em inglês: The arc arising from a generalization of the hermitian curve
Palavras-chave em inglês:
Algebraic curves
Exponencial sum
Finite geometry
Finite field (Algebra)
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Fernando Eduardo Torres Orihuela [Orientador]
Paulo Roberto Brumatti
Cícero Fernandes de Carvalho
Luciane Quoos Conte
José Gilvan de Oliveira
Data da defesa: 06-12-2011
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 06 de dezembro de 2011 e aprovada

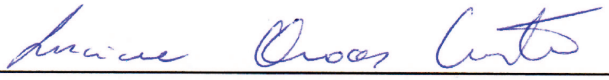
Pela Banca Examinadora composta pelos Profs. Drs.

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

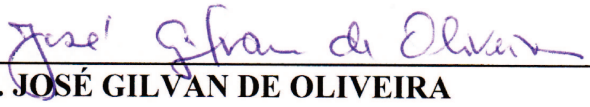


Prof(a). Dr(a). PAULO ROBERTO BRUMATTI

Prof(a). Dr(a). CÍCERO FERNANDES DE CARVALHO



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



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

AGRADECIMENTOS

Começo essa tese agradecendo aqueles que me ajudaram, direta ou indiretamente, nesses quase cinco anos de doutorado.

Ao meu orientador, Fernando, que me recebeu na Unicamp no curso de álgebra comutativa duvidando que eu quisesse mesmo trabalhar com ele. Agradeço por todos os artigos, os livros, as discussões e pela consideração.

Ao meu coorientador, Herivelto, que me recebeu em um momento difícil e me apresentou a curva $\mathcal{H}$ (entre outras).

Às minhas famílias do Rio e de Campinas. À primeira, por me incentivar a ir com tudo para Campinas e, mesmo assim, me receber de braços abertos cada vez que eu voltava com saudades (e queria contar todas as histórias do mundo). À segunda, por me acolher com tanto carinho. Em especial, às minhas primas que passaram pelo furacão do doutorado ao mesmo tempo que eu e aos meus (já não tão mais) pequenos primos por tudo que me ensinaram sobre a vida não matemática.

Ao meu querido Bruno pela motivação, pelas viagens longas à Campinas, pelas músicas, os filmes e os passeios. Mas, principalmente, por me acompanhar em cada ideia maluca que tive (e ainda tenho).

Aos meus colegas de doutorado. Em especial aos algébricos (comutativos ou não), companheiros de tantas horas de estudo e tantos congressos.

Aos meus colegas do departamento de matemática da UFJF, principalmente por me mostrarem que o doutorado devia ser prioridade e me deixarem com tempo para terminá-lo. E aos meus alunos da UFJF por acharem tão legal e motivador eu estar fazendo doutorado.

Aos meus amigos cariocas por me procurarem mesmo estando longe e me incluírem nos programas mesmo que eu não pudesse ir.

Aos membros da banca por aceitarem o convite do Fernando e por apresentarem tantas contribuições relevantes. Em especial, à Luciane, que já tinha começado a me ensinar a escrever matemática durante o mestrado. E ao inventor do e-mail por me colocar em contato com o Coulter para falar sobre seus artigos.

Por fim, a meus pais (novamente), à Capes, ao CNPQ e ao programa PROQUALI pelo auxílio financeiro.

RESUMO

Obtemos novos arcos completos associados ao conjunto de pontos racionais de uma certa generalização da curva Hermitiana que é Frobenius não-clássica. A construção está relacionada ao cálculo do número de pontos racionais de uma classe de curvas de Artin-Schreier.

ABSTRACT

We obtain new complete arcs arising from the set of rational points of a certain generalization of the Hermitian plane curve which is Frobenius non-classical. Our construction is related to the computation of the number of rational points of a class of Artin-Schreier curves.

CONTEÚDO

INTRODUÇÃO

Há décadas, espaços projetivos finitos vem sendo estudados intensamente. Além de serem muito interessantes, tem aplicações, por exemplo, na teoria de códigos, que também vem sendo investigada cada vez mais. Há diversos trabalhos expondo essa relação, como [1, 18], bem como literatura básica de qualidade no assunto [20, 17]. Nessa área de contribuição entre códigos e geometria finita, podemos destacar os arcos planos, uma configuração de pontos tal que não mais do que uma certa quantidade pré-fixada é colinear. A quantidade de pontos nessa configuração é denotada por n e o número máximo de pontos colineares por d, que são ditos parâmetros do arco. Um $(n, d)-$arco é dito completo se não está contido em um arco de tamanho $n+1$ e mesmo parâmetro d.

Podemos transferir essas definições para a teoria de códigos. Temos que um $(n, d)-$arco é equivalente a um $[n, 3, n-d']-$código linear, onde a distância mínima $n-d'$ é tal que $d' \leq d$. Se o arco for completo, então esse código tem distância mínima exatamente $n-d$ e não pode ser estendido a um código com distância mínima maior.

Um exemplo natural de configuração de pontos no plano com essa propriedade é dado pelos pontos racionais de uma curva plana definida sobre um corpo finito $\mathbb{F}_q$. De fato, o conhecido teorema de Bézout da teoria de curvas algébricas afirma que uma reta no plano intercepta uma curva plana em no máximo d pontos, onde d é o

grau dessa curva. O estudo paralelo da geometria finita e da geometria algébrica foi iniciado por B. Segre por volta de 1955, quando esse utilizou cotas sobre o número de pontos racionais para encontrar o segundo maior $(n, 2)-$arco no plano projetivo sobre $\mathbb{F}_q$.

Nesse sentido de interação entre curvas e arcos, surge a questão: quando o conjunto de pontos racionais de uma curva plana forma um arco completo? Tal pergunta foi proposta em 1988 por Hirschfeld e Voloch [19]. Os primeiros exemplos encontrados foram as cônicas irredutíveis em característica ímpar e algumas cúbicas (veja [20, 17]). No Capítulo 1, apresentamos uma introdução ao assunto e exemplos associados a curvas com mais uma propriedade em comum: são Frobenius não-clássicas. Uma curva é dita Frobenius não-clássica se para todo ponto P não-singular, o ponto obtido pelo morfismo de Frobenius em P pertence a reta tangente à curva em P. Tais curvas foram estudadas por Hefez e Voloch em [16] de acordo com a teoria apresentada em [31]. Recentemente, Giulietti et al [15] estudaram o conjunto de $\mathbb{F}_q-$pontos racionais de curvas Frobenius não-clássicas que dão exemplos de arcos completos, porém ainda são conhecidos poucos exemplos. Além disso, apresentamos ainda nesse capítulo, um contra-exemplo para uma pergunta natural sobre a existência de arcos completos associados a curvas Frobenius não-clássicas não-singulares.

O problema principal dessa tese, resolvido no Teorema 4.4, é explorar o arco associado ao conjunto de pontos racionais de uma curva que generaliza a conhecida curva Hermitiana, isto é, a curva plana $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$. Essa generalização foi apresentada por Borges em [3]. No Capítulo 2 dessa tese, fazemos uma breve apresentação da curva, seguida de comparações com a generalização da curva Hermitiana dada por Garcia e Stichtenoth em [13]. Apresentamos também detalhadamente o problema principal, apontando o fato de que para resolvê-lo é necessário conhecer o número de pontos afins de uma família de curvas de Artin-Schreier. Para mais informações sobre essa família de curvas, indicamos [30, 17].

Em 1989, Wolfmann [33] calculou o número de pontos racionais das curvas de

Artin-Schreier do tipo

$$y^q - y = ax^s + b$$

sobre $\mathbb{F}_{q^k}$ com k par, $a \in \mathbb{F}_{q^k}^*$, $b \in \mathbb{F}_{q^k}$, para alguns s inteiros especiais. Treze anos depois, Coulter [9], calculando explicitamente o valor de algumas somas exponenciais, estendeu os resultados de Wolfmann para curvas do tipo

$$y^{p^n} - y = ax^{p^\alpha+1} + L(x)$$

sobre $\mathbb{F}_q = \mathbb{F}_{p^e}$ onde $L(x)$ é um polinômio linearizado (conforme [25], seção 3.4) e $\alpha, n, e \in \mathbb{N}$ satisfazem certas relações. Na tentativa de estudar o arco associado à curva Hermitiana generalizada, nos deparamos com casos especiais de curvas de Artin-Schreier do tipo

$$y^{p^n} - y = ax^{p^\alpha+1} + L(x) + c \tag{1}$$

e nos espelhamos nos métodos de Wolfmann e Coulter para calcular o número de pontos da família de curvas, o que foi feito no Capítulo 3, sendo os resultados caso a caso apresentados nos Teoremas 3.6, 3.7 e 3.8.

Na última seção desse capítulo, estudamos quais são as condições necessárias e suficientes para que uma curva da família (1) seja maximal, isto é, atinja a conhecida cota de Hasse-Weil (indicamos novamente [30, 17]), que diz que uma curva plana de gênero g sobre $\mathbb{F}_q$ tem seu número N de pontos racionais satisfazendo

$$N \leq q + 1 + 2g\sqrt{q}\,.$$

Fechamos a tese no Capítulo 4, onde usamos os resultados sobre o número de pontos afins da família (1) para determinar sobre que condições a Hermitiana generalizada de Borges [3] dá origem a um arco completo. Mais ainda, quando não é possível obter um arco completo diretamente, apresentamos uma forma de completá-lo, isto é, indicamos como adicionar pontos do plano projetivo ao conjunto de pontos racionais da curva a fim de obter um arco completo. Em um dos casos apresentados no Teorema, encontramos um arco completo com os mesmos parâmetros do arco associado

a um certo produto de curvas Hermitianas apresentado por Giulietti et al na última seção de [15], porém usamos um argumento simples para mostrar que tais arcos não são isomorfos.

No apêndice, colecionamos alguns resultados clássicos sobre a função traço, caracteres e somas exponenciais. Introduzimos ainda alguns resultados básicos da teoria de códigos para auxiliar na compreensão do texto da tese. Para mais detalhes sobre os assuntos do apêndice, indicamos [24, 21, 30].

CAPÍTULO 1

PRELIMINARES

Nesse primeiro capítulo, apresentamos conceitos que serão utilizados ao longo da tese. Fazemos uma introdução à teoria de arcos planos, seguida pela apresentação das curvas de Artin-Schreier, que serão ferramenta importante para o resultado principal (Teorema 4.4).

Ao longo dessa parte, sejam q uma potência de primo, $\mathbb{F}_q$ o corpo finito com q elementos e $PG(2,q)$ o plano projetivo sobre $\mathbb{F}_q$.

1.1 Arcos

Para começar, estudamos uma configuração de pontos no plano projetivo que possui características interessantes do ponto de vista da geometria finita e da teoria de códigos.

Definição 1.1. Um conjunto $\mathcal{K}$ de n pontos em $PG(2,q)$ é um $(n,d)-arco$ (plano) se não mais que d pontos de $\mathcal{K}$ são colineares e há uma reta no plano que contém exatamente d pontos de $\mathcal{K}$.

Dois arcos $\mathcal{K}_1$ e $\mathcal{K}_2$ de mesmos parâmetros são ditos isomorfos se existe uma colineação T (isto é, uma aplicação bijetora que preserva pontos colineares) tal que $T(\mathcal{K}_1) = \mathcal{K}_2$.

Algumas perguntas interessantes surgem da definição 1.1:

(a) Fixados q e d para quais n_i existe algum $(n_i, d)-$arco sobre $\mathbb{F}_q$?

(b) De tais n_i qual é o maior?

(c) Existem dois (n_i, d)-arcos não isomorfos?

A última questão voltará a aparecer no Capítulo 4. Já a base para pergunta principal dessa tese segue do seguinte exemplo natural:

Exemplo 1.2. Pelo Teorema de Bèzout, o conjunto de n pontos racionais de uma curva plana $\mathcal{X}$ de grau d é um exemplo de $(n, d')-$arco, onde $d' \leq d$.

Proposição 1.3. *Fixando $d \in \mathbb{N}$ e um corpo finito $\mathbb{F}_q$, temos a seguinte cota para o número de pontos n de um $(n, d)-$arco $\mathcal{K}$:*

$$n \leq (d-1)q + d \, .$$

Demonstração. De fato, seja $P \in \mathcal{K}$. Cada reta que contém P contém no máximo outros $d-1$ pontos de $\mathcal{K} \setminus \{P\}$. Como passam $q+1$ retas por P, obtemos a cota. □

Definição 1.4. Seja $\mathcal{K}$ um $(n, d)-$arco em $PG(2, q)$. Dizemos que $\mathcal{K}$ é um $(n, d)-$arco *completo* se não está contido em um $(n+1, d)-$arco plano.

No caso de um $(n, d')-$arco associado a uma curva plana $\mathcal{X}$ de grau d (como no exemplo 1.2), a condição acima é equivalente a: dado qualquer ponto $P \in PG(2, q) \setminus \mathcal{X}(\mathbb{F}_q)$, existe uma reta racional ℓ contendo P e exatamente d' pontos de $\mathcal{X}(\mathbb{F}_q)$. No caso em que $d' = d$, dizemos que $\mathcal{X}$ tem a *propriedade do arco*.

Fechamos essa seção com uma observação sobre a relação direta entre um arco completo e um código linear.

Teorema 1.5. *Um $(n, n-d)-$arco completo $\mathcal{K}$ é equivalente a um $[n, 3, d]-$código linear $\mathcal{C}$.*

Demonstração. Consideremos $\{v_1, v_2, v_3\}$ uma base para $\mathcal{C}$. Definimos vetores u_i com $i = 1, 2, 3$ como $(u_i)_j = (v_j)_i$, isto é, a j-ésima coordenada de u_i é a $i-$ésima coordenada de v_j. A matriz dada pelas colunas u_i (ou pelas linhas v_j) é a *matriz geradora* de $\mathcal{C}$. Como o peso mínimo de um vetor v de $\mathcal{C}$ é d, então v tem no máximo $n-d$ coordenadas nulas. Assim, para todo $a_j \in \mathbb{F}_q^3$, $\sum a_j v_j$ tem no máximo $n-d$ coordenadas nulas. Isso significa que para $i = 1, ..., n$:

$$\sum_{j=1}^{3} a_j (u_i)_j = \sum_{j=1}^{3} a_j (v_j)_i = 0$$

tem no máximo $n-d$ soluções. Ou seja, no máximo $n-d$ dos n pontos são colineares. A outra implicação é análoga. □

Observação 1.6. *Notamos que, pela construção, não é possível estender tal código para outro com distância mínima maior.*

1.1.1 Arcos associados a curvas Frobenius não-clássicas

Seja $\mathcal{X}$ uma curva plana irredutível não-linear. Os números $0 = \epsilon_0 < \epsilon_1 = 1 < \epsilon_2$ representam todas as possibilidades de multiplicidades de interseção de $\mathcal{X}$ com retas do plano em um ponto genérico, já que uma reta pode não interceptar $\mathcal{X}$ em um ponto P, interceptá-la transversalmente ou tangenciá-la em tal ponto. Essa sequência é a menor na ordem lexicográfica tal que

$$det \begin{pmatrix} D_t^{\epsilon_0} x & D_t^{\epsilon_0} y & D_t^{\epsilon_0} z \\ D_t^{\epsilon_1} x & D_t^{\epsilon_1} y & D_t^{\epsilon_1} z \\ D_t^{\epsilon_2} x & D_t^{\epsilon_2} y & D_t^{\epsilon_2} z \end{pmatrix} \neq 0\,,$$

onde x, y, z definem um morfismo de $\mathcal{X}$ em $PG(2, q)$ e D_t^k denota a diferencial de

Hasse [1] de ordem k com respeito a uma variável separadora t, e é chamada sequência de ordem de $\mathcal{X}$. Caso $\epsilon_2 = 2$, a curva é dita clássica. Caso contrário, $\mathcal{X}$ é não-clássica.

