UM EXEMPLO DE CÓDIGOS DE GOPPA SUPORTADOS EM UM PONTO SOBRE UMA CURVA NÃO MAXIMAL *

J. BEZERRA **

L. QUOOS †

Resumo

Apresentamos aqui uma nova família de códigos de Goppa suportados num ponto ilustrando o teorema de Garcia-Kim-Lax [1]. Estes códigos são construídos sobre curvas não-maximais.

1 Introdução

Sejam q uma potência de um primo, $\mathbb{F}_q$ o corpo finito com q elementos e $\mathbb{F}_q^n$ o $\mathbb{F}_q$ -espaço vetorial formado pelas n -uplas de elementos de $\mathbb{F}_q$. Um *código linear* é um subespaço vetorial C de $\mathbb{F}_q^n$. O conjunto $\mathbb{F}_q$ é chamado de alfabeto, os elementos de $\mathbb{F}_q^n$ são chamados de palavras e o inteiro n é chamado o comprimento das palavras. Para um código C temos definida uma métrica, a distância de Hamming:

$$d(x, y) = \#\{i : 1 \leq i \leq n, x_i \neq y_i\},$$

onde $x = (x_1, \dots, x_n)$ e $y = (y_1, \dots, y_n) \in C$. O peso $w(x)$ de uma palavra x pertencente a C é a distância dela a origem, e o mínimo dessas distâncias é chamada *distância mínima* do código.

Um código $C \subset \mathbb{F}_q^n$ é chamado um $[n, k, d]$ -código se sua dimensão é k e a sua distância mínima é d . Um código com distância mínima d pode corrigir $\lfloor \frac{1}{2}(d-1) \rfloor$ erros. Para um $[n, k, d]$ -código C , define-se $R = R(C) = k/n$ a taxa de transmissão de C , e $\delta = \delta(C) = d/n$ a distância mínima relativa de C . Um problema central na Teoria de Códigos é a determinação de códigos longos (comprimento grande) com transmissão de informação segura, o que se traduz, em termos dos parâmetros relativos, na determinação de códigos longos que corrijam uma porcentagem fixa de erros por palavra e que tenham taxa de transmissão estritamente positiva.

Corpos de funções algébricas ou geometricamente falando, curvas algébricas projetivas irredutíveis e não-singulares, têm servido de inspiração para a teoria dos códigos na medida que melhoram a famosa cota de Gilbert-Varshmov [3], que mede o quanto os parâmetros de um código podem ser bons. Goppa usou o Teorema de Riemann-Roch, um teorema clássico da geometria algébrica, para mostrar que determinados códigos, produzidos a partir de dois divisores G e D sobre uma curva, têm bons parâmetros. Em [1], Garcia, Kim e Lax construíram códigos de Goppa considerando G um múltiplo especial de um ponto P , e mostraram que as lacunas em P podem originar códigos cuja distância mínima melhora a cota

**Palavras chave:* Curvas Algébricas, Corpos de funções Algébricas, Lacunas, Códigos Corretores de Erros, Códigos de Goppa

**Departamento de Análise Matemática, IME/UERJ, bezerra@ime.uerj.br

†Departamento de Matemática Pura, Instituto de Matemática, UFRJ, luciane@im.ufrj.br

inferior obtida por Goppa. Neste artigo, os autores ilustram o seu principal resultado com a construção de códigos de Goppa definidos sobre curvas maximais.

Neste trabalho apresentamos outra ilustração para o resultado de Garcia, Lax e Kim, construindo códigos de Goppa sobre uma família de curvas não maximais. Na seção 2 introduzimos os conceitos básicos de corpos de funções algébricas e formulamos os principais resultados necessários à nossa construção. Na seção 3 apresentamos a nova família de códigos de Goppa e calculamos o valor exato de seus parâmetros.

