Os Códigos Controle da Paridade $CP_q(n)$ obtidos por restrição de um Código de Goppa Racional

Jaime Edmundo Apaza Rodriguez *
Departamento de Matemática, UNESP, Ilha Solteira

18 de outubro de 2012

Resumo

Os Códigos Controle da Paridade surgiram como um exemplo de uma família de códigos detectores de um erro simples. Seu nome provêm de um código binário que acrescentava um símbolo extra para que o número de 1's fosse par. Em 1977, *V. D. Goppa* introduziu uma nova forma de construir códigos lineares usando curvas algébricas definidas sobre corpos finitos. Esses códigos são chamados de Códigos Geometricos de Goppa. Neste trabalho usamos algumas das idéias de Goppa para construir uma certa classe de Códigos de Controle da Paridade $CP_q(n)$ sobre o corpo $\mathbb{F}_q$. Construimos o Código de Controle da Paridade $CP_q(n)$ como restrição de um Código de Goppa Racional. No processo de construção são considerados dois casos, dependendo de se o comprimento n do código é divisível ou não pela característica do corpo finito $\mathbb{F}_q$.

Palavras Chave: Códigos Lineares, Corpo Finito, Curva Algébrica não-singular, Códigos Geométricos de Goppa, Teorema de Riemann-Roch.

1 Introdução

Os Códigos Controle da Paridade surgiram no século passado como exemplo de uma família de códigos detectores de um erro simples. Seu nome provêm de um código binário que acrescentava um símbolo extra para que o número de 1's fosse par.

Os Códigos Controle da Paridade são utilizados pelo fato de usar um número mínimo de símbolos de redundância, o que reduz custos de implementação e decodificação em sistemas de erro simples.

Os códigos de Goppa ilustram uma construção prática para famílias de bons códigos que ultrapassam determinadas cotas assintóticas conhecidas, mostrando ser uma boa alternativa no futuro das comunicações moveis.

O processo de construção dos Códigos de Controle da Paridade $CP_q(n)$, usando Códigos de Goppa, permite colocar esta importante classe de códigos algébricos clássicos no contexto da teoria moderna de códigos, pois eles tem se mostrado ser eficientes.

A Teoria de Códigos Detectores e Corretores de Erros teve suas origens em 1948 com os trabalhos de *C. E. Shannon, R. Hamming, M. Golay* e outros. No início estes códigos foram criados usando unicamente conceitos da Álgebra e Teoria dos

*Email: jaime@mat.feis.unesp.br

Números. Posteriormente, em 1977, *V. D. Goppa* introduziu uma nova forma de construir códigos lineares usando Curvas Algébricas definidas sobre corpos finitos, hoje conhecidos como os *Códigos Geometricos de Goppa.*

Neste trabalho usamos algumas das idéias de Goppa para construir os Códigos de Controle da Paridade $CP_q(n)$, usando a técnica de restrição de um código linear (Código de Goppa Racional). Em geral, se C é um código linear definido sobre um corpo finito $\mathbb{F}_q$, a restrição de C a $\mathbb{F}_q$ é dada por $C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$. Apresentamos aqui dois casos concretos e exibimos um exemplo em cada caso.

2 Códigos de Goppa

Faremos um breve resumo de conceitos e resultados sobre Curvas Algébricas e Corpos de Funções Algébricas. Neste contexto apresentamos um clássico resultado da Geometria Algébrica, o *Teorema de Riemann-Roch*, o qual permite estimar os parâmetros para os Códigos de Goppa.

Seja F um corpo extensão de um corpo K e se denota por F/K. A *Teoria de Corpos de Funções Algébricas* garante que se F/K é um corpo de funções de uma variável, então existe uma curva projetiva não-singular X (única salvo isomorfismo) cujo corpo de funções $K(X)$ é isomorfo a F. Este isomorfismo permite "traduzir" definições e resultados dos corpos de funções algébricas para curvas algébricas e vice-versa.