A partir dessa sequência, escolhemos $\nu_0 = 0 < \nu_1$, onde $\nu_1 \in \{1, \epsilon_2\}$ é o menor inteiro tal que

$$det \begin{pmatrix} x^q & y^q & z^q \\ x & y & z \\ D_t^{\nu_1} x & D_t^{\nu_1} y & D_t^{\nu_1} z \end{pmatrix} \neq 0 \, .$$

Esses números são as ordens de Frobenius de $\mathcal{X}$ e ν_1 é dita ordem de contato genérica de uma reta com a curva $\mathcal{X}$. Se $\nu_1 = 1$, então $\mathcal{X}$ é dita $q-$Frobenius clássica. Caso contrário, $\mathcal{X}$ é $q-$Frobenius não-clássica. Notamos que isso é equivalente a dizer que $\mathcal{X} : \ F(x, y) = 0$ é $q-$Frobenius não-clássica se

$$F(x, y) | ((x^q - x)F_x + (y^q - y)F_y) \, .$$

Observação 1.7. *Geometricamente, a curva é q-Frobenius não-clássica se e somente se para todo ponto não-singular P de $\mathcal{X}$, o ponto $\Phi(P)$ pertence a reta tangente a $\mathcal{X}$ em P (onde $\Phi((x : y : z)) = (x^q : y^q : z^q)$ é o morfismo de Frobenius em P).*

Para curvas do tipo $y^d = f(x)$, estudadas por Garcia [10], temos a seguinte caracterização apontada por Borges.

Teorema 1.8. *A curva $\mathcal{X} : \ F(x, y) = y^d - f(x) = 0$ é $q-$Frobenius não-clássica se e somente se:*

(a) $d | (q - 1)$

(b) $d \, . \, f(x)(f(x)^{\frac{q-1}{d}} - 1) = (x^q - x)f'(x) \, .$

[1] Seja x um elemento transcendente sobre o corpo $\mathbb{F}$, para $i, j \in \mathbb{N}_0$, definimos $D_x^i x^j = \binom{i}{j} x^{j-i}$ e estendemos linearmente em $\mathbb{F}[x]$. Indicamos [32] para propriedades e detalhes sobre a diferencial de Hasse.

Demonstração. Temos que a propriedade da curva ser Frobenius não-clássica é equivalente a

$$(y^q - y) = \frac{F_y}{F_x}(x^q - x) \ .$$

Como $\frac{F_y}{F_x} = \frac{f'(x)}{dy^{d-1}}$, temos

$$d(y^{d+q-1} - y^d) = (x^q - x)f'(x) \ .$$

Sabemos que $y^d = f(x)$, donde

$$d(y^{d+q-1} - f(x)) = (x^q - x)f'(x) \ .$$

Em particular, $y^{d+q-1} \in \mathbb{F}_q[x]$, isto é, $d|(q-1)$. Assim:

$$d((f(x))^{\frac{q-1}{d}+1} - f(x)) = (x^q - x)f'(x) \ .$$

□

Segue diretamente do Teorema 1.8 que:

Corolário 1.9. *Se $\mathcal{X}$ é $q-$Frobenius não-clássica, então:*

(a) *$p \nmid d$ (onde p é a característica de $\mathbb{F}_q$);*

(b) *Se $f(x)$ só tem raízes simples, então todas pertencem a $\mathbb{F}_q$;*

(c) *Para todo $a \in \mathbb{F}_q$, $f(a) \in \mathbb{F}_{\frac{q-1}{d}+1}$. Em particular, se $d = \frac{p^r-1}{p^s-1}$, então $f(a) \in \mathbb{F}_{p^s}$ para todo $a \in \mathbb{F}_{p^r}$.*

Exemplo 1.10. Dado $p > 1$, as curvas de Fermat

$$x^d + y^d + z^d = 0$$

sobre $\mathbb{F}_q = \mathbb{F}_{p^n}$, onde $d = \frac{q-1}{q'-1}$ e q' é uma potência de p, são curvas Frobenius não-clássicas. A curva Hermitiana sobre $\mathbb{F}_{q^2}$ (ver exemplo 1.15) faz parte dessa família.

Exemplo 1.11. Seja q ímpar. A seguinte curva, apresentada por Garcia e Stichtenoth em [13], embora seja singular, é é $\mathbb{F}_{q^3}-$Frobenius não-clássica pelo Teorema 1.8.

$$y^{q^2+q+1} = x^{q^2+q} + x^{q^2+1} + x^{q+1} - \gamma\,,$$

onde $\gamma \in \mathbb{F}_q$ é tal que $0 \neq \gamma = N_{\mathbb{F}_{q^2}|\mathbb{F}_q}(\beta)$ com $Tr(\beta) = 0$. Tal curva tem $(q^2+q)(q^3+1)$ pontos racionais e também pode ser vista como

$$N(y) = Tr(x^{q+1}) \pmod{x^{q^3} - x} - \gamma\,,$$

onde N e Tr são respectivamente a norma e o traço de $\mathbb{F}_{q^3}$ em $\mathbb{F}_q$. A curva vista desse modo, tem forma parecida com a da curva $\mathcal{H}$ do Capítulo 2.

Não são conhecidas muitas curvas Frobenius não-clássica, porém elas tem propriedades muito interessantes (veja [16]). Por exemplo, tendem a ter muitos pontos racionais e, com a hipótese adicional de não-singularidade, podemos saber exatamente quantos são, como diz o resultado provado por Hefez e Voloch em [16]:

Teorema 1.12. *Se $\mathcal{X}$ é uma curva plana não-singular Frobenius não-clássica de grau d, então:*

$$\#\mathcal{X}(\mathbb{F}_q) = d(q - d + 2)\,.$$

As curvas Frobenius não-clássicas foram apontadas como possível "fonte"de arcos completos por essa tendência a terem muitos pontos racionais. Nessa direção, Giullieti, Pambianco, Torres e Ughi provaram o seguinte Teorema em [15].

Teorema 1.13. *Seja $\mathcal{X}$ uma curva plana F_q-Frobenius não-clássica de grau d com k pontos racionais. Então, $\mathcal{X}(F_q)$ é um $(n,d)-$arco completo se*

$$n > (d - \nu)(q + 1 - \#S) + (d - 1)\#S\,, \tag{1.1}$$

onde S é o conjunto de pontos singulares de $\mathcal{X}$ e ν é a ordem de contato genérica.

Corolário 1.14. *Se $\mathcal{X}$ for não-singular, o Teorema 1.13 nos diz que $\mathcal{X}(\mathbb{F}_q)$ é um $(n,d)-$arco completo se*

$$n > (d-\nu)(q+1). \tag{1.2}$$

Exemplo 1.15. Seja H a curva Hermitiana de grau $q+1$ sobre $\mathbb{F}_{q^2}$

$$H:\ y^{q+1} = x^q + x\,.$$

Temos que $\nu = q$ e $\#H(\mathbb{F}_{q^2}) = q^3+1$. Pelo corolário 1.14, como

$$q^3+1 > ((q+1)-q)(q^2+1) = q^2+1$$

segue que a curva tem a propriedade do arco, isto é, $H(\mathbb{F}_{q^2})$ é um $(q^3+1, q+1)-$arco completo.

Exemplo 1.16. A Quártica de Klein sobre $\mathbb{F}_8$

$$x^3y + y^3 + x = 0$$

é não-singular, tem $\nu = 2$ e 24 pontos racionais (pelo Teorema 1.12). Como

$$24 > (4-3)(9+1) = 10\,,$$

segue que tal curva também tem a propriedade do arco.

Conhecemos, porém, poucos exemplos de curvas Frobenius não-clássicas que satisfazem o Teorema 1.13. E, de fato, a condição apresentada não é necessária, como mostrado no seguinte exemplo.

Exemplo 1.17. Sejam $p > 2$, $d = p^2+p+1$ e $a, b \in \mathbb{F}_p$. Consideremos as seguintes curvas sobre $\mathbb{F}_{p^3}$.

$$\mathcal{F}:\ y^d = -(ax^d+1)/b$$

$$\mathcal{G}:\ y^d = x^d + x^{p^2} + x^p + x$$

Tais curvas são não-clássicas e Frobenius não-clássicas com $\nu = p$ ([10]) e, como são não-singulares, tem $p^5 - p^3 - p^2 + 1$ pontos racionais pelo Teorema 1.12 (mas não são isomorfas). Em [15], foi provado que ambas tem a propriedade do arco, porém observamos que não satisfazem a condição do Teorema 1.13.

Observação 1.18. *As duas curvas do exemplo 1.17 são casos especiais da seguinte família*

$$\mathcal{Z}: \ N(y) = aN(x) + bTr(x) + c$$

sobre $\mathbb{F}_{q^\ell}$ com $a, b, c \in \mathbb{F}_q$, onde N e Tr denotam as funções norma e traço de $\mathbb{F}_{q^\ell}$ em $\mathbb{F}_q$. Pelo Teorema 1.8, $\mathcal{Z}$ é uma curva Frobenius não-clássica. Se $b = 0$, então não há pontos singulares.

Se $b \neq 0$, os pontos singulares são $(1 : 0 : z)$ tais que $N_{\mathbb{F}_{q^{\ell-1}}/\mathbb{F}_q}(z) = -a/b$ e $Tr_{\mathbb{F}_{q^{\ell-1}}/\mathbb{F}_q}(z) = ca/b^2$. Se $a = 0$, o problema de determinar esses pontos é fácil. Caso contrário, a quantidade $N_\ell(-a/b, ca/b^2)$ de elementos de $\mathbb{F}_{q^\ell}$ com tal propriedade é limitada por Moisio-Wan em [28] como

$$\left| N_\ell(-a/b, ca/b^2) - \frac{q^{\ell-1} - 1}{q - 1} \right| \leq (\ell - 1)q^{\frac{\ell-2}{2}} \, . \tag{1.3}$$

Com o crescimento do número de pontos singulares, torna-se cada vez mais difícil estudar a propriedade do arco de $\mathcal{Z}$.

Por exemplo, no caso em que $a = 0$ e $b \neq 0$, consideremos a curva

$$y^{q^{\ell-1}+\cdots+q+1} = b(x^{q^{\ell-1}} + \cdots + x^q + x) + c$$

que tem um único ponto singular $(1 : 0 : 0)$ (é também seu único ponto no infinito). Dado um ponto no infinito fora da curva, isto é, um ponto do tipo $P = (\alpha : 1 : 0)$, tomemos as retas $x = \alpha y + \gamma$ com $\gamma \in \mathbb{F}_{q^\ell}$. Temos que o polinômio

$$N(y) = bTr(\alpha y) + bTr(\gamma) + c$$

tem menos de $q^{\ell-1} + \cdots + q + 1$ raízes se $\alpha \in \mathbb{F}_q$, já que a quantidade de raízes é igual ao número de elementos y em $\mathbb{F}_{q^3}$ com traço λ e norma $\alpha b\lambda + bTr(\gamma) + c$, que é limitado por Moisio-Wan como na cota (1.3). Como a reta $z = 0$ intercepta $\mathcal{Z}$ em apenas um ponto, segue que a curva não pode ter a propriedade do arco.

Até agora, vimos exemplos de curvas Frobenius não-clássicas não-singulares que apresentam a propriedade do arco. É natural, então, questionar se todas as curvas com essas características estão associadas a arcos completos. Apresentamos um exemplo que nega tal conjectura.

Exemplo 1.19. Sejam $3 \leq n \in \mathbb{N}$ e $\alpha \in \mathbb{F}_2$. Consideremos a seguinte família sobre $\mathbb{F}_{2^n}$:

$$\mathcal{X}_\alpha : \; y^{2^n-1} = \frac{x^{2^n} + x}{x^2 + x} + \alpha \, .$$

Temos que $\mathcal{X}_\alpha$ tem grau $d = 2^n - 1$ e segue do Teorema 1.8 que $\mathcal{X}_\alpha$ é 2^n-Frobenius não-clássica. Além disso, se $\alpha = 0$, então $\mathcal{X}_\alpha$ é não-singular e segue do Teorema 1.12 que

$$k = \#\mathcal{X}_0(\mathbb{F}_{2^n}) = 3(2^n - 1) = 3\,(\deg \mathcal{X}_0) \, .$$

Suponhamos que tal curva tenha a propriedade do arco, isto é, que $\mathcal{X}_0(\mathbb{F}_{2^n})$ seja um $(k, d) = (3(2^n - 1), 2^n - 1)-$arco completo. Então, tomando $P_1 \notin \mathcal{X}_0(\mathbb{F}_{2^n})$, temos que existe uma reta L_1, tal que $\#(\mathcal{X}_0 \cap L_1) = d$. Seja então $P_2 \notin (\mathcal{X}_0(\mathbb{F}_{2^n}) \cup \{P_1\})$. Existe uma reta L_2 tal que $\#(L_2 \cap \mathcal{X}_0) = d$. Temos que $L_1 \cap L_2 = \emptyset$ ou $L_1 \cap L_2 = \{\text{um único ponto racional de } \mathcal{X}_0\}$. Isto significa que até aqui já contamos $2d$ ou $2d-1$ pontos racionais de $\mathcal{X}_0$ distintos. Escolhemos agora $P_3 \notin (\mathcal{X}_0(\mathbb{F}_{2^n}) \cup \{P_1, P_2\})$. Existe uma reta L_3 tal que $\#(L_3 \cap \mathcal{X}_0) = d$ e tal reta pode interceptar nenhuma, uma ou duas das retas anteriores. No caso em que haja interseção, deve ser em um único ponto racional de $\mathcal{X}_0$ em cada reta. Isto é, depois desse passo, contamos pelo menos $3d - 3$ pontos racionais distintos em $\mathcal{X}_0$. Repetindo isso para um quarto ponto P_4, teríamos pelo menos $4d - 6$ pontos, que já é mais dos que os $3d$ pontos racionais de $\mathcal{X}_0$. Portanto, $\mathcal{X}_0$ não pode ter a propriedade do arco.

Observação 1.20. *Temos ainda que razão entre o número de pontos racionais e o grau da curva do contra-exemplo acima é muito pequena, fazendo com que não seja viável completar o arco, isto é, adicionar r pontos ao conjunto* $\mathcal{X}_0(\mathbb{F}_{2^n})$ *de forma a obter um arco completo de parâmetros* $(r + \#\mathcal{X}_0(\mathbb{F}_{2^n}), deg\,(\mathcal{X}_0(\mathbb{F}_{2^n})))$

Observação 1.21. *Embora não sejam curvas Frobenius não-clássicas, podemos proceder com um argumento análogo para os exemplos a seguir, que foram retirados de [11] e são curvas sobre $\mathbb{F}_{q^2}$ com grau q^2-1. Seja m um divisor de q^2-1, as seguintes curvas tem $m(q^2-1)$ pontos racionais.*

(a) *Seja*

$$y^m = \frac{(x^{q+1}+x+1)^q}{x^{q+1}+x^q+1}$$

onde $q \equiv 1 \pmod 3$, com $(q-1)|mdc(m, q-1)$, ou $q \equiv 2 \pmod 3$. Tomando por exemplo os pares $q^2 = 25, m = 6$ e $q^2 = 16, m = 3$ não obtemos arcos incompletos.