Observação 1.1 *Nós usamos como bibliografia fundamental o livro de Stichtenoth [3]. Todos os resultados da Teoria de corpos de funções algébricas e da teoria de códigos citados, com a única exceção do Teorema 2.2 [1], estão neste livro. Assim como também seguimos a sua notação.*

2 Preliminares

Um corpo de funções algébricas (de uma variável) sobre $\mathbb{F}_q$ é uma extensão finitamente gerada de corpos $F/\mathbb{F}_q$ com grau de transcendência 1, tal que $\mathbb{F}_q$ é algebricamente fechado em F . Para um corpo de funções $F/\mathbb{F}_q$ denotamos $N(F)$ o número de lugares de grau um de $F/\mathbb{F}_q$ e $g(F)$ o gênero de $F/\mathbb{F}_q$. Um corpo de funções é dito maximal se a cota de Weil é atingida, isto é, $N(F) = q + 1 + 2g\sqrt{q}$ [3].

Seja k o fecho algébrico de $\mathbb{F}_q$. Uma curva algébrica plana irredutível $\mathcal{X}$ sobre $\mathbb{F}_q$ é definida por um polinômio absolutamente irredutível $f(x, y)$ em $\mathbb{F}_q[x, y]$ como $\mathcal{X} = \{(a, b) \in k \times k \mid f(a, b) = 0\}$. Uma curva algébrica plana $\mathcal{X}$ está associada a um corpo de funções algébricas. Se $f(x, y) \in \mathbb{F}_q[x, y]$ é o polinômio irredutível que define $\mathcal{X}$, sejam A o anel residual de $\mathbb{F}_q[x, y]$ módulo $f(x, y)$ e F o corpo de frações de A , então F é o corpo de funções algébricas associado à $\mathcal{X}$. Quando $\mathcal{X}$ é não-singular, os pontos de $\mathcal{X}$ estão em correspondência biunívoca com os lugares de seu corpo de funções algébricas, e os lugares de grau um correspondem aos pontos $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$.

Seja $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero $g = g(F)$. Para um conjunto $D = \{P_1, \dots, P_n\}$ de n lugares de grau 1 distintos de $F/\mathbb{F}_q$, seja L um subespaço $\mathbb{F}_q$ -linear de F tal que nenhuma função $f \in L$ tenha pólo nos lugares P_i . A aplicação $\alpha : L \rightarrow \mathbb{F}_q^n$ definida por $\alpha(f) = (f(P_1), \dots, f(P_n))$ é $\mathbb{F}_q$ -linear e portanto sua imagem é um código. No caso em que L é um espaço de Riemann-Roch, isto é, $L = L(G) = \{f \in F : \text{div}(f) + G \geq 0\}$ para algum divisor G com suporte disjunto de D , a imagem de α é o que chamamos de código algébrico-geométrico ou código de Goppa, e é denotada por $C_L(D, G)$. Uma outra maneira de construirmos um código de Goppa C é utilizando $\Omega(D)$, o espaço de diferenciais holomorfas do divisor D . Neste caso $C = C_\Omega(D, G)$ é a imagem da aplicação $\mathbb{F}_q$ -linear $\Omega(G - D) \rightarrow \mathbb{F}_q^n$ definida por

$$\eta \rightarrow (\text{res}_{P_1}\eta, \dots, \text{res}_{P_n}\eta) \in \mathbb{F}_q^n.$$

Como consequência do Teorema de Riemann-Roch temos:

Teorema 2.1 *O código $C_\Omega(D, G)$ é um $[n, k, d]$ -código com parâmetros:*

- (1) $d \geq \text{grau } G - (2g - 2)$.
- (2) Se $\text{grau } G > 2g - 2$, então $k \geq n + g - 1 - \text{grau } G$.
- (2) Se $2g - 2 < \text{grau } G < n$, então $k = n + g - 1 - \text{grau } G$.

Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g e P um lugar de $F/\mathbb{F}_q$. Uma lacuna de Weierstrass em P é um inteiro não negativo l tal que não existe função $x \in F$ com um único pólo em P de multiplicidade l . Seqüências de lacunas de Weierstrass ajudam a melhorar a cota inferior para d dada no item (1) do Teorema 2.1, conforme o seguinte resultado de Garcia, Kim e Lax [1]:

Teorema 2.2 *Sejam $\alpha, \alpha + 1, \dots, \alpha + t, \beta - (t - 1), \dots, \beta - 1, \beta$ lacunas em P , com $\alpha + t \leq \beta$ e $t \geq 1$. Sejam $G = (\alpha + \beta - 1)P$ e $D = P_1 + P_2 + \dots + P_n$, onde os P_i 's são pontos racionais. Suponha que $\text{sup } G \cap \text{sup } D = \emptyset$. Se o código $C_\Omega(G, D)$ tem dimensão positiva, então a sua distância mínima d satisfaz, $d \geq \text{grau } G - (2g - 2) + (t + 1)$.*

Note que a cota inferior para a distância mínima obtida pelo Teorema 2.2 melhora em $t + 1$ unidades a cota do Teorema 2.1. Em [1], os autores finalizam o trabalho ilustrando o teorema 2.2 com a construção de um $[n, k, d]$ código de Goppa, $C_\Omega(G, D)$, sobre a curva maximal definida pela equação $y^q + y = x^m$ sobre $\mathbb{F}_{q^2}$, onde $m > 2$ divide $q + 1$. Neste exemplo eles determinam o valor exato de d .

3 Resultado principal

Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g e P um lugar de grau um. Vamos aplicar o Teorema 2.2 no caso $t = 1$ e a maior lacuna em P é $\beta = 2g - 1$ (semigrupo de Weierstrass em P simétrico). Esta é uma maneira de forçarmos a desigualdade $\text{grau } G > 2g - 2$ e obtermos o valor exato da dimensão do código.

Teorema 3.1 *Sejam q uma potência de dois, $\mathcal{X}$ a curva definida sobre $\mathbb{F}_q$ pela equação afim*

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

e $F\mathbb{F}_q/F_q$ o corpo de funções definido por $\mathcal{X}$. Suponha que o gênero de $\mathcal{X}$ é maior do que 2, então existe um código de Goppa suportado num ponto sobre $\mathcal{X}$ com os seguintes parâmetros:

$$[n, k, d] = [n, n - q(q - 2)/2 - b(q - 1) + 3, b(q - 1)]$$

para cada $0 < b \leq \frac{q}{2} - 1$ com $b(q - 1) + 2g - 4 \leq n \leq (q - 1)q$.

Demonstração 3.1 *Todos os zeros de $x^l - x^r + 1$ e pólos de x são totalmente ramificados na extensão de Kummer $\mathbb{F}_q(x, y)|\mathbb{F}_q(x)$ definida pela curva $\mathcal{X}$. Aplicando a fórmula de Riemann-Hurwitz a extens de corpos $\mathbb{F}_q(x, y)|\mathbb{F}_q(x)$, determinamos $g = q(q - 2)/2$, o gênero de $\mathcal{X}$.*

O pólo de x é totalmente ramificado e todos os elementos em $\mathbb{F}_q$ se decompõem totalmente na extensão $\mathbb{F}_q(x, y)|\mathbb{F}_q(x)$. Note que se γ pertence a $\mathbb{F}_q$, então $\gamma^l - \gamma^r + 1 = 1$. Portanto o número N de lugares racionais de $\mathcal{X}$ é $N = q(q - 1) + 1$.

Seja P_∞ o único pólo de x na extensão $\mathbb{F}_q(x, y) | \mathbb{F}_q(x)$. Os divisores de pólos de x e y são dados por $(x)_\infty = (q-1)P_\infty$ e $(y)_\infty = (q+1)P_\infty$. O número de não-lacunas no intervalo $[0, 2g-1]$ definidas como $i(q+1) + j(q-1)$ para $(i, j) \in \mathbb{N} \times \mathbb{N}$ é $g-1$. De fato: para cada inteiro i , $0 \leq i \leq q-3$ temos $0 \leq j \leq q - \lceil (i(q+1) + q + 1)/(q-1) \rceil = q + \lfloor -((q+1) - i(q+1))/(q-1) \rfloor$. Assim

$$\begin{aligned} \#\{(i, j) \mid i(q+1) + j(q-1) \leq 2g-1, i \geq 0, j \geq 0, ij \neq 0\} &= \\ &= q - \lceil \frac{q+1}{q-1} \rceil + \sum_{i=1}^{q-3} \left(q + 1 + \left\lfloor \frac{-i(q+1) - (q+1)}{q-1} \right\rfloor \right) = \\ &= q + (q-3)(q+1) + \frac{(q-2)(-q-2)}{2} = g-1. \end{aligned}$$

Onde $\lfloor t \rfloor$ é o maior inteiro menor ou igual a t e $\lceil t \rceil$ é o menor inteiro maior ou igual a t . Na última igualdade estamos usando resultados sobre somatórios destas funções conforme [2].

