Códigos de Controle da Paridade via Códigos de Goppa

Jaime Edmundo Apaza Rodriguez **Edson Donizete de Carvalho**

Departamento de Matemática, FEIS, UNESP
15385-000, Ilha Solteira, SP
E-mail: jaime@mat.feis.unesp.br edson@mat.feis.unesp.br

Resumo: *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. Inicialmente, os códigos detectores e corretores de erros foram criados usando unicamente conceitos de àlgebra e teoria dos números. Posteriormente, em 1977, V. D. Goppa introduziu uma nova forma de construir códigos lineares usando curvas algébricas definidas sobre corpos finitos, conhecidos como os Códigos Geometricos de Goppa. Neste trabalho usamos as idéias de Goppa para construir os códigos controle da paridade, usando a técnica de restrição de um código linear.*

Palavras-chave: *alfabeto, corpo finito, curva algébrica, corpo de funções racionais, 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 amplamente 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, embora esteja se a procura de "bons" códigos, cuja existência é garantida pela *Teoria de Shannon*, desde outras perspectivas, como as probabilísticas, as algebrico-geométricas, etc. Sem dúvida alguma, esta alternativa de construção permite compreender a implementação dos códigos geométricos de Goppa, gerando códigos comumente utilizados e confiáveis em problemas de comunicação através de canais do tipo AWGN (*Additive White Gaussian Noise*). Tais canais são caracterizados pelo tipo de ruído responsável por degradar a comunicação a ser um ruído branco adicionado ao sinal.

A comunicação móvel é aquela onde existe a possibilidade de movimento relativo entre partes ou as partes sistêmicas envolvidas. Como exemplo tem-se a comunicação entre aeronaves, entre aeronaves e uma base terrestre, entre veículos, a telefonia celular, a computação móvel, algumas classes de sistemas de telemetria, etc. Uma comunicação fixa (por exemplo um link de microondas entre uma estação rádio base e uma central de comutação e controle de um sistema de telefonia celular) não caracteriza uma comunicação móvel, mas pode fazer parte de um sistema de comunicação móvel. Vários exemplos dessa natureza podem ser encontrados na prática.

Os canais associados a sistemas de comunicação móvel podem ser agrupados em dois tipos: canal via satélite e canal terrestre. O canal de comunicação via satélite é um canal do tipo AWGN, onde predominam fortes atenuações e muitas vezes grandes atrasos de propagação do sinal.

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

O processo de construção de códigos de controle da paridade, usando Códigos de Goppa, permite colocar este importante código algébrico clássico no contexto da teoria moderna de códigos, pois os códigos de Goppa tem mostrado ser mais 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 de àlgebra e teoria dos números. Posteriormente, em 1977, *V. D. Goppa* introduziu uma nova forma de construir códigos lineares usando curvas algébricas definidas sobre corpos finitos, conhecidos como os Códigos Geometricos de Goppa.

Neste trabalho usamos as idéias de Goppa para construir os códigos controle da paridade, usando a técnica de restrição de um código linear.

2 Preliminares

Consideremos o corpo finito $\mathbb{F}_q$ como sendo o alfabeto de um código C. O Código 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 $\mathbb{F}_q$. Mais precisamente, $CP_q(n)$ é um $[n, n-1, 2]$-código q-ario, dado por

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

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.

Agora, considere o corpo de funções $F/\mathbb{F}_q$ associado a uma curva algébrica X, não-singular, definida sobre o corpo finito $\mathbb{F}_q$. Sejam $P_1, \cdots, P_n$ lugares distintos de grau 1 em $F/\mathbb{F}_q$. Considere o divisor

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

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 como

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

onde $\mathcal{L}(G)$ é um espaço vetorial definido por

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

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.*

Um clássico e 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).

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 acima, temos

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

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

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 então que a imagem de ϕ forma um subespaço vetorial de $\mathbb{F}_q^n$. Este subespaço é precisamente o *Código Geométrico de Goppa*.