(b) *Seja*

$$y^m = \frac{(x^q - ax)^q}{x - a^q x^q}$$

onde $a \in \mathbb{F}_{q^2}$, $a^{q+1} \neq 1$ e $mdc(m, q-1) = q-1$. Tomando por exemplo os pares $q^2 = 9, m = 2$, $q^2 = 25, m = 2$ e $q^2 = 16, m = 3$ não é possível obter arcos completos.

O mesmo argumento serve para outros exemplos de curvas planas em que a razão entre o número de pontos racionais e o grau seja pequena.

Observação 1.22. *A curva $\mathcal{X}_1$ no exemplo 1.19 pode ser vista como*

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

que é uma das curvas com muitos pontos racionais contruídas por Garcia e Quoos em [11]. Tal curva tem $N = (2^n-2)(2^n-1)+3$ pontos racionais em $\mathbb{F}_{2^n}$ e, assim, a razão entre N e o grau de $\mathcal{X}_1$ é muito próxima ao próprio grau da curva, o que indica que a curva deve ter a propriedade do arco.

1.2 Curvas de Artin-Schreier

Uma curva de Artin-Schreier é uma curva plana com equação da forma

$$y^q + \delta y = f(x)$$

com δ em alguma extensão finita $\mathbb{K}$ de $\mathbb{F}_q$ e $f(x) \in \mathbb{K}[X]$. Mais informações podem ser encontradas no capítulo VI de [30] e tais curvas foram estudadas em diversos contextos, citamos por exemplo [9, 12, 14, 22]. Nessa classe, está, por exemplo, a curva Hermitiana $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$.

No caso em que $\delta = -1$, apresentamos dois lemas que serão passos importantes dos resultados principais. Seja $N(f)$ o número de soluções $(x, y) \in \mathbb{F}_q^2$ de $y^{p^n} - y = f(x)$ (isto é, $N(f)$ representa o número de pontos afins de tal curva). Seja tr_i o traço de $\mathbb{F}_q$ em $\mathbb{F}_{p^i}$.

Lema 1.23. *O número de $\mathbb{F}_q-$pontos afins de $y^{p^n} - y = f(x)$ é dado por*

$$p^n \cdot (\#\{a \in \mathbb{F}_q | tr_n(f(a)) = 0\}) .$$

Demonstração. Seja $(a, b) \in \mathbb{F}_q^2$ tal que $b^{p^n} - b = f(a)$. Então,

$$0 = tr_n(b^q - b) = tr(f(a)) .$$

Por outro lado, seja $a \in \mathbb{F}_q$ tal que $f(a) = \delta$ tem traço zero, então a equação $y^{p^n} - y - \delta = 0$ tem p^n possíveis soluções em $\mathbb{F}_q$. □

Seja χ_1 o caracter aditivo canônico de $\mathbb{F}_q$, isto é, $\chi_1(u) = e^{2\pi\, i\, tr_1(u)/p}$ para $u \in \mathbb{F}_q$.

Lema 1.24. *O número $N(f)$ satisfaz*

$$q\ N(f) = \sum_{h,x,y \in \mathbb{F}_q} \chi_1(h\ f(x) - h(y^{p^n} - y)) .$$

Demonstração. Se (x, y) é solução de $y^{p^n} - y = f(x)$, então

$$tr_1(h\ f(x) - h(y^{p^n} - y)) = 0$$

e

$$\chi_1(h\ f(x) - h(y^{p^n} - y)) = 1$$

qualquer que seja $h \in \mathbb{F}_q$. Para os demais $x, y \in \mathbb{F}_q$, temos $\lambda = y^{p^n} - y - f(x) \neq 0$. Consideremos, então, o caracter aditivo $\chi_\lambda(u) = \chi_1(\lambda u)$ para todo $u \in \mathbb{F}_q$ e, pelo lema A.5, temos que o somatório $\sum_{h \in \mathbb{F}_q} \chi_1(\lambda h) = 0$. □

CAPÍTULO 2

UMA GENERALIZAÇÃO DA CURVA HERMITIANA

Nesse capítulo, apresentamos uma generalização da curva Hermitiana dada por Borges em [3]. Nosso maior interesse é o arco formado por seu conjunto de pontos racionais, mas apresentamos ainda outras propriedades de tal curva.

2.1 Apresentação da curva

Sejam p um primo, $q = p^n$ e $\ell \geq 2$. Consideremos $r = r(\ell) \geq \ell/2$ o menor inteiro tal que $mdc(r, \ell) = 1$, isto é

$$r = \begin{cases} 1, & \text{se } \ell = 2 \\ (\ell+1)/2, & \text{se } \ell \text{ é ímpar} \\ \ell/2+1, & \text{se } \ell \equiv 0 \pmod 4 \\ \ell/2+2, & \text{se } \ell \equiv 2 \pmod 4. \end{cases}$$

Para qualquer z, fixamos $tr(z) := z^{q^{\ell-1}} + z^{q^{\ell-2}} + \ldots + z$ e definimos a seguinte

curva sobre $\mathbb{F}_{q^\ell}$

$$\mathcal{H}: \quad tr(y) = tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}. \tag{2.1}$$

Exemplo 2.1. Para facilitar a compreensão da equação da curva $\mathcal{H}$, vamos considerar o caso $\ell = 5$. Tomamos o primeiro inteiro r maior que $5/2$ tal que $mdc(r, 5) = 1$, isto é, $r = 3$.

Do lado esquerdo, temos

$$tr(y) = y^{q^4} + y^{q^3} + y^{q^2} + y^q + y\,.$$

Agora, para ver o lado direito, começamos com

$$tr(x^{q^3+1}) = x^{q^7+q^4} + x^{q^6+q^3} + x^{q^5+q^2} + x^{q^4+q} + x^{q^3+1}\,.$$

Depois, reduzimos o grau usando $\pmod{x^{q^5} - x}$, obtendo o polinômio

$$x^{q^2+q^4} + x^{q+q^3} + x^{1+q^2} + x^{q^4+q} + x^{q^3+1}\,.$$

Portanto, para $\ell = 5$, a curva $\mathcal{H}$ é dada pela equação

$$y^{q^4} + y^{q^3} + y^{q^2} + y^q + y = x^{q^2+q^4} + x^{q+q^3} + x^{1+q^2} + x^{q^4+q} + x^{q^3+1}$$

A curva $\mathcal{H}$ tem as seguintes características, segundo [3].

Teorema 2.2. *A curva $\mathcal{H}$ tem grau $d = q^{\ell-1} + q^{r-1}$, gênero $g = \frac{q^r(q^{\ell-1}-1)}{2}$ e $N = q^{2\ell-1} + 1$ pontos racionais sobre $\mathbb{F}_{q^\ell}$ onde apenas um é singular, o ponto $(0:1:0)$.*

Notamos que se $\ell = 2$ e $p > 2$, então $\mathcal{H}$ é a curva Hermitiana e $\mathcal{H}(\mathbb{F}_{q^2})$ é um $(q^3 + 1, q + 1)-$arco completo bem conhecido. Então, nossa investigação se foca no caso $\ell > 2$.

No Teorema 4.1 de [13], Garcia e Stichtenoth definiram a seguinte curva sobre $\mathbb{F}_{q^d}$.

$$\mathcal{C}: \; y^{q^{d-1}} + \cdots + y^q + y = x^{1+q} + x^{1+q^2} + \cdots + x^{q^{d-2}+q^{d-1}}$$

para $d \geq 2$, que pode ser vista como $s_{d,1}(y) = s_{d,2}(x)$, onde $s_{d,1}$ e $s_{d,2}$ representam o primeiro e o segundo polinômios simétricos em $\mathbb{F}_{q^d}[x]$ nas variáveis $x, x^q, \ldots, x^{q^{d-1}}$.

Tal curva foi depois estudada em [5, 27, 26]. A curva $\mathcal{C}$ possui $q^{2d-1}+1$ pontos racionais sobre $\mathbb{F}_{q^d}$, gênero $q^{d-1}(q^{d-1}-1)/2$ e grau $q^{d-2}+q^{d-1}$.

Para $d=\ell=3$, $\mathcal{C}$ e $\mathcal{H}$ são a mesma curva. Já para $d=\ell=4$ e $d=\ell=6$, coincidem o grau, o número de pontos racionais e o gênero das curvas, porém cálculos feitos no Magma ([4]) indicam que as curvas não são isomorfas (o que ocorre, provavelmente, pelas diferenças entre os semigrupos de Weierstrass sobre os únicos pontos no infinito de $\mathcal{C}$ e $\mathcal{H}$). Em geral, embora o número de pontos racionais dessas curvas sempre coincidam, o gênero e o grau de $\mathcal{H}$ são menores que os mesmos parâmetros de $\mathcal{C}$, o que torna as comparações N/g e $N/grau$ maiores.

Observação 2.3. *Em [5] e [27], os autores estudaram códigos hermitianos generalizados, isto é, códigos associados à curva $\mathcal{C}$ acima. Para isso, estudaram o semigrupo de Weierstrass e o espaço de Riemann-Roch no ponto de $\mathcal{C}$ no infinito. Para a curva $\mathcal{H}$, essa tarefa parece mais complicada.*

Considerando $p=2$ e ℓ ímpar, o semigrupo de Weierstrass no único ponto do modelo não-singular sobre $P_\infty=(0:1:0)\in\mathcal{H}(\mathbb{F}_{q^\ell})$ é

$$H(P_\infty)=\left\langle 2^{\ell-1},2^{\ell-1}+2^{r-1},2^{\ell}+2^{r-1},2^{\ell}+2^{r}+1\right\rangle ,$$

que é um semigrupo telescópico e, portanto, simétrico. Além disso, como o número de pontos racionais atinge a cota $N\leq 2^{\ell}\rho_2(P_\infty)+1$, onde $\rho_2(P_\infty)$ é o primeiro elemento não-nulo de $H(P_\infty)$ (veja [23]), segue que $\mathcal{H}$ é uma curva de Castle (conforme [26]) e podemos obter algumas informações sobre códigos em $\mathcal{H}$.

Seja $(C_m)_{m\geq 1}$ uma sequência de códigos onde cada C_m é definido como

$$C(\mathcal{H},P_1+\cdots+P_{2^{2l-1}},mP_\infty)$$

e tem dimensão k_m e distância mínima d_m. Escrevemos o semigrupo de Weierstrass em P_∞ como $H(P_\infty)=\{0=\rho_1<\rho_2<\dots\}$ e definimos a função

$$\begin{aligned}\iota:\ &\mathbb{N}_0\to\mathbb{N}\\ &m\mapsto \iota(m):=max\{i|\rho_i\leq m\}=dim\mathcal{L}(mQ)\end{aligned}$$

Segue de [26] que

$$k_m = \begin{cases} \iota(m), & \text{se } m < 2^{2\ell-1} \\ \iota(m) - \iota(m - 2^{2\ell-1}), & \text{se } m \geq 2^{2\ell-1} \end{cases}$$

e que, para $0 \leq m < n$, d_m *atinge a cota de Goppa se e somente se* $d_{2^{2\ell-1}-m}$ *também atinge. Mais ainda,* $d_{2^{2\ell-1}} \geq 2^{\ell-2}$ *e o dual de* C_m *é isométrico a* $C_{2^{2\ell-1}+2^{\ell+r-1}-2^r-2-m}$.

2.2 O problema

Estamos interessados no arco associado ao conjunto $\mathcal{H}(\mathbb{F}_{q^\ell})$ de pontos racionais sobre $\mathbb{F}_{q^\ell}$ da curva $\mathcal{H}$ definida em (2.1).

A curva $\mathcal{H}$ é Frobenius não-clássica ([3]), no entanto a abordagem do arco associado ao seu conjunto de pontos racionais não usa essa propriedade da curva (Teorema 4.4). A estratégia consiste em usar a definição de arco completo, ou seja, considerar $\mathbb{F}_{q^\ell}-$retas L no plano e contar o número de $\mathbb{F}_{q^\ell}-$pontos racionais de $\mathcal{H}$ em L.

Para uma reta $L : y = bx + c$ definimos $M_{r,n}(b, c) := \#L \cap \mathcal{H}(\mathbb{F}_{q^\ell})$. Então, $M_{r,n}(b, c)$ é o número de $\mathbb{F}_{q^\ell}$-raízes da equação

$$tr(bx + c) = tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}$$

Notamos que esse é o mesmo número de $\mathbb{F}_{q^\ell}$-raízes de

$$tr(x^{q^r+1} - bx - c) \pmod{x^{q^\ell} - x} = 0\,,$$

e, portanto, o mesmo número de $\mathbb{F}_{q^\ell}$-raízes de

$$tr(x^{q^r+1} - bx - c) = 0\,,$$

Então, pelo Lema 1.23, $M_{r,n}(b, c)$ pode ser calculado usando a relação

$$N_{r,n}(1, -b, -c) = qM_{r,n}(b, c)\,, \tag{2.2}$$

onde $N_{r,n}(1, -b, -c)$ é o número de $\mathbb{F}_{q^\ell}$-pontos afins da curva de Artin-Schreier

$$y^q - y = x^{q^r+1} - (bx + c)\,. \tag{2.3}$$

Portanto, o problema de estudar o arco associado a $\mathcal{H}$ é reduzido ao problema de contar os $\mathbb{F}_{q^\ell}$-pontos afins da curva (2.3). No próximo capítulo, calculamos o número de pontos afins de uma família mais geral de curvas de Artin-Schreier para então voltarmos ao problema apresentado.

CAPÍTULO 3

O NÚMERO DE PONTOS DE UMA CLASSE DE CURVAS ARTIN-SCHREIER

Nesse capítulo, calculamos o número de pontos afins sobre $\mathbb{F}_q$ de uma classe de curvas do tipo Artin-Schreier seguindo um raciocínio análogo ao feito por Coulter em [9] ao generalizar o trabalho Wolfmann ([33]).

3.1 A família

Sejam α, n, e inteiros positivos tais que $t = mdc(n, e)$ divide $d = mdc(\alpha, e)$. Sejam $q = p^e$ e $a, b, c \in \mathbb{F}_q$ com $a \neq 0$. Vamos representar por tr_i a função traço definida de $\mathbb{F}_q$ em $\mathbb{F}_{p^i}$. Consideremos a curva

$$\mathcal{S}: \ y^{p^n} - y = ax^{p^\alpha+1} + bx + c$$

sobre $\mathbb{F}_q$. Queremos calcular seu número $N_{\alpha,t}(a, b, c)$ de $\mathbb{F}_q$-pontos afins.

Começamos com algumas observações preliminares.

Alguns dos resultados que seguem dependem da solubilidade do polinômio

$$f(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax \tag{3.1}$$

em $\mathbb{F}_q$. O seguinte resultado foi provado por Coulter.

Lema 3.1. *([6], Teorema 4.1) Seja $p \neq 2$. A equação $f(x) = 0$ é solúvel para $x \in \mathbb{F}_q^*$ se e somente se e/d é par com $e = 2m$ e $a^{(q-1)/(p^d+1)} = (-1)^{m/d}$. Nesse caso, há $p^{2d} - 1$ soluções não-nulas.*

Para característica 2, um Teorema análogo foi provado por Coulter em [8] (Teorema 3.1), porém o omitimos pois não é utilizado nesse trabalho.

Um polinômio $f \in \mathbb{F}_q[x]$ é dito um *polinômio de permutação* se $x \mapsto f(x)$ induz uma permutação em $\mathbb{F}_q$. Se f é um polinômio linearizado, isto é, do tipo

$$L(x) = \sum_i a_i x^{p^{si}}$$

(como, por exemplo, o polinômio (3.1)) então f é um polinômio de permutação se e somente se $x = 0$ é sua única raiz em $\mathbb{F}_q$ (ver o Teorema 7.9 de [25]). Sendo assim, o lema 3.1 nos dá uma caracterização de quando o polinômio $f(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax$ é um polinômio de permutação em $\mathbb{F}_q$.