Agora, considere uma curva algébrica não-singular X, definida sobre o corpo finito $\mathbb{F}_q$ e seja $F(X)$ seu corpo de funções (sobre $\mathbb{F}_q$) associado. Sejam $P_1, \cdots, P_n$ lugares distintos de grau 1 em $F/\mathbb{F}_q$ (equivalentemente, $P_1, \cdots, P_n$ pontos racionais da curva). Considere o divisor (soma formal de lugares ou pontos da curva)

$$D = \sum_{i=1}^{n} P_i$$

e seja G qualquer outro divisor de $F/\mathbb{F}_q$ tal que $P_i \notin supp(G)$, para todo $i = 1, \cdots, n$ (ou seja $supp(G) \cap supp(D) = \emptyset$). O código geométrico de Goppa, associado aos divisores D e G, está definido por

$$C_{\mathcal{L}}(D, G) = \{(x(P_1), \cdots, x(P_n)) : x \in \mathcal{L}(G)\} \subseteq F_q^n,$$

sendo $\mathcal{L}(G)$ um espaço vetorial (espaço de funções algébricas) dado por

$$\mathcal{L}(G) = \{x \in F/\mathbb{F}_q - \{0\} : div(x) + G \geq 0\} \cup \{0\},$$

onde $div(x)$ é o divisor (principal) associado à função (algébrica) x. O espaço $\mathcal{L}(G)$ é finito dimensional sobre $\mathbb{F}_q$ e a sua dimensão denota-se por $\ell(G)$. Por definição temos que $dim(G) = dim\ \mathcal{L}(G)$.

Observação 2.1 *Para um lugar P de grau 1 e um elemento $x \in F$, com $v_P(x) \geq 0$, temos que $x(P)$ é o valor de x em P (ou seja, $x(P) \in \mathbb{F}_q$ e $v_P(x - x(P)) > 0$). v_P é dita a valoração de F no lugar P.*

Considerando a aplicação

$$\phi : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n, \quad \text{dada por} \quad \phi(x) = (x(P_1), x(P_2), \cdots, x(P_n)),$$

observamos que a imagem de ϕ é um subespaço vetorial de $\mathbb{F}_q^n$. Este subespaço é precisamente o *Código Geométrico de Goppa.* Dado que a aplicação ϕ é $\mathbb{F}_q$-linear e $C_{\mathcal{L}}(D, G) = \phi(\mathcal{L}(G))$, temos que $C_{\mathcal{L}}(D, G)$ é um q-ário código linear.

Um importante resultado da Geometria Algébrica é o *Teorema de Riemann-Roch*, que apresentamos a seguir para o caso específico do corpo de funções $F/\mathbb{F}_q$.

W é dito divisor canônico se $deg(W) = 2g - 2$ e $dim(W) = dim\ \mathcal{L}(W) = g$, onde g é o gênero do corpo $F/\mathbb{F}_q$ (o gênero g é um invariante do corpo de funções $F/\mathbb{F}_q$ ou da curva algébrica associada X).

Teorema 2.1 *(Riemann-Roch) Seja W um divisor canônico de $F/\mathbb{F}_q$. Então, para qualquer divisor A, temos que*

$$dim(A) = deg(A) + 1 - g + dim(W - A).$$

Pelo teorema de *Riemann-Roch*, para o divisor G da definição de Código Geométrico de Goppa temos

$$\ell(G) \geq deg(G) + 1 - g,$$

e a igualdade vale se $deg(G) \geq 2g - 1$.

O teorema de *Riemann-Roch* permite estimar os parâmetros para os Códigos Geométricos de Goppa.

Teorema 2.2 *Sejam $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero g, e $D \subset F(\mathbb{F}_q)$ ($F(\mathbb{F}_q)$ é o conjunto de lugares de grau 1), com $|D| = n$ (cardinalidade de D). Seja G um divisor com $g \leq deg(G) < n$ e $supp(G) \cap D = \emptyset$. Então $C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$-código linear sobre $\mathbb{F}_q$ satisfazendo:*

$$k \geq deg(G) - g + 1, \qquad d \geq n - deg(G).$$

Mais ainda, se $deg(G) \geq 2g - 1$, então $k = deg(G) - g + 1$.