Desta forma obtemos o semigrupo simétrico de Weierstrass em P_∞ como sendo o conjunto $[0, 2g-1] \setminus \{(i, j) \mid i(q+1) + j(q-1) \leq 2g-1, i \geq 0, j \geq 0, ij \neq 0\}$. Seja $\beta = 2g-1$ a maior lacuna no infinito. O objetivo é acharmos outra lacuna α tal que:

- $\alpha = b(q-1) - 2$, onde $b \in \mathbb{N}^*$ e
- $\alpha + 1$ é também uma lacuna.

O elemento $\alpha = b(q-1) - 2$ é uma não-lacuna no infinito se, e somente se, existem $i, j > 0$ tais que $b(q-1) - 2 = i(q+1) + j(q-1)$, o que significa $i = -1 + (q-1)t$ e $b-j = -1 + (q+1)t$, $t \in \mathbb{Z}$. Considerando ambas as condições, $b-j \geq 0$ e $i \geq 0$ concluímos que:

$$t \geq \max\left\{ \left\lceil \frac{1}{q+1} \right\rceil, \left\lceil \frac{1}{q-1} \right\rceil \right\} = \left\lceil \frac{1}{q-1} \right\rceil = 0$$

A condição $t \geq 1$ implica $b-j \geq -1 + q-1 = q-2$. Assim, para todo $b < q-2$, temos que α é uma lacuna em P_∞ . Analogamente, se $b \leq \frac{q}{2}$, $\alpha + 1$ é uma lacuna em P_∞ .

Agora estamos prontos para construir códigos de Goppa C sobre a curva $\mathcal{X}$ suportado no ponto P_∞ . Para β e α como acima sejam:

$$G = (\alpha + \beta - 1)P_\infty \text{ e } D = \sum_{P \in J} P - P_\infty,$$

onde $J = \{P \in \mathcal{X} \mid \text{grau } P = 1\}$ e $\#J = n$. Para $b(q-1) + 2g - 4 \leq n \leq (q-1)q$, os parâmetros do código $C = C_\Omega(D, G)$ satisfazem:

$$k = n + g - 1 - \text{deg } G \text{ e } d \geq \text{grau } G - (2g - 2) + 2 = b(q-1).$$

Para concluirmos a demonstração devemos mostrar que a distância mínima é atingida. Consideremos a diferencial:

$$\omega = \frac{dx}{\prod_{\gamma \in I} (x - \gamma)y^{q-2}}, \text{ onde } I \subset \{x(P) \mid P \in J\} \text{ e } \#I = b$$

O divisor de ω é $(\omega) = [(b + q + 1)(q - 1) - (q + 1) - q]P_\infty - \sum_{i=1}^{q-1} P_{\gamma,i}$, onde $P_{\gamma,i}$, $1 \leq i \leq q - 1$ denota os lugares racionais sobre $x - \gamma$. Esta diferencial tem exatamente $b(q - 1)$ pólos de ordem um, e é fácil ver que ω pertence ao espaço $\Omega(G - D)$. $\square$

Referências

- [1] A. GARCIA, S. J. KIM and R. F. LAX, *Consecutive Weierstrass gaps and minimum distance of Goppa Codes*, J. of Pure and Applied Algebra **84** (1993), 199–207.
- [2] D. E. KNUTH, O. PATASHNIK and R. L. GRAHAM, *Concrete mathematics: a foundation for computer science*, Addison-Wesley, c1994.
- [3] H. STICHTENOTH: “Algebraic Function Fields and Codes”. Springer Universitext, Springer-Verlag, Berlin-Heidelberg, 1993.