Lema 3.2. *Seja $a \in \mathbb{F}_q^*$. O polinômio $f(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax$ é um polinômio de permutação em $\mathbb{F}_q$ se e somente se e/d é ímpar ou e/d é par $e = 2m$ e $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$.*

Notamos ainda que se o polinômio $f(x)$ em (3.1) é de permutação, segue que para cada $b \in \mathbb{F}_q$, existe uma única raiz de $f(x) = b$ em $\mathbb{F}_q$.

3.2 O número $N_{\alpha,t}(a, b, c)$

Sejam novamente α, n, e inteiros positivos tais que $t = mdc(n, e)$ divide $d = mdc(\alpha, e)$ e $q = p^e$. Segue do Lema 1.24 que

Lema 3.3. *Sejam α, n, e inteiros positivos tais que $t = mdc(n, e)$ divide $d = mdc(\alpha, e)$. Sejam $q = p^e$ e $a, b, c \in \mathbb{F}_q$ com $a \neq 0$. O número de $\mathbb{F}_q-$pontos afins de $y^{p^n} - y = ax^{p^\alpha+1} + bx + c$ é*

$$N_{\alpha,t}(a, b, c) = \sum_{h\in\mathbb{F}_{p^t}} \left(\sum_{x\in\mathbb{F}_q} \chi_1(h(ax^{p^\alpha+1} + bx + c)) \right) . \tag{3.2}$$

Demonstração.

$$\begin{aligned} q\ N(f) &= \sum_{h,x,y\in\mathbb{F}_q} \chi_1(h\ f(x) - h(y^{p^n} - y)) \\ &= \sum_{h,x,y\in\mathbb{F}_q} \chi_1(h\ f(x))\chi_1(h(y^{p^n} - y)) \\ &= \sum_{h,x\in\mathbb{F}_q} \chi_1(h\ f(x)) \left(\sum_{y\in\mathbb{F}_q} \chi_1(h(y^{p^n} - y)) \right) \\ &= \sum_{h,x\in\mathbb{F}_q} \chi_1(h\ f(x)) \left(\sum_{y\in\mathbb{F}_q} \chi_1(y^{p^n}(h^{p^n} - h)) \right) . \end{aligned}$$

Se $h \in \mathbb{F}_{p^t}$ então $\sum_{y\in\mathbb{F}_q} \chi_1(y^{p^n}(h^{p^n} - h)) = q$, caso contrário, pelo Lema A.6, a soma é 0. Portanto,

$$q\ N(f) = q \sum_{h\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_q} \chi_1(h\ f(x))$$

□

Lema 3.4. *Seja $L(x) = \sum_{i=0}^{e/t-1} b_i x^{p^{ti}} \in \mathbb{F}_q[x]$. Defina $b = \sum_{i=0}^{e/t-1} b_i^{p^{e-ti}}$. Então, o número de pontos afins da curva*

$$y^{p^n} - y = ax^{p^\alpha+1} + L(x) + c$$

com as mesmas condições do Lema 3.3 é também dado por $N_{\alpha,t}(a, b, c)$ como no Lema 3.3.

Demonstração. O resultado segue notando-se que $\prod_{i=1}^{e/t-1} \chi_1(hb_i x^{p^{ti}}) = hbx$. □

Consideremos a seguinte soma

$$R_\alpha(a,b,c) = \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1} + bx + c)\,. \tag{3.3}$$

Em [6, 7, 8] Coulter calculou $R_\alpha(a,0,0)$ e $R_\alpha(a,b,0)$. Notamos que

$$\chi_1(ax^{p^\alpha+1} + bx + c) = \chi_1(ax^{p^\alpha+1} + bx)\ \chi_1(c)$$

o que implica em

$$\begin{aligned} R_\alpha(a,b,c) &= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1} + bx)\ \chi_1(c) \\ &= \chi_1(c) \left(\sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1} + bx) \right) \\ &= \chi_1(c)\ R_\alpha(a,b,0) \end{aligned}$$

Seja η o caracter quadrático de $\mathbb{F}_q$ (como em (A.2) no apêndice A.2). Pela observação acima, calculamos (3.3) usando resultados de [9]:

Teorema 3.5. *Seja $f(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax$. Então, $R_\alpha(a,b,c) = 0$ a menos dos seguintes casos*

(a) *Se e/d é ímpar:*

I) ([9], pg 8, Teorema 4.6) Se $p \equiv 1 \pmod 4$ e x_0 é a única solução de $f(x) = -b^{p^\alpha}$ em $\mathbb{F}_q$:

$$R_\alpha(a,b,c) = (-1)^{e-1}\ \sqrt{q}\ \eta(-a)\ \chi_1(c)\ \overline{\chi_1(ax_0^{p^\alpha+1})}\,.$$

II) ([9], pg 8, Teorema 4.6) Se $p \equiv 3 \pmod 4$ e x_0 é a única solução de $f(x) = -b^{p^\alpha}$ em $\mathbb{F}_q$:

$$R_\alpha(a,b,c) = (-1)^{e-1} i^{3e}\ \sqrt{q}\ \eta(-a)\ \chi_1(c)\ \overline{\chi_1(ax_0^{p^\alpha+1})}\,.$$

III) ([9], pg 7, Teorema 4.5) Se $p = 2$, então, como $mdc(2^e - 1, 2^\alpha + 1) = 1$, existe $\kappa \in \mathbb{F}_q^*$ o único elemento de $\mathbb{F}_q$ tal que $\kappa^{2^\alpha+1} = a$:

$$R_\alpha(a,b,c) = R_\alpha(1, b\kappa^{-1}, c)\,.$$

i. Se $tr_d(b) \neq 1$, então $R_\alpha(1,b,c) = 0$;

ii. Se $tr_d(b) = 1$, então existe $w \in \mathbb{F}_q$ tal que $b = w^{2^{2\alpha}} + w + 1$ e

$$R_\alpha(1,b,c) = \chi_1(w^{2^\alpha} + w + c)\left(\frac{2}{e/d}\right)^d 2^{(e+d)/2}$$

onde $\left(\frac{2}{s}\right)$ é o símbolo de Jacobi, isto é,

$$\left(\frac{2}{s}\right) = \begin{cases} 1, & \text{se } e/d \equiv \pm 1 \pmod 8 \\ -1, & \text{se } e/d \equiv \pm 3 \pmod 8 \end{cases} \tag{3.4}$$

(b) *([9], pg 8, Teorema 4.7) Se e/d é par e $e = 2m$:*

I) Se $f(x)$ é um polinômio de permutação e x_0 é a única solução de $f(x) = -b^{p^\alpha}$ em $\mathbb{F}_q$:

$$R_\alpha(a,b,c) = (-1)^{m/d} p^m \chi_1(c)\, \overline{\chi_1(a x_0^{p^\alpha+1})}\,.$$

II) Se $f(x)$ não é um polinômio de permutação, mas $f(x) = -b^{p^\alpha}$ é solúvel em $\mathbb{F}_q$ com solução x_0:

$$R_\alpha(a,b,c) = (-1)^{m/d+1} p^{m+d} \chi_1(c)\, \overline{\chi_1(a x_0^{p^\alpha+1})}\,.$$

O Teorema anterior será usado agora para calcular $N_{\alpha,t}(a,b,c)$ (partindo do resultado do Lema 3.3) em três etapas: e/d ímpar e $p = 2$, e/d e p ímpares, e/d par e p qualquer.

Teorema 3.6. *Seja tr_d o traço de $\mathbb{F}_q$ em $\mathbb{F}_{p^d}$. Suponhamos e/d ímpar e $p = 2$. Seja $\kappa \in \mathbb{F}_q^*$ o único elemento de $\mathbb{F}_q$ tal que $\kappa^{2^\alpha+1} = a$. Então, $N_{\alpha,t}(a,b,c) = N_{\alpha,t}(1, b\kappa^{-1}, c)$.*

(a) *Se $tr_d(b) \notin \mathbb{F}_{2^t}^*$ então $N_{\alpha,t}(1,b,c) = q$;*

(b) *Se $tr_d(b) \in \mathbb{F}_{2^t}^*$ então $N_{\alpha,t}(1,b,c) = q + \chi_1(\omega^{2^\alpha+1} + \omega + c\, tr_d(b)^{-2})(\frac{2}{e/d})^d 2^{(e+d)/2}$ onde $\omega \in \mathbb{F}_q$ é o único elemento tal que $b\, tr_d(b)^{-1} = \omega^{2^{2\alpha}} + \omega + 1$.*

Demonstração. Pela definição de κ temos que

$$\sum_{x\in\mathbb{F}_q}\chi_1(hax^{2^\alpha+1}+hbx)=\sum_{x\in\mathbb{F}_q}\chi_1(h(\kappa x)^{2^\alpha+1}+hb\kappa^{-1}(\kappa x))\,.$$

Trocando κx por y temos:

$$\sum_{x\in\mathbb{F}_q}\chi_1(hax^{2^\alpha+1}+hbx)=\sum_{y\in\mathbb{F}_q}\chi_1(hy^{2^\alpha+1}+hb\kappa^{-1}y)\,.$$

Então

$$\begin{aligned}N_{\alpha,t}(a,b,c)&=q+\sum_{h\in\mathbb{F}_{2^t}^*}\chi_1(ch)\left(\sum_{y\in\mathbb{F}_q}\chi_1(hy^{2^\alpha+1}+hb\kappa^{-1}y)\right)\\&=q+\sum_{h\in\mathbb{F}_{2^t}^*}\sum_{y\in\mathbb{F}_q}\chi_1(hy^{2^\alpha+1}+hb\kappa^{-1}y+ch)\\&=N_{\alpha,t}(1,b\kappa^{-1},c)\,.\end{aligned}$$

Assim, podemos nos ater ao cálculo de $N_{\alpha,t}(1,b,c)$. Para cada $h\in\mathbb{F}_{2^t}^*$, como $mdc(2^t-1,2^\alpha+1)=1$, existe um único $\omega\in\mathbb{F}_{2^t}^*$ tal que $\omega^{2^\alpha+1}=h$. Então

$$\begin{aligned}N_{\alpha,t}(1,b,c)&=q+\sum_{h\in\mathbb{F}_{2^t}}\sum_{x\in\mathbb{F}_q}\chi_1(hx^{2^\alpha+1}+hbx+hc)\\&=q+\sum_{w\in\mathbb{F}_{2^t}}\sum_{x\in\mathbb{F}_q}\chi_1((\omega x)^{2^\alpha+1}+b\omega^{2^\alpha}(\omega x)+c\omega^{2^\alpha+1})\\&=q+\sum_{\omega\in\mathbb{F}_{2^t}^*}R_\alpha(1,\omega b,c\omega^2)\,,\end{aligned}$$

pois, como $w\in\mathbb{F}_{2^t}^*\subseteq\mathbb{F}_{2^\alpha}$, segue que $\omega^{2^\alpha}=\omega$. Pelo Teorema 3.5, ítem (a)-III, $R_\alpha(1,\omega b,c\omega^{2^\alpha+1})=0$ a menos que $1=tr_d(b\omega)=\omega tr_d(b)$. Se $tr_d(b)\notin\mathbb{F}_{2^t}^*$, então $\omega tr_d(b)\neq 1$ para todo $\omega\in\mathbb{F}_{2^t}^*$, o que implica em $N_{\alpha,t}(1,b,c)=q$. Se $tr_d(b)$ é um elemento não-nulo de $\mathbb{F}_{2^t}$ então para todo $\omega\neq tr_d(b)^{-1}$ ainda temos $N_{\alpha,t}(1,b,c)=q$. Resta apenas o caso em que $\omega=tr_d(b)^{-1}$, que implica em

$$N_{\alpha,t}(1,b,c)=q+R_\alpha(1,b\,tr_d(b)^{-1},c\,tr_d(b)^{-2})$$

O resultado segue então do Teorema 3.5, ítem (a)-III. □

Teorema 3.7. *Seja tr_t o traço de $\mathbb{F}_q$ em $\mathbb{F}_{p^t}$ e η o caracter quadrático de $\mathbb{F}_{p^t}$. Sejam e/d e p ímpares. Seja $x_0 \in \mathbb{F}_q$ a única solução de $a^{p^\alpha}x^{p^{2\alpha}} + ax = -b^{p^\alpha}$. Seja $c_1 = ax_0^{p^\alpha+1} - c$. Há duas possibilidades.*

(a) *Se e/t é ímpar e $tr_t(ax_0^{p^\alpha+1} - c) = 0$ então $N_{\alpha,t}(a,b,c) = q$. Caso contrário*

$$N_{\alpha,t}(a,b,c) = \begin{cases} q + p^{(e+t)/2}\eta(a\ tr_t(c_1)), & \text{if } p \equiv 1 \pmod 4 \\ q + (-1)^{(3e+t)/2}p^{(e+t)/2}\eta(c_1), & \text{if } p \equiv 3 \pmod 4 \,. \end{cases}$$

(b) *Se e/t é par e $e = 2m$*

$$N_{\alpha,t}(a,b,c) = \begin{cases} q - (p^t-1)p^m\eta(a), & \text{se } p \equiv 1 \pmod 4 \text{ e } tr_t(c_1) = 0 \\ q + p^m\eta(a), & \text{se } p \equiv 1 \pmod 4 \text{ e } tr_t(c_1) \neq 0 \\ q - (-1)^m(p^t-1)p^m\eta(a), & \text{se } p \equiv 3 \pmod 4 \text{ e } tr_t(c_1) = 0 \\ q + (-1)^m p^m\eta(a), & \text{se } p \equiv 3 \pmod 4 \text{ e } tr_t(c_1) \neq 0 \,. \end{cases}$$

Demonstração. Se $p \equiv 1 \pmod 4$ então pelo Teorema 3.5, ítem (a)-I:

$$\begin{aligned} N_{\alpha,t}(a,b,c) &= q + \sum_{h \in \mathbb{F}_{p^t}^*} (-1)^{e-1}\sqrt{q}\ \eta(-ah)\ \chi_1(ch)\ \overline{\chi_1(ahx_0^{p^\alpha+1})} \\ &= q + (-1)^{e-1}p^{e/2}\ (\sum_{h \in \mathbb{F}_{p^t}^*} \eta(-ah)\ \chi_1(ch)\ \overline{\chi_1(ahx_0^{p^\alpha+1})}) \,. \end{aligned}$$

Se e/t é ímpar e η' é o caracter quadrático de $\mathbb{F}_{p^e}$, então, pelo lema A.2, temos

que

$$\begin{aligned}\sum_{h\in\mathbb{F}^*_{p^t}} \eta(-ah)\ \chi_1(ch)\ \overline{\chi_1(ahx_0^{p^\alpha+1})} &= \eta(a)\sum_{h\in\mathbb{F}^*_{p^t}} \eta(-h)\chi_1(-h(ax_0^{p^\alpha+1}-c))\\ &= \eta(a)\sum_{h\in\mathbb{F}^*_{p^t}} \eta'(-h)\mu_1(tr_t(-h(ax_0^{p^\alpha+1}-c)))\\ &= \eta(a)\sum_{h\in\mathbb{F}^*_{p^t}} \eta'(-h)\mu_1(-h\ tr_t(ax_0^{p^\alpha+1}-c))\\ &= \eta(a)\sum_{h\in\mathbb{F}^*_{p^t}} \eta'(-h)\mu(-h)\\ &= \eta(a)G(\eta',\mu)\ ,\end{aligned}$$

onde $G(\eta',\mu)$ é a soma Gaussiana em $\mathbb{F}^*_{p^t}$, μ_1 é o caracter multiplicativo de $\mathbb{F}_{p^t}$ e $\mu = \mu_{tr_1(ax_0^{p^\alpha+1}-c)}$. Usamos os lemas A.7 e A.8 para calcular $G(\eta',\mu)$. Se $tr_1(ax_0^{p^\alpha+1}-c) = 0$ então μ é o caracter aditivo trivial e a soma acima é 0, o que implica em $N_{\alpha,t}(a,b,c) = q$. Suponhamos que o traço seja não-nulo.