Dado que a aplicação ϕ acima definida 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.

O teorema de *Riemann-Roch* permite estimar os parâmetros para estes códigos.

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 geométrico de Goppa associado aos divisores do corpo de funções $\mathbb{F}_q(z)/\mathbb{F}_q$ é chamado de Código Geométrico de Goppa racional, onde z é um elemento transcendente de $\mathbb{F}_q$.

3 Resultados

Construiremos o código $CP_q(n)$ como a restrição de um código geométrico de Goppa racional. Para isso vamos considerar dois casos, dependendo de se o comprimento n do código é divisível ou não pela característica do corpo (alfabeto) $\mathbb{F}_q$.

Caso 1: $\text{char}(\mathbb{F}_q) \nmid n$:

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

Consideremos os divisores

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

no corpo de funções $\mathbb{F}_{q^m}(z)/\mathbb{F}_{q^m}$, 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 $\mathcal{L}(G)$.

Considere agora a aplicação avaliação ϕ. Temos que $\phi(z^j) = (1, \beta^j, \cdots, (\beta^{n-1})^j)$ e como β 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. Logo, se $x \in \mathcal{L}(G)$, então x 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

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

Assim resulta, finalmente, que

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

Caso 2: $\mathrm{char}(\mathbb{F}_q)|n$:

Neste caso, 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. Consideremos o corpo de funções racionais $\mathbb{F}_{q^m}(z)/\mathbb{F}_{q^m}$ e denotemos por P_i o zero da função $z - \beta^{i-1}$, para $i = 1, \cdots, n-1$ e $P_n := P_0$ o zero de z.

Consideremos os divisores

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

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

Como $deg(G) = n-2$, então $dim(G) = n-1$ onde o conjunto $\{1, z, z^2, \cdots, z^{n-2}\}$ é uma base para o espaço $\mathcal{L}(G)$. Assim $\phi(1) = (1, 1, \cdots, 1)$ e

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

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. Desta forma, como no caso anterior, obtemos

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

4 Exemplos

1) O código $CP_2(3)$

Dado que $2 \nmid 3$, seja $\beta \in \mathbb{F}_4$ uma terceira raiz primitiva 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 $P_0, P_1, P_\beta, P_{\beta^2}, P_\infty$. 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, a imagem é exatamente $\{(0,0,0), (0,1,1), (1,1,0), (1,0,1)\}$. Assim

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

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

Observação 4.1 *Todo código cíclico pode ser definido por determinadas condições de anulamento. Isto conduz a uma classe importante de códigos: os códigos BCH (Bose-Chaudhuri-Hocquenghem). Assim, os códigos BCH são códigos cíclicos construídos a partir de um adequado conjunto de raízes n-ésimas da unidade, fornecendo uma cota inferior para sua distância mínima.*

Os códigos de Goppa (clássicos) foram introduzidos por meio de certas relações polinomiais, generalizando assim os códigos BCH. Esta classe de códigos podem ser apresentados desde um outro ponto de vista, ilustrando um caminho para um processo de construção mais geral dos códigos algébrico-geometricos de Goppa. Tal processo de construção requer conhecimentos sólidos sobre curvas algébricas, um assunto enquadrado dentro da chamada Geometria Algébrica. Para o caso de curvas algébricas não-singulares, existe uma correspondência (isomorfismo) com um corpo de funções algébricas. Isto significa que a todo corpo de funções algébricas esta associado uma (única, salvo isomorfismo) curva algébrica projetiva não-singular (veja-se [1]).

Referências

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

[2] *V. D. Goppa*; Codes on Algebraic Curves, Soviet. Math. Dokl., Vol. 24, N. 1, 170-172, 1981.

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

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

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

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

[7] *C. E. Shannon*; A Mathematical Theory of Communication, Bell System Technical Journal, vol. 27, pp. 379-423, 623-656, 1948.