Se n é muito mais grande do que $deg(G)$, então ϕ é um mergulho em $\mathbb{F}_q^n$ e a dimensão k de $C_{\mathcal{L}}(D, G)$ é igual a $\ell(G)$.

Um código de Goppa associado aos divisores do corpo de funções algébricas $\mathbb{F}_q(z)/\mathbb{F}_q$ é chamado de *Código de Goppa Racional*, onde z é um elemento transcendente de $\mathbb{F}_q$. De maneira mais formal, considere um divisor $D = P_1 + P_2 + \cdots + P_n$, onde os P_i são lugares de grau 1 (pontos racionais da curva correspondente), e um outro divisor E, de grau positivo, tal que $supp(E) \cap supp(D) = \emptyset$. Seja f uma função racional no corpo das funções racionais $\mathbb{F}_q(z)$. Para cada $f \in \mathcal{L}(E) - \{0\}$ temos que $f(P_i)$ esta bem definido e é um elemento do corpo $\mathbb{F}_q$.

Por meio do divisor D, a função avaliação $\phi : \mathcal{L}(E) \longrightarrow \mathbb{F}_q$, dada por $\phi(f) = (f(P_1), \cdots, f(P_n))$, é linear sobre $\mathbb{F}_q$ e sua imagem é o subespaço linear de $\mathbb{F}_q^n$, dado por

$$C(D, E) = \{(f(P_1), \cdots, f(P_n)) : f \in \mathcal{L}(E)\}.$$

Portanto, $C(D, E)$ é um código linear, chamado *Código de Goppa Racional* associado aos divisores D e E.

Os Códigos de Goppa (clássicos) foram introduzidos por meio de relações polinomiais, generalizando os *Códigos BCH* (*Bose-Chauhuri-Hocquenghem*) (códigos cíclicos junto a um conjunto conveniente de raízes n-ésimas da unidade e com uma cota inferior mínima).

3 Códigos Controle da Paridade

Um código linear C é um subespaço vetorial do espaço $\mathbb{K}^n$, sendo $\mathbb{K} = \mathbb{F}_q$ um corpo finito de cardinalidade q e $n \in \mathbb{N}$. Consideremos o corpo finito $\mathbb{F}_q$ como sendo o alfabeto do código C.

Todo código linear C possui três parâmetros fundamentais, n, m *e* d, sendo n seu comprimento, m sua dimensão e d sua distância mínima. Assim, dizemos que C é um $[n, m, d]$-código.

O Código de Controle da Paridade, $CP_q(n)$ é um subespaço vetorial de $\mathbb{F}_q^n$, obtido ao acrescentar a cada elemento do espaço $\mathbb{F}_q^{n-1}$ uma última componente, de modo que a soma de todas as entradas seja zero em $\mathbb{F}_q$. Formalmente, $CP_q(n)$ é dado por

$$CP_q(n) = \{(c_1, \cdots, c_n) : (c_1, \cdots, c_{n-1}) \in \mathbb{F}_q^{n-1}, \ \sum_{i=1}^{n} c_i = 0\},$$

e é um $[n, n-1, 2]$-código q-ario. Isto significa que $CP_q(n)$ é um código de comprimento n, dimensão $n-1$ e distância mínima 2 e, portanto, trata-se de um código detector de um erro simples.

O Código de Controle da Paridade $CP_q(n)$ será obtido como a restrição de um Código de Goppa Racional. Serão considerados dois casos, dependendo de se o comprimento n do código é divisível ou não pela característica do corpo finito $\mathbb{F}_q$.

Teorema 3.1 *Se* $char(\mathbb{F}_q) \nmid n$, *então* $C_{\mathcal{L}}(D, G)|_{\mathbb{F}_q} = CP_q(n)$.