$$\begin{aligned}G(\eta',\mu) &= G(\eta',\mu_{tr_t(ax_0^{p^\alpha+1})})\\ &= \eta'(tr_t(ax_0^{p^\alpha+1}))G(\eta',\mu_1)\\ &= \eta'(tr_t(ax_0^{p^\alpha+1}))\ (-1)^{e-1}\sqrt{p^t}\ .\end{aligned}$$

Portanto

$$\begin{aligned}N_{\alpha,t}(a,b,c) &= q+\eta(a)\eta(tr_t(ax_0^{p^\alpha+1}-c))((-1)^{e-1})^2p^{e/2}p^{t/2}\\ &= q+p^{(e+t)/2}\eta(a\ tr_t(ax_0^{p^\alpha+1}-c))\ .\end{aligned}$$

Agora, suponhamos e/t par. Então, $\eta(-h)=1$ para todo $h\in\mathbb{F}^*_{p^t}$ e

$$\begin{aligned}\sum_{h\in\mathbb{F}^*_{p^t}} \eta(-ah)\chi_1(ch)\overline{\chi_1(ahx_0^{p^\alpha+1})} &= \eta(a)\sum_{h\in\mathbb{F}^*_{p^t}} \eta(-h)\chi_1(h(c-ax_0^{p^\alpha+1}))\\ &= \eta(a)\sum_{h\in\mathbb{F}^*_{p^t}} \chi_1(h(c-ax_0^{p^\alpha+1}))\ .\end{aligned}$$

Usando o Lema A.6 segue que

$$\sum_{h\in\mathbb{F}_{p^t}^*}\chi_1(h(c-ax_0^{p^\alpha+1}))=\begin{cases}p^t-1, & \text{if } tr_t(c-ax_0^{p^\alpha+1})=0\\ -1, & \text{if } tr_t(c-ax_0^{p^\alpha+1})\neq 0\,.\end{cases} \tag{3.5}$$

Logo

$$N_{\alpha,t}(a,b,c)=\begin{cases}q-(p^t-1)p^m\eta(a), & \text{se } tr_t(b-ax_0^{p^\alpha+1})=0\\ q+p^m\eta(a), & \text{se } tr_t(b-ax_0^{p^\alpha+1})\neq 0\,.\end{cases}$$

O caso em que e/d é ímpar e $p\equiv 3 \pmod 4$ é análogo (usando o Teorema 3.5, ítem (a)-II).

□

Teorema 3.8. *Seja tr_t o traço de $\mathbb{F}_q$ em $\mathbb{F}_{p^t}$. Seja e/d par e $e=2m$. Se $a^{p^\alpha}x^{p^{2\alpha}}+ax=-b^{p^\alpha}$ não é solúvel em $\mathbb{F}_q$ então $N_{\alpha,t}(a,b,c)=q$. Caso contrário, seja x_0 uma raiz de $a^{p^\alpha}x^{p^{2\alpha}}+ax=-b^{p^\alpha}$ em $\mathbb{F}_q$, há duas possibilidades:*

(a) *Se $f(x)=a^{p^\alpha}x^{p^{2\alpha}}+ax$ não é um polinômio de permutação*

$$N_{\alpha,t}(a,b,c)=q+\begin{cases}(-1)^{m/d+1}p^{m+d}(p^t-1), & se\ tr_t(-c+ax_0^{p^\alpha+1})=0\\ (-1)^{m/d}p^{m+d}, & se\ tr_t(-c+ax_0^{p^\alpha+1})\neq 0\,.\end{cases}$$

(b) *Se $f(x)=a^{p^\alpha}x^{p^{2\alpha}}+ax$ é um polinômio de permutação*

$$N_{\alpha,t}(a,b,c)=q+\begin{cases}(-1)^{m/d}p^m(p^t-1), & se\ tr_t(-c+ax_0^{p^\alpha+1})=0\\ (-1)^{m/d+1}p^m, & se\ tr_t(-c+ax_0^{p^\alpha+1})\neq 0\,.\end{cases}$$

Demonstração. Se $a^{p^\alpha}x^{p^{2\alpha}}+ax+b^{p^\alpha}=0$ não é solúvel em $\mathbb{F}_q$, então $R(ah,bh,ch)=0$ e $N_{\alpha,t}(a,b,c)=q$. Suponhamos então que o polinômio acima seja solúvel com solução $x_0\in\mathbb{F}_q$.

Se $f(x)=a^{p^\alpha}x^{p^{2\alpha}}+ax$ não é um polinômio de permutação então pelo Teorema 3.5, ítem (b)-II:

$$
\begin{aligned}
N_{\alpha,t}(a,b,c) &= q + \sum_{h\in\mathbb{F}_{p^t}^*} (-1)^{m/d+1} p^{m+d} \chi_1(ch)\overline{\chi_1(ahx_0^{p^\alpha+1})} \\
&= q + (-1)^{m/d+1} p^{m+d} \sum_{h\in\mathbb{F}_{p^t}^*} \chi_1(ch - ahx_0^{p^\alpha+1}) \\
&= q + (-1)^{m/d+1} p^{m+d} \sum_{h\in\mathbb{F}_{p^t}^*} \chi_1(h(c - ax_0^{p^\alpha+1}))\,.
\end{aligned}
$$

Usando (3.5) temos

$$
N_{\alpha,t}(a,b,c) = q + \begin{cases} (-1)^{m/d+1} p^{m+d}(p^t-1), & \text{se } tr_t(c - ax_0^{p^\alpha+1}) = 0 \\ (-1)^{m/d} p^{m+d}, & \text{se } tr_t(c - ax_0^{p^\alpha+1}) \neq 0\,. \end{cases}
$$

Se $f(x)$ é um polinômio de permutação então, pelo Teorema 3.5, ítem (b)-II:

$$
\begin{aligned}
N_{\alpha,t}(a,b,c) &= q + \sum_{h\in\mathbb{F}_{p^t}^*} (-1)^{m/d} p^{m} \chi_1(ch)\overline{\chi_1(ahx_0^{p^\alpha+1})} \\
&= q + (-1)^{m/d} p^{m} \sum_{h\in\mathbb{F}_{p^t}^*} \chi_1(h(c - ax_0^{p^\alpha+1}))\,.
\end{aligned}
$$

□

3.3 Curvas maximais

Na seção anterior, determinamos o número de $\mathbb{F}_q-$pontos afins da curva

$$
y^{p^n} - y = ax^{p^\alpha+1} + L(x) + c\,, \tag{3.6}
$$

onde $q = p^e$, $t = mdc(n,e)$ divide $d = mdc(\alpha,e)$, $b,c \in \mathbb{F}_q$, $a \in \mathbb{F}_q^*$ e $L(x) = \sum_{i=0}^{e/t-1} b_i x^{p^{ti}}$. É claro que tal curva tem apenas um ponto no infinito.

Suponhamos $\deg L(x) \leq p^\alpha$. Então, o grau do polinômio $ax^{p^\alpha+1} + L(x) + c$ é $p^\alpha + 1$, que é primo com p. Segue então (Teorema VI.4.1 de [30]) que a curva (3.6) é

absolutamente irredutível, não-singular e, logo, tem gênero $g = p^\alpha(p^n - 1)/2$. Além disso, seu número de pontos racionais sobre $\mathbb{F}_q$ é dado por $N = N_{\alpha,t}(a, b, c) + 1$, onde $N_{\alpha,t}(a, b, c)$ foi determinado nos teoremas 3.6, 3.7, 3.8.

Para a curva (3.6), a cota de Hasse-Weil é

$$N \leq q + 1 + p^\alpha(p^n - 1)\sqrt{q}\ . \tag{3.7}$$

Assim, para determinar os casos em que tal curva é maximal, precisamos inicialmente exigir $e = 2m$, tornando a cota (3.7) a seguinte

$$N \leq q + 1 + p^{\alpha+m}(p^n - 1)\ . \tag{3.8}$$

Dessa forma, as única possibilidades de termos uma curva maximal são as do Teorema 3.8. Considerando tr_t a função traço definida de $\mathbb{F}_q$ em $\mathbb{F}_{p^t}$ e analisando os valores de $N_{\alpha,t}(a, b, c)$ nesse teorema, temos que os únicos resultados que se assemelham à cota (3.8) são os casos:

(a) Caso 1:

(a) O polinômio $f(x) = a^{p^\alpha}x^{p^{2\alpha}} + ax$ não é um polinômio de permutação;

(b) A equação $f(x) = -b^{p^\alpha}$ tem alguma solução x_0 em $\mathbb{F}_q$;

(c) $tr_t(-c + ax_0^{p^\alpha+1}) = 0$

(b) Caso 2:

(a) O polinômio $f(x) = a^{p^\alpha}x^{p^{2\alpha}} + ax$ é um polinômio de permutação;

(b) A única solução de $f(x) = -b^{p^\alpha}$ em $\mathbb{F}_{q^\ell}$ é x_0 é tal que $tr_t(-c+ax_0^{p^\alpha+1}) = 0$.

No caso 1 acima, temos $N_{\alpha,t}(a, b, c) = q + (-1)^{m/d}p^m(p^t - 1)$. Comparando com a cota (3.8), vemos que precisamos exigir m/d par, $\alpha = 0$ e $n|e$. Porém, quando $\alpha = 0$, temos $d = mdc(e, \alpha) = e$, donde $m/d = 1/2$, o que não é possível.

Resta então apenas o segundo caso acima. Nesse caso, temos

$$N_{\alpha,t}(a, b, c) = q + (-1)^{m/d+1}p^{m+d}(p^t - 1)\ .$$

Comparando esse valor com a cota (3.8), vemos que ainda precisamos exigir que $n|\alpha$ e $\alpha|m$ (para termos $n = t$ e $d = \alpha$) e que m/d seja ímpar. Assim, obtemos o seguinte teorema.

Teorema 3.9. *Seja $\mathcal{C}$ a curva dada pela equação (3.6) sobre $\mathbb{F}_q$. Temos que o número de $\mathbb{F}_q-$pontos racionais de $\mathcal{C}$ atinge a cota de Hasse-Weil se e somente se todas as condições abaixo são satisfeitas.*

(a) $e = 2m$;

(b) $n|\alpha$ *e* $\alpha|m$;

(c) m/d *ímpar;*

(d) *O polinômio* $f(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax$ *não é um polinômio de permutação;*

(e) *A equação* $f(x) = -b^{p^\alpha}$ *tem alguma solução* x_0 *em* $\mathbb{F}_q$;

(f) $tr_t(-c + ax_0^{p^\alpha+1}) = 0$.

Exemplo 3.10. Apresentamos um exemplo de curva maximal do tipo (3.6).

Tomamos $m \in \mathbb{N}$, $q = 2^{2m}$ e $n = \alpha = m$ (satisfazendo a condição (b) do Teorema 3.9). Temos $f(x) = x^{2^{2m}} + x$ não é um polinômio de permutação, já que dado qualquer $s \in \mathbb{F}_{2^{2m}}$, temos $s^{2^{2m}} = s$ e, portanto, $f(s) = 0$. Assim, para $b = 0$, a condição (d) do Teorema 3.9 é sempre satisfeita. Consideramos, por exemplo, $x_0 = 1$ e escolhemos $c \in \mathbb{F}_{2^{2m}}$ tal que $tr_m(c) = tr_m(1)$ (onde tr_m é a função traço definida de $\mathbb{F}_{2^{2m}}$ em $\mathbb{F}_{2^m}$). Segue do Teorema 3.9 que a curva

$$y^{2^m} - y = x^{2^m+1} + c$$

é maximal sobre $\mathbb{F}_{2^{2m}}$.

CAPÍTULO 4

O ARCO PLANO ASSOCIADO À CURVA $\mathcal{H}$

Nesse capítulo, voltamos ao problema apresentado na seção 2.2. Sejam $\ell > 2$ e $r \leq \ell/2$ o primeiro inteiro tal que $mdc(\ell, r) = 1$. Começamos usando os Teoremas 3.6, 3.7, 3.8 para determinar o número de pontos afins sobre $\mathbb{F}_{q^\ell}$ da curva

$$\mathcal{A}: \; y^q - y = x^{q^r+1} - (bx + c)$$

e, em seguida, determinamos em que condições o arco associado a curva $\mathcal{H}$

$$tr(y) = tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}$$

é completo.

4.1 Número de pontos racionais da curva $\mathcal{A}$

Nos Teoremas 3.6, 3.7, 3.8 da seção 3.2, calculamos o número $N_{\alpha,t}(a, b, c)$ de pontos afins sobre $\mathbb{F}_q$ da curva

$$\mathcal{S}: \; y^{p^n} - y = ax^{p^\alpha+1} + bx + c\,,$$

onde

(a) $q = p^e$;

(b) $a, b, c \in \mathbb{F}_q$;

(c) $t = mdc(n, e)$ divide $d = mdc(\alpha, e)$.

Agora, usamos tais resultados para determinar o número de pontos afins sobre $\mathbb{F}_{q^\ell}$ da curva

$$\mathcal{A} : \, y^q - y = x^{q^r+1} - (bx + c) \, ,$$

onde $\ell > 2$ e $r \geq \frac{\ell}{2}$ é o menor inteiro tal que $mdc(r, \ell) = 1$ (como definido em (2.1)).

Fazendo $p^e = q^\ell$, temos $e = n\ell$ e $q = p^n$ e a curva $\mathcal{A}$ pode ser vista como

$$y^{p^n} - y = x^{p^{nr}+1} - (bx + c)$$

Ou seja, agora, em notação da curva $\mathcal{S}$, temos:

(a) $\alpha = nr$

(b) $t = mdc(n, n\ell) = n$

(c) $d = mdc(nr, n\ell) = n \, mdc(r, \ell) = n$

Logo, queremos calcular $N_{nr,n}(1, -b, -c)$, que vamos tratar como $N_{r,\ell}(1, -b, -c)$.

Assim, por exemplo, no Teorema 3.7, as hipóteses

(a) e/d ímpar,

(b) p ímpar,

(c) η o caracter quadrático de $\mathbb{F}_{p^t}$,

(d) $x_0 \in \mathbb{F}_q$ a única solução de $a^{p^\alpha} x^{p^{2\alpha}} + ax = -b^{p^\alpha}$,

tornam-se

(a) $n\ell/n = \ell$ ímpar,

(b) p ímpar,

(c) η o caracter quadrático de $\mathbb{F}_q$,

(d) $x_0 \in \mathbb{F}_{q^\ell}$ a única solução de $x^{q^{2r}} + x = b^{q^r}$

Agora, como $e/t = n\ell/n = \ell$ e já consideramos ℓ ímpar como hipótese, temos que apenas o caso (a) do Teorema 3.7 é possível e, definindo tr como a função traço de $\mathbb{F}_{q^\ell}$ em $\mathbb{F}_q$, seu resultado se traduz aqui como

$$N_{r,\ell}(1,-b,-c) = \begin{cases} q^\ell, & \text{se } tr(c_1) = 0 \\ q^\ell + q^{(\ell+1)/2}\eta(tr(c_1)), & \text{se } p \equiv 1 \pmod 4 \\ q^\ell + (-1)^{n(3\ell+1)/2} q^{(\ell+1)/2}\eta(tr(c_1)), & \text{se } p \equiv 3 \pmod 4 . \end{cases}$$

Trabalhamos analogamente com as hipóteses dos Teoremas 3.6 e 3.8, notando ainda que:

Observação 4.1. *Como $f(x) = x^{q^{2r}} + x \in \mathbb{F}_{q^\ell}[x]$ é um polinômio linearizado, então é de permutação se e somente se sua única raiz é o zero. Porém, em característica 2, é claro que $f(1) = 0$, donde $f(x)$ não é um polinômio de permutação independentemente de ℓ e r. Além disso, pelo Lema 3.2, temos que, em característica ímpar, $f(x)$ é um polinômio de permutação se e somente se ℓ ou $\ell/2$ é ímpar.*

Portanto, obtemos o seguinte resultado.