Prova: Seja m um inteiro tal que $n|q^{m-1}$ e seja $\beta \in \mathbb{F}_{q^m}$ uma n-ésima raiz primitiva da unidade. Consideremos o corpo de funções racionais $\mathbb{F}_{q^m}(z)/\mathbb{F}_{q^m}$ e denotemos por P_i os zeros da função $z - \beta^{i-1}$, para $i = 1, \cdots, n$. Também consideremos os divisores

$$G = (n-1)P_\infty - P_0 \quad e \quad D = \sum_{i=1}^{n} P_i,$$

onde P_0 é o lugar zero e P_∞ o lugar infinito de z em $\mathbb{F}_{q^m}(z)/\mathbb{F}_{q^m}$.

Dado que $deg(G) = n-2$, o *Teorema de Riemann-Roch* garante que $dim(G) = n-1$. Assim o conjunto $\{z, z^2, \cdots, z^{n-1}\}$ é uma base para o espaço $\mathcal{L}(G)$. Agora considere a aplicação avaliação ϕ da seção anterior. Para cada $j = 1, \cdots, n-1$, temos que

$$\phi(z^j) = (1, \beta^j, \cdots, (\beta^{n-1})^j),$$

e como β é uma n-ésima raiz primitiva da unidade, obtemos

$$\sum_{i=0}^{n-1} (\beta^i)^j = 0,$$

ou seja, a soma das componentes é igual a zero em $\mathbb{F}_q$. Logo, todo elemento $x \in \mathcal{L}(G)$ é da forma

$$x = \sum_{k=1}^{n-1} a_k z^k,$$

com $a_k \in \mathbb{F}_{q^m}$, para $k = 1, \cdots, n-1$. Portanto

$$\begin{aligned}\phi(x) &= (x(P_1), x(P_2), \cdots, x(P_n)) \\ &= \left(\sum_{k=1}^{n-1} a_k z^k(P_1),\ \sum_{k=1}^{n-1} a_k z^k(P_2), \cdots,\ \sum_{k=1}^{n-1} a_k z^k(P_n)\right) \\ &= \left(\sum_{k=1}^{n-1} a_k,\ \sum_{k=1}^{n-1} a_k \beta^k, \cdots, \sum_{k=1}^{n-1} a_k (\beta^{n-1})^k\right).\end{aligned}$$

Em consequência temos que $C_{\mathcal{L}}(D, G) = CP_{q^m}(n)$, pois

$$\sum_{k=1}^{n-1} a_k + \cdots + \sum_{k=1}^{n-1} a_k (\beta^{n-1})^k = \sum_{k=1}^{n-1} a_k \Big(\sum_{i=0}^{n-1} (\beta^i)^k\Big) = 0,$$

e os vetores $v_j = (1, \beta^j, \cdots, (\beta^{n-2})^j)$, para $j = 1, 2, \cdots, n$, formam uma base para o espaço $\mathbb{F}_{q^m}^{n-1}$. Assim resulta que

$$C_{\mathcal{L}}(D, G)|_{\mathbb{F}_q} = CP_q(n).$$

Teorema 3.2 *Se char($\mathbb{F}_q$)$|n$, então $C_{\mathcal{L}}(D, G)|_{\mathbb{F}_q} = CP_q(n)$.*

Prova: De maneira similar, seja m um inteiro tal que $(n-1)|q^{m-1}$ e $\beta \in \mathbb{F}_{q^m}$ uma $(n-1)$-ésima raiz primitiva da unidade. Considere o corpo de funções racionais $\mathbb{F}_{q^m}(z)/\mathbb{F}_{q^m}$ e denotemos por P_i os zeros da função $z - \beta^{i-1}$, para $i = 1, \cdots, n-1$ e por $P_n := P_0$ o zero de z.

Consideremos os divisores

$$G = (n-2)P_\infty \quad e \quad D = \sum_{i=1}^{n-1} P_i,$$

no corpo de funções racionais $\mathbb{F}_{q^m}(z)/\mathbb{F}_{q^m}$, como no caso 1.