Teorema 4.2. *Sejam tr a função traço definida de $\mathbb{F}_{q^\ell}$ em $\mathbb{F}_q$ e η o caracter quadrático de $\mathbb{F}_q$. Sobre o número $N_{r,\ell}(1,-b,-c)$ de pontos afins sobre $\mathbb{F}_{q^\ell}$ da curva*

$$\mathcal{A} : \; y^q - y = x^{q^r+1} - (bx + c) ,$$

temos os seguintes possíveis casos:

(a) *Sejam ℓ e p ímpares. Sejam x_0 a única raiz de $x^{q^{2r}}+x=b^{q^r}$ em $\mathbb{F}_{q^\ell}$ e $c_1 = x_0^{q^r+1}+c$. Se $tr(c_1)=0$, então $N_{r,\ell}(1,-b,-c)=q^\ell$, caso contrário*

$$N_{r,\ell}(1,-b,-c)=\begin{cases} q^\ell + q^{(\ell+1)/2}\eta(tr(c_1)), & \text{se } p\equiv 1 \pmod 4 \\ q^\ell + (-1)^{n(3\ell+1)/2}q^{(\ell+1)/2}\eta(tr(c_1)), & \text{se } p\equiv 3 \pmod 4 . \end{cases}$$

(b) *Sejam ℓ par, p ímpar e $e=2m$ (isto é, $n\ell=2m$). Se $x^{q^{2r}}+x=b^{q^r}$ não é solúvel em $\mathbb{F}_{q^\ell}$, então $N_{r,\ell}(1,-b,-c)=q^\ell$, caso contrário sejam $x_0\in\mathbb{F}_{q^\ell}^*$ uma raiz de $x^{q^{2r}}+x=b^{q^r}$ e $c_1=x_0^{q^r+1}+c$:*

$$N_{r,\ell}(1,-b,-c)=\begin{cases} q^\ell - q^r(q-1), & \text{se } \ell\equiv 0 \pmod 4 \text{ e } tr(c_1)=0 \\ q^\ell + q^r, & \text{se } \ell\equiv 0 \pmod 4 \text{ e } tr(c_1)\neq 0 \\ q^\ell - q^{r-2}(q-1), & \text{se } \ell\equiv 2 \pmod 4 \text{ e } tr(c_1)=0 \\ q^\ell + q^{r-2}, & \text{se } \ell\equiv 2 \pmod 4 \text{ e } tr(c_1)\neq 0 . \end{cases}$$

(c) *Sejam ℓ ímpar e p par. Se $\gamma := tr(b)=0$ então $N=q^\ell$, caso contrário*

$$N_{r,\ell}(1,-b,-c)=\begin{cases} q^\ell + q^r, & \text{se } tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(k)=0 \text{ e } \ell\equiv\pm 1 \pmod 8 \\ q^\ell - q^r, & \text{se } tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(k)=1 \text{ e } \ell\equiv\pm 1 \pmod 8 \\ q^\ell + q^r, & \text{se } tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(k)=0, n \text{ é par e } \ell\equiv\pm 3 \pmod 8 \\ q^\ell - q^r, & \text{se } tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(k)=0, n \text{ é ímpar e } \ell\equiv\pm 3 \pmod 8 \\ q^\ell - q^r, & \text{se } tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(k)=1, n \text{ é par e } \ell\equiv\pm 3 \pmod 8 \\ q^\ell + q^r, & \text{se } tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(k)=1, n \text{ é ímpar e } \ell\equiv\pm 3 \pmod 8 , \end{cases}$$

onde $\omega\in\mathbb{F}_{q^\ell}$ é o único elemento de $\mathbb{F}_{q^\ell}$ tal que $\omega^{q^{2r}}+\omega+1=b\gamma^{-1}$ e $k := \omega^{q^r}+\omega-c\gamma^{-2}$.

(d) *Sejam ℓ e p pares. Se $x^{q^{2r}}+x=b^{q^r}$ não é solúvel em $\mathbb{F}_{q^\ell}$ então $N_{r,\ell}(1,-b,-c)=q^\ell$, caso contrário sejam $x_0\in\mathbb{F}_{q^\ell}^*$ uma raiz de $x^{q^{2r}}+x=b^{q^r}$ e $c_1=x_0^{q^r+1}+c$,*

então

$$N_{r,\ell}(1,-b,-c) = q^{\ell} + \begin{cases} -q^r(q-1), & \text{se } \ell \equiv 0 \pmod 4 \text{ e } tr(c_1) = 0 \\ +q^r, & \text{se } \ell \equiv 0 \pmod 4 \text{ e } tr(c_1) \neq 0 \\ +q^{r-1}(q-1), & \text{se } \ell \equiv 2 \pmod 4 \text{ e } tr(c_1) = 0 \\ -q^{r-1}, & \text{se } \ell \equiv 2 \pmod 4 \text{ e } tr(c_1) \neq 0 \end{cases}$$

Observação 4.3. *Seja $L(x)$ um polinômio linearizado dado por*

$$L(x) = \sum_{i=0}^{\ell-1} b_i x^{q^i}$$

e defina $b := \sum_{i=0}^{\ell-1} b_i^{q^{\ell-i}}$. Então, pelo Lema 3.4, o número de pontos afins da curva de Artin-Schreier

$$y^q - y = x^{q^r+1} - L(x) - c$$

é também dado por $N_{r,\ell}(1,-b,-c)$ como no Teorema 4.2. Isso será útil na demonstração do resultado principal.

4.2 O arco $\mathcal{H}(\mathbb{F}_{q^\ell})$

Agora, utilizamos o Teorema 4.2 para estudar o arco formado pelos $\mathbb{F}_{q^\ell}-$pontos racionais de $\mathcal{H}$. Para isso, usamos a relação

$$N_{r,\ell}(1,-b,-c) = qM_{r,\ell}(b,c)$$

(como em (2.2)) entre o número $N_{r,\ell}(1,-b,-c)$ de pontos afins sobre $\mathbb{F}_{q^\ell}$ da curva

$$\mathcal{A}: \; y^q - y = x^{q^r+1} - (bx+c)$$

e o número $M_{r,\ell}(b,c)$ de raízes em $\mathbb{F}_{q^\ell}$ do polinômio

$$tr(bx+c) = tr(x^{q^r+1}) \pmod{x^{q^\ell} - x},$$

que é o mesmo número de pontos racionais da curva

$$\mathcal{H}: \ tr(y) = tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}$$

em uma reta $L: \ y = bx + c$.

Teorema 4.4. *Seja $\mathcal{H}$ a curva definida por $tr(y) = tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}$ onde $\ell > 2$ e $r \geq \ell/2$ é o menor inteiro tal que $mdc(\ell, r) = 1$ (como em (2.1)). Então:*

(a) *$\mathcal{H}(\mathbb{F}_{q^\ell})$ é um $(q^{2\ell-1} + 1, q^{\ell-1} + q^{r-1})-$arco completo se e somente se ℓ e p são ímpares*

(b) *$\mathcal{H}(\mathbb{F}_{q^\ell})$ é um $(q^{2\ell-1} + 1, q^{\ell-1} + q^{\ell/2-1})$-arco completo se e somente se p é ímpar e $\ell \equiv 2 \pmod 4$.*

Nos demais casos, $\mathcal{H}(\mathbb{F}_{q^\ell})$ não é um arco completo, mas pode ser completado como segue. Seja H o conjunto

$$H = \{b \in \mathbb{F}_{q^\ell} \mid x^{q^{2r}} + x = b^{q^r} \text{ é solúvel em } \mathbb{F}_{q^\ell}\}$$

(a) *Se $\ell \equiv 0 \pmod 4$,*

$$\mathcal{H}(\mathbb{F}_{q^\ell}) \cup \{(1 : b_i : 0) \mid b_i \notin H, \, i = 1, \ldots, q^{\ell-1} + q^{r-1} - 1\}$$

é um $(q^{2\ell-1} + q^{\ell-1} + q^{r-1}, q^{\ell-1} + q^{r-1})$-arco completo.

(b) *Se p é par e $\ell \equiv 2 \pmod 4$,*

$$\mathcal{H}(\mathbb{F}_{q^\ell}) \cup \{(1 : b_i : 0) \mid b_i \notin H, \, i = 1, \ldots, q^{\ell-1} + q^{r-2}(q-1) - 1\}$$

é um $(q^{2\ell-1} + q^{\ell-1} + q^{r-2}(q-1), q^{\ell-1} + q^{r-2}(q-1))$-arco completo.

(c) *Se p é par ℓ é ímpar, então*

$$\mathcal{H}(\mathbb{F}_{q^\ell}) \cup \{(1 : b : 0) \mid tr(b) = 0\}$$

é um $(q^{2\ell-1} + q^{\ell-1} + 1, q^{\ell-1} + q^{r-1})$-arco completo.

Demonstração. **Caso 1: ℓ e p são ímpares.**

Nesse caso, $r = \frac{\ell+1}{2}$.

Apresentamos o cálculo no caso em que $p \equiv 1 \pmod 4$, os demais casos são análogos.

Se $(a : b : 1)$ é um ponto no complementar de $\mathcal{H}(\mathbb{F}_{q^\ell})$ então, pelo ítem (a) do Teorema 4.2, uma reta $y = m(x-a)+b$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{\ell-1}+q^{r-1}$ pontos se e somente se

$$tr(x_0^{q^r+1} + b - ma)$$

é um quadrado não-nulo em $\mathbb{F}_q$ onde $x_0 \in \mathbb{F}_{q^\ell}$ é a única raiz de $x^{q^{2r}} + x = m^{q^r}$ (já que $x^{q^{2r}} + x$ é um polinômio de permutação em $\mathbb{F}_{q^\ell}$).

Como cada $m \in \mathcal{H}(\mathbb{F}_{q^\ell})$ tem correspondência com um único $x_0 \in \mathbb{F}_{q^\ell}$ tal que $x_0^q + x_0 = m^{q^r}$, então

$$x_0^{q^r} + x_0^{q^{r-1}} = (x_0^q + x_0)^{q^{r-1}} = (m^{q^r})^{q^{r-1}} = m^{q^{2r-1}} = m^{q^\ell} = m$$

e

$$tr(x_0^{q^r+1} + b - ma) = tr(x_0^{q^r+1} - a(x_0^{q^r} + x_0^{q^{r-1}}) + b)$$

Portanto, existe $x_0 \in \mathbb{F}_{q^\ell}$ tal que $tr(x_0^{q^r+1} + b - ma)$ é um quadrado não-nulo em $\mathbb{F}_q$ se e somente se existe $\lambda \in \mathbb{F}_q^*$ um quadrado e $\lambda' \in \mathbb{F}_{q^\ell}$ com $tr(\lambda') = \lambda$ tais que

$$tr(x_0^{q^r+1} - a(x_0^{q^r} + x_0^{q^{r-1}}) + b - \lambda') = 0\,.$$

A existência de um $x_0 \in \mathbb{F}_{q^\ell}$ tal que isso aconteça é, pelo Lema 1.23, equivalente à existência de pelo menos um ponto afim na curva de Artin-Schreier

$$y^q - y = x_0^{q^r+1} - a(x_0^{q^r} + x_0^{q^{r-1}}) + b - \lambda'$$

Mas, ainda pela Nota 4.3 e pelo ítem (a) do Teorema 4.2, tal curva de Artin-Schreier tem pelo menos $q^\ell - q^{\ell/2}$ pontos afins. Logo, existe $x_0 \in \mathbb{F}_{q^\ell}$ tal que o $m \in \mathbb{F}_{q^\ell}$ correspondente produz uma reta $y = m(x-a)+b$ que intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ in $q^{\ell-1}+q^{r-1}$ $\mathbb{F}_{q^\ell}$-pontos racionais.

Por fim, todas as retas que passam por um ponto do tipo $(1 : b : 0)$ com $b \in \mathbb{F}_{q^\ell}$ são do tipo $L : \ y = bx + \gamma$ com $\gamma \in \mathbb{F}_{q^\ell}$. Temos que, pelo ítem (a) do Teorema 4.2, L intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $N = q^{\ell-1} + q^{r-1}$ pontos se e somente se $tr(x_0^{q^r+1} + \gamma)$ é um quadrado não-nulo em $\mathbb{F}_q$.

Sejam $\lambda \in \mathbb{F}_q$ um quadrado não-nulo e $\lambda' \in \mathbb{F}_{q^\ell}$ tais que $tr(\lambda') = \lambda$. Escolhemos $\gamma := \lambda' - x_0^{q^r+1}$. Então:

$$tr(x_0^{q^r+1} + \gamma) = tr(x_0^{q^r+1} + \lambda' - x_0^{q^r+1}) = tr(\lambda') = \lambda$$

e isso conclui a prova de que $\mathcal{H}(\mathbb{F}_{q^\ell})$ é um $(q^{2\ell-1} + 1, q^{\ell-1} + q^{r-1})$-arco completo.

Caso 2: p é ímpar e $\ell \equiv 2 \pmod 4$.

Nesse caso, temos que $r = \frac{\ell}{2} + 2$.

Seja $(a : b : 1)$ um ponto no complementar de $\mathcal{H}(\mathbb{F}_{q^\ell})$. Pelo ítem (b) do Teorema 4.2, a reta $y = m(x - a) + b$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{\ell-1} + q^{\ell/2-1}$ pontos se e somente se existe $m \in \mathbb{F}_{q^\ell}$ tal que a única solução $x_0 \in \mathbb{F}_{q^\ell}$ de $x^{q^{2r}} + x = m^{q^r}$ satisfaz

$$tr(x_0^{q^r+1} - ma + b) \neq 0 \, .$$

Reescrevendo o traço a partir de $x_0^{q^{2r}} + x_0 = m^{q^r}$, temos

$$tr(x_0^{q^r+1} - ax_0^{q^{\ell-r+4}} - ax_0^{q^{\ell-r}} + b) \neq 0 \, .$$

Suponhamos que para todo $m \in \mathbb{F}_{q^\ell}$ temos $tr(x_0^{q^r+1} - ma + b) = 0$. Então, pelo Lema 1.23, a curva de Artin-Schreier

$$y^q - y = x_0^{q^r+1} - ax_0^{q^{\ell-r+4}} - ax_0^{q^{\ell-r}} + b$$

tem $q^{\ell+1}$ pontos afins sobre $\mathbb{F}_{q^\ell}$. Mas, pela Nota 4.3 e pelo ítem (b) do Teorema 4.2, tal curva tem no máximo $q^\ell + q^{\ell/2}$ pontos afins, donde podemos escolher $x_0 \in \mathbb{F}_{q^\ell}$ e tomar o $m \in \mathbb{F}_{q^\ell}$ correspondente afim de obter uma reta que intercepta $\mathcal{H}$ em $q^{\ell-1} + q^{\ell/2-1}$ pontos racionais sobre $\mathbb{F}_{q^\ell}$.