Como $deg(G) = n-2$, então $dim(G) = n-1$, e portanto o conjunto $\{1, z, z^2, \cdots, z^{n-2}\}$ é uma base para o espaço $\mathcal{L}(G)$. Alem disso, temos que

$$\phi(1) = (1, 1, \cdots, 1) \quad e \quad \phi(z^j) = (1, \beta^j, \cdots, (\beta^{n-2})^j, 0).$$

Então é claro que a soma das componentes de $\phi(1)$ e $\phi(z^j)$, para $j = 1, 2, \cdots, n-2$, é igual a zero em $\mathbb{F}_q$. Desta forma, como no caso anterior, obtemos

$$C_{\mathcal{L}}(D, G)|_{\mathbb{F}_q} = CP_q(n).$$

4 Aplicações

1) O código $CP_2(3)$:

Dado que $2 \nmid 3$, seja $\beta \in \mathbb{F}_4$ uma raiz primitiva terceira da unidade. Considere o corpo de funções racionais $\mathbb{F}_4(z)/\mathbb{F}_4$. Dado que $\mathbb{F}_4 = \{0, 1, \beta, \beta^2\}$, denotemos

os lugares de grau 1, em $\mathbb{F}_4(z)/\mathbb{F}_4$, por $P_0, P_1, P_\beta, P_{\beta^2}$ *e* P_∞. Agora considere os divisores

$$D = P_1 + P_\beta + P_{\beta^2} \quad e \quad G = 2P_\infty - P_0,$$

em $\mathbb{F}_4(z)/\mathbb{F}_4$. Assim temos que $\{z, z^2\}$ é uma base para o espaço $\mathcal{L}(G)$. Segue que, dos 16 elementos de $\mathcal{L}(G)$, os únicos cuja imagem a respeito de ϕ estão em $\mathbb{F}_2^3$ são

$$\{0,\ z + z^2,\ \beta z + \beta^2 z^2,\ \beta^2 z + \beta z^2\}.$$

Desta forma, sua imagem é exatamente $\{(0,0,0),(0,1,1),(1,1,0),(1,0,1)\}$. Assim obtemos que

$$C_{\mathcal{L}}(D,G)|_{\mathbb{F}_2} = CP_2(3).$$

2) O código $CP_2(4)$:

Dado que $2|4$, considere $\beta \in \mathbb{F}_4$ e o corpo de funções racionais $\mathbb{F}_4(z)/\mathbb{F}_4$, como no caso anterior. Agora considere os divisores

$$D = P_1 + P_\beta + P_{\beta^2} + P_0 \quad e \quad G = 2P_\infty,$$

em $\mathbb{F}_4(z)/\mathbb{F}_4$. Assim temos que $\{1, z, z^2\}$ é uma base para o espaço $\mathcal{L}(G)$. Segue que os únicos elementos, cuja imagem a respeito de ϕ estão em $\mathbb{F}_2^4$ e suas respectivas imagens, são:

0	(0,0,0,0)
1	(1,1,1,1)
$z + z^2$	(0,1,1,0)
$\beta z + \beta^2 z^2$	(1,1,0,0)
$\beta^2 z + \beta z^2$	(1,0,1,0)
$z + z^2 + 1$	(1,0,0,1)
$\beta z + \beta^2 z^2 + 1$	(0,0,1,1)
$\beta^2 z + \beta z^2 + 1$	(0,1,0,1)

Obtemos assim $C_{\mathcal{L}}(D,G)|_{\mathbb{F}_2} = CP_2(4)$.

Referências

[1] *H. Stichtenoth*; Algebraic Function Field and Codes, Springer-Verlag, Berlin-Heidelberg, 1993.

[2] *V. D. Goppa*; Geometry and Codes, Kluwer Academic Publisher, Boston 1988.

[3] *J. Van Lint*; Introduction to Coding Theory, Second edition, Springer-Verlag, 1992.

[4] *A. Hefez e M. L. T. Vilela*; Códigos Corretores de Erros, Série de Computação e Matemática, IMPA, Rio de Janeiro, 2002.

[5] *S. Roman*; Coding and Information Theory, Springer-Verlag, N.Y., 1991.