Para cada ponto $(1 : b : 0)$, pelo ítem (b) do Teorema 4.2, a reta $y = bx + \gamma$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{\ell-1} + q^{\ell/2-1}$ pontos se e somente se $tr(\gamma + x_0^{q^r+1}) \neq 0$, o que é sempre possível já que a função traço é sobrejetiva.

Portanto, $\mathcal{H}(\mathbb{F}_{q^\ell})$ é um $(q^{2\ell-1}+1, q^{\ell-1}+q^{\ell/2-1})_{q^\ell}-$arco completo.

Caso 3: $\ell \equiv 0 \pmod 4$**.**

Nesse caso, $r = \ell/2 + 1$.

Pelos ítens 2 e 4 do Teorema 4.2 (não importando a característica de $\mathbb{F}_{q^\ell}$), uma reta $y = m(x-a)+b$ contém $(a:b:1) \notin \mathcal{H}(\mathbb{F}_{q^\ell})$ e intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{l-1}+q^{r-1}$ pontos se e somente se existe uma solução $x_0 \in \mathbb{F}_{q^\ell}$ de $x^{q^{2r}}+x = m^{q^r}$ tal que

$$tr(x_0^{q^r+1} - ma + b) \neq 0\,.$$

Suponhamos que para todo $x_0 \in \mathbb{F}_{q^\ell}$ o traço acima é zero. Então,

$$tr(x_0^{q^r+1} - a(x_0^{q^{\ell-r+2}} + x_0^{q^{\ell-r}}) + b) = 0\,,$$

o que, pelo Lema 1.23, é equivalente a curva de Artin-Schreier

$$y^q - y = x^{q^r+1} - a(x_0^{q^{\ell-r+2}} + x_0^{q^{\ell-r}}) + b$$

ter $q^{\ell+1}$ pontos racionais. Porém, ainda pelos ítens 2 e 4 do Teorema 4.2, tal curva tem no máximo $q^\ell + q^r$ pontos racionais.

Para os pontos $(1:b:0) \notin \mathcal{H}(\mathbb{F}_{q^\ell})$, pelos ítens 2 e 4 do Teorema 4.2, a reta $y = bx+\gamma$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{\ell-1}+q^{r-1}$ pontos se e somente se existe $x_0 \in \mathbb{F}_{q^\ell}$ tal que $x_0^{q^{2r}} + x_0 = b^{q^r}$ e $tr(x_0^{q^r+1}+\gamma) \neq 0$.

É fácil ver que se $x^{q^{2r}}+x = b^{q^r}$ é solúvel em $\mathbb{F}_{q^\ell}$ então todas suas soluções estão em $\mathbb{F}_{q^\ell}$ e podemos escolher γ tal que $tr(x_0^{q^r+1}-\gamma) \neq 0$.

Assim, ficamos apenas com os casos em que $x^{q^{2r}}+x = b^{q^r}$ não é solúvel. Nesses casos, qualquer reta $y = bx+\gamma$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em menos de $q^{\ell-1}+q^{r-1}$ pontos racionais e, então, precisamos completar o arco com alguns pontos de forma que isso seja solucionado. A maneira mais natural é escolhendo $q^{\ell-1}+q^{r-1}-1$ pontos no infinito, de forma que a reta $z=0$ passe por tais pontos e por $(0:1:0)$, o único ponto no infinito de $\mathcal{H}$. Porém, precisamos garantir que isso é possível, estimando a quantidade de elementos $b \in \mathbb{F}_{q^\ell}$ para os quais a equação $x^{q^{2r}}+x = b^{q^r}$ não é solúvel.

Consideramos o conjunto

$$H = \{b \in \mathbb{F}_{q^\ell} | x^{q^{2r}} + x = b^{q^r} \text{ é solúvel em } \mathbb{F}_{q^\ell}\} .$$

Definimos o polinômio

$$h := \prod_{b \in H} (x^{q^2} + x - b^{q^r}) ,$$

então h tem $q^2(\#H)$ raízes em $\mathbb{F}_{q^\ell}$. Como $q^2(\#H) \leq q^\ell$ então $\#H \leq q^{\ell-2}$. Assim, o complementar de H em $\mathbb{F}_{q^\ell}$ tem pelo menos $q^\ell - q^{\ell-2}$ elementos. Portanto, é possível escolher $q^{\ell-1} + q^{r-1} - 1$ pontos $(1 : b : 0)$ com $b \notin H$ para completar o arco obtendo um $(q^{2\ell-1} + q^{\ell-1} + q^{r-1}, q^{\ell-1} + q^{r-1})_{q^\ell}-$arco completo.

Caso 4: p é par e $\ell \equiv 2 \pmod 4$.

Usamos o ítem (d) do Teorema 4.2 de forma análoga ao caso anterior, obtendo um arco completo de parâmetros $(q^{2\ell-1} + q^{\ell-1} + q^{r-2}(q-1), q^{\ell-1} + q^{r-2}(q-1))$.

Caso 5: p é par e ℓ é ímpar.

Nesse caso, $r = \frac{\ell+1}{2}$.

Apresentamos o caso em que $\ell \equiv \pm 1 \pmod 8$, os demais são análogos.

Seja $(a : b : 1) \notin \mathcal{H}(\mathbb{F}_{q^\ell})$. Então, pelo ítem (c) do Teorema 4.2, a reta $y = m(x-a)+b$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{\ell-1} + q^{r-1}$ pontos se e somente se $\alpha = tr(m) \neq 0$ e

$$tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(\omega^{q^r+1} + \omega + (b - ma)\alpha^{-2}) = 0 ,$$

onde $\omega \in \mathbb{F}_{q^\ell}$ é o único elemento tal que $\omega^q + \omega + 1 = m\alpha^{-1}$. Temos que

$$tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(\omega^{q^r+1} + \omega + (b - ma)\alpha^{-2}) = 0$$

é equivalente a

$$tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(\omega^{q^r+1} - a\alpha^{-1}\omega^q + \omega(1 - a\alpha^{-1}) + b\alpha^{-2} - a\alpha^{-1}) = 0 .$$

Suponhamos que para todo $\omega \in \mathbb{F}_{q^\ell}$ temos que o traço acima é não-nulo. Então, pelo Lema 1.23, a curva de Artin-Schreier

$$y^2 - y = \omega^{q^r+1} - a\alpha^{-1}\omega^q + \omega(1 - a\alpha^{-1}) + b\alpha^{-2} - a\alpha^{-1}$$

não tem pontos afins em $\mathbb{F}_{q^\ell}$. Porém, tal curva está na família $\mathcal{S}$ definida na seção 3.2 e, pelo Teorema 3.6, tem pontos afins em Fl.

Para os pontos $(1 : b : 0)$ a reta $y = bx + \gamma$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{\ell-1} + q^{r-1}$ pontos se e somente se $\alpha = tr(b) \neq 0$ e

$$tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(\omega^{q^r+1} + \omega + \gamma\alpha^{-2}) = 0\,,$$

onde $\omega \in \mathbb{F}_{q^\ell}$ é o único elemento tal que $\omega^{q+1} + \omega + \alpha = b$. Se $\alpha \neq 0$ escolhemos $\gamma = -\alpha^2(\omega^{q^r+1} + \omega)$ e segue que

$$\begin{aligned} tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(\omega^{q^r+1} + \omega + \gamma\alpha^{-2}) & \\ &= tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(\omega^{q^r+1} + \omega - \alpha^2(\omega^{q^r+1} + \omega)\alpha^{-2}) \\ &= tr_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(0) = 0\,. \end{aligned}$$

Se $\alpha = 0$ então toda reta $y = bx + \gamma$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $q^{\ell-1} - q^{r-1}$ pontos. Portanto, o conjunto

$$A = \mathcal{H}(\mathbb{F}_{q^\ell}) \cup \{(1 : b : 0) \mid tr(b) = 0\}$$

é um $(q^{2\ell-1} + q^{\ell-1} + 1, q^{\ell-1} + q^{r-1})_{q^\ell}-$arco completo. □

Observação 4.5. *Em [15], foi estudado o seguinte produto de curvas Hermitianas sobre* $\mathbb{F}_{q^\ell}$

$$\mathcal{X}_B : \prod_{\lambda \in B} \lambda X^{q^{\ell/2}+1} + XY^{q^{\ell/2}} + X^{q^{\ell/2}}Y + Z^{q^{\ell/2}+1} = 0\,.$$

Foi considerado ℓ *par e* B *um subconjunto de* $\mathbb{F}^*_{q^{\ell/2}}$ *contendo* b *elementos e foi provado que* $\mathcal{X}_B(\mathbb{F}_{q^\ell})$ *é um* $(q^{\ell+\ell/2}b + 1, b(q^{\ell/2} + 1))-$*arco completo se e somente se* $1 \leq b \leq q^{\ell/2} - 1$.

Seja B *um subconjunto de* $\mathbb{F}^*_{q^{\ell/2}}$ *com* $b = q^{\ell/2-1}$ *elementos, então* $\mathcal{X}_B(\mathbb{F}_{q^\ell})$ *é um arco completo com os mesmos parâmetros do encontrado no Teorema 4.4 no caso em que* p *é ímpar e* $\ell \equiv 2 \pmod 4$. *Afirmamos que tais arcos não são isomorfos.*

De fato, se tais arcos fossem isomorfos, existiria uma colineação T *em* $PG(2, q^\ell)$ *tal que* $T(\mathcal{H}(\mathbb{F}_{q^\ell})) = \mathcal{X}_B(\mathbb{F}_{q^\ell})$. *Como* $\mathcal{H}$ *é irredutível e tem grau maior do que* $\mathcal{X}_B$ *(que*

é redutível) então, pelo Teorema de Bézout, haveria $(q^{\ell-1}+q^{r-1})(q^{\ell-1}+q^{r-3})$ *pontos na interseção de* $\mathcal{H}$ *e* $\mathcal{X}_B$*, isto é, haveria pelo menos essa quantidade de pontos tanto em* $\mathcal{H}$ *quanto em* $\mathcal{X}_B$*. Como tal número é maior que* $q^{2\ell-1}+1$*, temos uma contradição.*

APÊNDICE A

ALGUNS RESULTADOS CLÁSSICOS

A.1 Função traço

Seja q uma potência de um primo p. Consideremos as extensões finitas

$$\mathbb{F}_q \subset \mathbb{F}_{q^k} \subset \mathbb{F}_{q^{mk}} .$$

Definição A.1. Para $u \in \mathbb{F}_{q^k}$, o traço $tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(u)$ de u sobre $\mathbb{F}_q$ é definido por

$$tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(u) := u^{q^{k-1}} + u^{q^{k-2}} + \cdots + u^q + u$$

Da definição acima temos as seguintes propriedades:

Lema A.2. (a) $tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(u+v) = tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(u) + tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(v)$ *para todos* $u, v \in \mathbb{F}_{q^k}$;

(b) $tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\lambda u) = \lambda\, tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(u)$ *para todos* $\lambda \in \mathbb{F}_q$ *e* $u \in \mathbb{F}_{q^k}$;

(c) $tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\lambda) = k\lambda$ *para todo* $\lambda \in \mathbb{F}_q$;

(d) $tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(u^q) = tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(u)$ *para todo* $u \in \mathbb{F}_{q^k}$.

A seguir, temos um resultado sobre a transitividade do traço:

Lema A.3. *Consideremos as extensões finitas* $\mathbb{F}_q \subset \mathbb{F}_{q^k} \subset \mathbb{F}_{q^{mk}}$. *Então:*

$$tr_{\mathbb{F}_{q^{mk}}/\mathbb{F}_q}(u) = tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(tr_{\mathbb{F}_{q^{mk}}/\mathbb{F}_{q^k}}(u))$$

para todo $u \in \mathbb{F}_{q^\ell}$.

Demonstração. Temos $[\mathbb{F}_{q^k} : \mathbb{F}_q] = k$, então temos:

$$\begin{aligned} tr_{\mathbb{F}_{q^{mk}}/\mathbb{F}_q}(u) &= \sum_{i=0}^{mk-1} u^{q^i} \\ &= \sum_{i=0}^{k-1}\sum_{j=0}^{m-1} u^{q^{jk+i}} \\ &= \sum_{i=0}^{k-1}(\sum_{j=0}^{m-1} u^{q^{jk}})^{q^i} \\ &= \sum_{i=0}^{k-1}(tr_{\mathbb{F}_{q^{mk}}/\mathbb{F}_{q^k}}(u))^{q^i} \\ &= tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(tr_{\mathbb{F}_{q^{mk}}/\mathbb{F}_{q^k}}(u)) \end{aligned}$$

□

A.2 Caracteres

Sejam G um grupo finito de ordem n e $\mathbb{C}^*$ o grupo multiplicativo do corpo $\mathbb{C}$. Um *caracter* de G é um homomorfismo de grupos $\chi : G \to \mathbb{C}^*$, isto é, $\chi(gh) = \chi(g)\chi(h)$ para todo $g, h \in G$. Em particular, $\chi(e) = 1$ se e é o elemento neutro multiplicativo de G. Temos que

$$1 = \chi(e) = \chi(g^n) = \chi(g)^n$$

para todo $g \in G$, donde $\chi(g)$ é uma raiz da unidade de ordem n, em particular

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}\,,$$

onde $\overline{\chi(g)}$ é o conjugado complexo de $\chi(g)$.

Consideremos o grupo aditivo de $\mathbb{F}_q$ e a função $tr = tr_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$. A função

$$\chi_1(u) = e^{2\pi\, i\, tr(u)/p}$$

é um caracter do grupo aditivo chamado *caracter aditivo canônico de* $\mathbb{F}_q$ já que

$$\chi_1(u+v) = \chi_1(u)\chi_1(v)$$

para todos $u, v \in \mathbb{F}_q$.

Além disso, dado $b \in \mathbb{F}_q$, temos que a função definida por $\chi_b(u) := \chi_1(bu)$, para cada $u \in \mathbb{F}_q$, é também um caracter aditivo de $\mathbb{F}_q$ já que:

$$\chi_b(u+v) = \chi_1(bu+bv) = \chi_1(bu)\chi_1(bv) = \chi_b(u)\chi_b(v)\,.$$

Do Lema A.3 e da definição do caracter aditivo canônico, temos o seguinte resultado:

Lema A.4. *Consideremos as extensões finitas* $\mathbb{F}_q \subset \mathbb{F}_{q^k} \subset \mathbb{F}_{q^{mk}}$ *e* χ_1 *e* μ_1 *os caracteres aditivos canônicos de* $\mathbb{F}_{q^k} \to \mathbb{F}_q$ *e* $\mathbb{F}_{q^{mk}} \to \mathbb{F}_q$ *respectivamente. Então:*

$$\chi_1(tr_{\mathbb{F}_{q^{mk}}/\mathbb{F}_{q^k}}(u)) = \mu_1(u)$$

para todo $u \in \mathbb{F}_{q^{mk}}$.

Os caracteres do grupo multiplicativo $\mathbb{F}_q^*$ são dados por

$$\psi_j(g^k) = e^{2\pi ijk/(q-1)}$$

onde g é um elemento primitivo de $\mathbb{F}_q^*$ e $k = 0, 1, \ldots, q-2$. Segue daí que para todo j:

$$\sum_{u\in\mathbb{F}_q^*} \psi_j(u) = 0\,. \tag{A.1}$$

Tomando $j = (q-1)/2$ temos o *caracter quadrático de* $\mathbb{F}_q$, que é dado por

$$\eta(u) = \begin{cases} 1, & \text{se } u \text{ é um quadrado em } \mathbb{F}_q \\ -1, & \text{caso contrário}\,. \end{cases} \tag{A.2}$$

Notamos que existe uma relação entre o caracter quadrático η de $\mathbb{F}_{q^{mk}}$ e o caracter quadrático η' de $\mathbb{F}_{q^k}$:

$$\eta(h) = \begin{cases} 1, & \text{se } m \text{ é par} \\ \eta'(h), & \text{se } m \text{ é ímpar} \end{cases}$$

A.3 Somas exponenciais

Seja χ_1 o caracter aditivo canônico de $\mathbb{F}_q$ como na seção anterior. Para $b \in \mathbb{F}_q$, seja $\chi_b(u) = \chi_1(bu)$, para todo $u \in \mathbb{F}_q$, um caracter aditivo não-trivial de $\mathbb{F}_q$ para $\mathbb{F}_p$. Como para cada $u \in \mathbb{F}_q$, temos que $\chi_1(u)$ é uma raiz da unidade de ordem p e estamos percorrendo todos os elementos de $\mathbb{F}_q$, então:

Lema A.5. $\sum_{u \in \mathbb{F}_q} \chi_b(u) = 0$

Vamos usar o resultado abaixo diversas vezes:

Lema A.6. *Para $\mathbb{F}_q = \mathbb{F}_{p^e}$ e $\zeta \in \mathbb{F}_q$ e $k|e$, temos*

$$\sum_{\beta \in \mathbb{F}_{p^k}} \chi_1(\zeta\beta) = \begin{cases} p^k, & \textit{se } tr_{\mathbb{F}_q/\mathbb{F}_{p^k}}(\zeta) = 0 \\ 0, & \textit{caso contrário}\,. \end{cases}$$

Demonstração. Para todo $\beta \in \mathbb{F}_{p^k}$ temos $tr_{\mathbb{F}_q/\mathbb{F}_{p^k}}(\beta\zeta) = \beta\, tr_{\mathbb{F}_q/\mathbb{F}_{p^k}}(\zeta)$, assim:

$$\begin{aligned} \chi_1(\zeta\beta) &= e^{2\pi i tr_{\mathbb{F}_q/\mathbb{F}_p}(\zeta\beta)/p} \\ &= e^{2\pi i tr_{\mathbb{F}_{p^k}/\mathbb{F}_p}(tr_{\mathbb{F}_q/\mathbb{F}_{p^k}}(\zeta\beta))/p} \\ &= e^{2\pi i tr_{\mathbb{F}_{p^k}/\mathbb{F}_p}(\beta\, tr_{\mathbb{F}_q/\mathbb{F}_{p^k}}(\zeta))/p}\,. \end{aligned}$$

Agora, se $tr_{\mathbb{F}_q/\mathbb{F}_{p^k}}(\zeta) = 0$, temos que $\chi_1(\zeta\beta) = 1$ para todo β, donde $\sum_{\beta \in \mathbb{F}_{p^k}} \chi_1(\beta\zeta) = p^k$. Caso contrário, como $\delta = tr_{\mathbb{F}_q/\mathbb{F}_{p^k}}(\zeta) \in \mathbb{F}_{p^k}$, então, pelo lema A.5 aplicado à extensão $F_{p^k}|\mathbb{F}_p$, temos o resultado. □

Dados ψ um caracter multiplicativo e χ um caracter aditivo de $\mathbb{F}_q$, definimos a *soma Gaussiana*:

$$G(\psi, \chi) = \sum_{u \in \mathbb{F}_q} \psi(u)\chi(u) \ ,$$

que satisfaz as seguintes propriedades:

Lema A.7. (a) $G(\psi, \chi_0) = 0$ *se* $\psi \neq \psi_0$*;*

(b) $G(\psi, \chi_{ab}) = \overline{\psi(a)}G(\psi, \chi_b)$ *para todos* $a \in \mathbb{F}_q^*$ *e* $b \in \mathbb{F}_q$*.*

Demonstração. *(a)* Segue de (A.1), já que $\chi_0(u) = 1$ para todo $u \in \mathbb{F}_q$.

(b) Temos que $\chi_{ab}(u) = \chi_b(au)$, então

$$\begin{aligned} G(\psi, \chi_{ab}) &= \sum_{u \in \mathbb{F}_q^*} \psi(u)\chi_{ab}(u) \\ &= \sum_{u \in \mathbb{F}_q^*} \psi(u)\chi_b(au) \\ &= \sum_{au \in \mathbb{F}_q^*} \psi(a^{-1}au)\chi_b(au) \\ &= \sum_{au \in \mathbb{F}_q^*} \psi(a^{-1})\psi(au)\chi_b(au) \\ &= \psi(a^{-1}) \sum_{au \in \mathbb{F}_q^*} \psi(au)\chi_b(au) \\ &= \overline{\psi(a)}G(\psi, \chi_b) \ . \end{aligned}$$

□

Teorema A.8. *([25], Teorema 5.15, pg 199) Seja* $\mathbb{F}_q$ *um corpo finito com* $q = p^e$*, onde* p *é um primo ímpar e* $e \in \mathbb{N}$*. Seja* η *o caracter quadrático de* $\mathbb{F}_q$ *e* χ_1 *o caracter aditivo canônico de* $\mathbb{F}_q$*. Então:*

$$G(\eta, \chi_1) = \begin{cases} (-1)^{e-1}\sqrt{q}, & \text{se } p \equiv 1 \pmod 4 \\ (-1)^{e-1}i^e\sqrt{q}, & \text{se } p \equiv 3 \pmod 4 \ . \end{cases}$$

A.4 Códigos lineares

Definição A.9. Um código linear $\mathcal{C}$ sobre $\mathbb{F}_q$ é um subespaço vetorial não nulo de $\mathbb{F}_q^n$, $n \geq 1$. Dizemos que n é o comprimento de $\mathcal{C}$ e $k := \dim \mathcal{C}$ é a dimensão de $\mathcal{C}$ sobre $\mathbb{F}_q$.

Os elementos de $\mathbb{F}_q$ formam o alfabeto, e os elementos de $\mathcal{C}$ são ditos palavras do código.

Uma matriz geradora M para $\mathcal{C}$ é uma matriz $k \times n$ sobre $\mathbb{F}_q$ cujas linhas formam uma base para $\mathcal{C}$. Um elemento $y \in \mathbb{F}_q^k$ é codificado como $u = yM \in \mathbb{F}_q^n$, isto é, $C = \{yM \mid y \in \mathbb{F}_q^k\}$.

Definimos o *peso* de $u \in \mathbb{F}_q^n$ como o número de coordenadas não nulas de u e denotamos por $w(u)$. Definimos a *distância entre* $u, v \in \mathbb{F}_q^n$ como

$$d(u, v) = d(u - v, 0) := w(u - v).$$

Por fim, definimos a *distância mínima de* $\mathcal{C}$ como

$$d = \min\{w(u) \mid 0 \neq u \in C\}.$$

Definição A.10. Um código linear $\mathcal{C}$ sobre $\mathbb{F}_q$ com comprimento n, dimensão k e distância mínima d é dito um $[n, k, d]-$código.

Durante a transmissão de uma informação codificada através de um canal de comunicação, podem ocorrer eventuais erros. Então, é preciso garantir que o código $\mathcal{C}$ utilizado seja capaz de identificar e corrigir erros para que possamos recuperar a mensagem original.

Seja $t \in \mathbb{N}$. Dizemos que um código linear $\mathcal{C}$ *corrige* t *erros* se para todo $y \in \mathbb{F}_q^n$ existe no máximo uma palavra u em $\mathcal{C}$ tal que $d(y, u) \leq t$.

Sejam $u \in C$ uma palavra transmitida e x a informação recebida com no máximo t erros. Se $\mathcal{C}$ corrige t erros, então temos $d(x, u) \leq t$ e $d(x, v) > t$ para toda palavra $v \neq u$ do código. Isto significa que u é a palavra de $\mathcal{C}$ mais próxima de x e, portanto, a informação correta.

O próximo resultado deixa clara a importância do tamanho da distância mínima de um código.

Proposição A.11. *Seja $\mathcal{C}$ um código linear com distância mínima d. Então, $\mathcal{C}$ pode corrigir até $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros, onde $\lfloor x \rfloor$ denota a parte inteira de x.*

Demonstração. Sejam $u, v \in C$ e $B_t(u)$ e $B_t(v)$ bolas de raio $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ centradas em u e v respectivamente. Suponhamos que exista $x \in B_t(u) \cap B_t(v)$. Então,

$$d(u, v) \leq d(u, x) + d(x, v) \leq t + t \leq d - 1,$$

o que é uma contradição se $u \neq v$, já que a distância mínima de $\mathcal{C}$ é d.

Dessa forma, se transmitimos a palavra $u \in C$ e recebemos y com $r \leq t$ erros, temos $d(u, y) = r \leq t$ e $d(v, y) > t$ para toda palavra $v \in C$ diferente de u. □

Desde que a teoria de códigos corretores de erros foi introduzida por C. E. Shanon em 1948, ela tem se tornado uma área cada vez mais explorada. Na década de 80, o russo V. D. Goppa utilizou curvas algébricas para introduzir novos códigos dessa classe, os códigos geométricos de Goppa, que descrevemos a seguir. Seja $\mathcal{X}$ uma curva algébrica sobre $\mathbb{F}_q$ de gênero g. Seja $\mathbb{F}_q(\mathcal{X})$ o corpo de funções algébricas associado a $\mathcal{X}$. Consideramos $P_1, \ldots, P_n$ lugares de grau 1 distintos, definimos $D = P_1 + \cdots + P_n$ e escolhemos G um divisor de $\mathbb{F}_q(\mathcal{X})$ tal que $supp(G) \cap supp(D) = \emptyset$. Definimos o espaço vetorial $\mathcal{L}(G) := \{f \in F | (f) + G \geq 0\}$. O código geométrico de Goppa $C_{\mathcal{L}}$ associado aos divisores D e G é definido como a imagem da aplicação

$$f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n \,.$$

Teorema A.12. *Temos que $C_{\mathcal{L}}$ tem parâmetros $[n, k, d]$ tais que*

$$k = dim(\mathcal{G}) - dim\mathcal{L}(G - D)$$

$$d \geq n - deg(G) \quad (\textit{cota de Goppa}) \,.$$

Mais ainda, se $n > \deg G > 2g - 2$, então

$$k = \deg G + 1 - g \,.$$

Para mais propriedades dessa classe de códigos, nos referimos a [30].

REFERÊNCIAS BIBLIOGRÁFICAS

[1] S. Ball e J.W.P. Hirstchfeld, *Bounds on (n,r)-arcs and their application to linear codes*, Finite Fields Appl. **11** (2005) 326–336.

[2] H. Borges Filho, *On Complete (N,d)-Arcs derived from Plane Curves*, Finite Fields App. **15**(1) (2009), 82–96.

[3] H. Borges Filho, *On a generalization of the Hermitian curve*, work in progress.

[4] W. Bosma, J. Cannon e C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[5] S.V. Bulygin, *Generalized Hermitian codes over GF(2,r)*, IEEE Trans. Inform. Theory **52** (2006), 4664–4669.

[6] R.S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arithmetica **83** (1998), 241–251.

[7] R.S. Coulter, *Further evaluations of Weil sums*, Acta Arithmetica **86** (1998), 217–226.

[8] R.S. Coulter, *On the evaluation of a class of Weil sums in characteristic 2*, New Zealand J. Math. **28** (1999), 171–184.

[9] R.S. Coulter, *The number of rational points of a class of Artin-Schreier curves*, Finite Fields App. **8** (2002), 397–413.

[10] A. Garcia, *The curves $y^n = f(x)$ over finite fields*, Arch. Math. **74** (1990), no.1, 36–44.

[11] A. Garcia e L. Quoos, *A Construction of Curves over Finite Fields*, Acta Arithmetica **98** (2001), 181–195.

[12] A. Garcia e H. Sitchtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Inventiones Mathematicae **121** (1995), number 1, 211–222.

[13] A. Garcia e H. Sitchtenoth, *A class of polynomials over finite fields*, Finite Fields and Their Applications **5** (1999), 424–435.

[14] G. van der Geer e M. van der Vlut, *Fibre Products of Artin-Schreier Curves and Generalized Hamming Weights of Codes*, J. of Combinatorial Theory, Series A **70** (1995), 337–348.

[15] M. Giulietti, F. Pambianco, F. Torres and E. Ughi, *On complete arcs arising from plane curves*, Des. Codes Cryptogr. **25**(3) (2002), 237–246.

[16] A. Hefez and J.F. Voloch, *Frobenius nonclassical curves*, Arch. Math. **54** (1990), 263–273.

[17] J.W.P Hirstchfeld, G. Korchmaros e F. Torres, "Algebraic Curves Over a Finite Field", Princeton Series in Applied Mathematics, Princeton University Press (2008).

[18] J.W.P. Hirstchfeld e L. Storme, *The packing problem in statistics, coding theory and finite projective spaces*, J. of Statistical Planning and Inference *72* (1998), N^{os} 1-2, 355–380.

[19] J.W.P. Hirschfeld and J.F. Voloch, *The characterization of elliptic curves over finite fields*, J. Austral. Math. Soc. Ser. A **45** (1988), 275–286.

[20] J.W.P. Hirschfeld, "Projective Geometries over Finite Fields", second edition, Oxford University Press, Oxford (1998).

[21] Jungnickel, "Finite fields: structure and arithmetics", B.I. Wissenschaftsverlag (1993).

[22] A. Lauder e D. Wan, *Computing Zeta Functions of Artin-Schreier curves over finite fields*, LMS J. Comput. Math. **5** (2002), 34–55.

[23] J. Lewittes, *Places of degree one in function fields over finite fields*, J. Pure Appl. Algebra **69** (1990), 177–183.

[24] R. Lidl e H. Niederreiter, "Introduction to Finite Fields and their Applications", Cambridge University Press, 2 edition (1994).

[25] R. Lidl e H. Niederreiter, "Encyclopedia of mathematics and its applications 20: Finite Fields", second edition, Cambridge University Press (1997).

[26] C. Munuera, A. Sepúlveda e F. Torres, *Algebraic Geometry codes from Castle curves*, Lecture Notes in Comput. Sci. **5228** (2008), Springer-Verlag Berlin Heidelberg, 117–127.

[27] C. Munuera, A. Sepúlveda e F. Torres, *Generalized Hermitian codes*, preprint.

[28] M. Moisio e D. Wan, *On Katz's bound for the number of elements with given trace and norm*, J. Reine Angew. Math. **638** (2010) 69–74.

[29] A. Sepúlveda, *Sobre codigos hermitianos generalizados*, Tese de Doutorado, Instituto de Matemática, Estatística e Computação Científica, UNICAMP (2008)

[30] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag (1993).

[31] K.O. Stöhr e J.F. Voloch, *Weierstrass points and curves over Finite Fields*, Proc. London Math. Soc. *52* (1986), 1–19.

[32] F. Torres, *The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs: Expanded version of lectures given at Essen (April 1997) and Perugia (February 1998)*, Relatório de Pesquisa RP 40/00, IMECC-UNICAMP (2000). Disponível em `http://www.ime.unicamp.br/~ftorres/RESEARCH/ARTS_PDF/wp.pdf`

[33] J. Wolfmann, *The number of points on certain algebraic curves over Finite Fields*, Comm. Algebra **17** (1989), 2055–2060.