Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos Espaço Temporais Provenientes de Álgebras Cíclicas

Fabiana Aucco Egidio[1]
UNESP, Ilha Solteira, SP
Edson Donizete de Carvaho[2]
Departamento de Matemática, UNESP, Ilha Solteira, SP

Em canais de comunicação sem fio a propagação do sinal é realizada por meio de vários caminhos, resultando em perdas de percurso e alterações na amplitude do sinal, comportamento conhecido como *desvanecimento*. Para contornar problemas desta natureza foi proposto códigos espaço temporais para sistemas de comunicação sem fio que utilizam múltiplas antenas transmissoras e múltiplas antenas receptoras.

Através de técnicas de diversidade, fornecendo réplicas de informações ao receptor. Para cada tempo $t = T$, tomamos x_{mt}, onde $m = 1, \cdots, M$, sinais que são transmitidos a partir de M antenas. Em cada tempo t, o sinal recebido y_t^j, a partir da antena j, é dado por $y_t^j = \sum_{i=1}^{n} h_{i,j} x_{mt} + w_t^t$, onde $h_{i,j}$ é o caminho do canal entre a antena de transmissão i e a antena receptora j, e w_t^j é o ruído introduzido pelo canal. As informações são avaliadas sobre todas as palavras códigos através da métrica de decisão acumulada $\sum_{t=1}^{t} \sum_{j=1}^{m} |y_t^j - \sum_{i=1}^{n} h_{i,j} x_{mt}|^2$, e decide em favor da palavra código que minimiza esta soma.

Este modelo de transmissão pode ser descrito de forma matricial $X = YH + W$, onde Y é a matriz de sinal recebida; X a matriz codificação; H a matriz dos caminhos entre as antenas do canal, e W a matriz que representa o ruído. Então, fazemos uso do *critério do posto* para maximizar o posto r da matriz $X(s_1) - X(s_j)$, tomados sobre todos os pares de sinais distintos (s_1, s_j).

Tomando as matrizes códigos a partir de um espaço de matrizes de ordem n sobre um anel de divisão (onde todo elemento não nulo possui um inverso multiplicativo), obtemos através do critério uma maneira algébrica para maximizar a diversidade. Assim, o código tem diversidade máxima se $|det(X_i - X_j)|^2 \neq 0, \forall X_i \neq X_j \in C$. Porém, caso estes códigos sejam lineares, podemos simplificar o critério do posto avaliando o determinante $|det(X)|^2 \neq 0, \forall 0 \neq X \in C$.

Para satisfazer estes critérios, focaremos nos códigos obtidos a partir de álgebras cíclicas de divisão, onde todo elemento não nulo tem inverso multiplicativo. Consideremos K/F uma extensão de corpos de grau n com grupo de Galois cíclico, $G =< \sigma >$, onde σ é o gerador do grupo cíclico associado a K/F e $\mathcal{O}_F$ e $\mathcal{O}_K$ os anéis de inteiros dos corpos K e F, respectivamente.

Então, $\mathcal{A} = (K/F, \sigma, \gamma)$ é a sua correspondente álgebra cíclica de grau n dada por

$$\mathcal{A} = 1K \oplus eK \oplus \cdots \oplus e_{n-1}K, \tag{1}$$

com $e \in K$ tal que $le = e\sigma(l), \forall l \in K$ e $e^n = \lambda \in F^* = F - \{0\}$.

Podemos identificar estas álgebras cíclicas de grau n por espaço de matrizes $M_{n\times n}(K)$ da seguinte forma: para cada $x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1} \in \mathcal{A}$, tomamos $X \in M_{n\times n}(K)$ por

[1]fabiana.egidio30@hotmail.com
[2]edson.donizete@unesp.br

$$X = \begin{bmatrix} x_0 & \gamma\sigma(x_{n_1}) & \gamma\sigma^2(x_{n_2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n_1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n_2}) & \sigma^2(x_{n_3}) & \cdots & \gamma\sigma^{n-1}(x_n) \end{bmatrix}, \quad (2)$$

ou seja, uma aplicação

$$\begin{aligned} \lambda : \mathcal{A} &\longrightarrow M_{n\times n}(K) \\ x &\mapsto \lambda(x) = X. \end{aligned}$$

Sem muita dificuldade, mostra-se que λ é um isomorfismo. Na álgebra cíclica $\mathcal{A}$, temos a aplicação norma reduzida definida por $N_{rd}(x) = x \cdot \overline{x}$, onde $\overline{x} = x_0 - e_1x_1 - \cdots - e_{n-1}x_{n-1}$, desde que $x = x_0 + e_1x_1 + \cdots + e_nx_n$. A norma reduzida de um elemento x da álgebra $\mathcal{A}$ é igual ao determinante da correspondente matriz X via a aplicação λ. Desde que a álgebra cíclica seja de divisão. Então, todas as matrizes não nulas tem determinantes não nulo, satisfazendo os propósitos que buscamos para a construção dos códigos a partir de $\mathcal{A}$.

Alguns resultados importantes no estudo de norma de um elemento em uma álgebra cíclica são dados por:

Proposição 0.1 [2] *Se $\mathcal{A} = (K/F, \sigma, \gamma)$ é uma álgebra cíclica, então a norma reduzida $N_{rd}(x) \in F, \forall x \in \mathcal{A}$.*

Corolário 0.1 [2] *Seja $\mathcal{A} = (K/F, \sigma, \gamma)$ uma álgebra cíclica. Se $x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1}$, onde $x_0, \cdots, x_{n-1} \in \mathcal{O}_F$, então a norma reduzida $N_{rd}(x) \in \mathcal{O}_F, \forall x \in \mathcal{A}$.*

A seguir apresentaremos o exemplo do famoso Código de Ouro. Para isto, considere $K = (\mathbb{Q}(i), \sqrt{5}) = \{a + b\theta; a, b \in \mathbb{Q}(i)\}$. Temos que para qualquer número inteiro algébrico $z = a + b\theta \in \mathcal{O}_K$, com $a, b \in \mathbb{Z}[i]$, a norma relativa de K sobre $\mathbb{Q}(i)$ é dada por $N_{K/\mathbb{Q}(i)}(a+b\theta) = (a+b\theta)(a+b\overline{\theta}) = a^2 + ab - b^2 \in \mathbb{Z}[i]$.

Assim, tomaremos códigos espaços temporais a partir de uma álgebra cíclica de divisão $\mathcal{A} = (K/F, \sigma, \gamma)$, onde $F = \mathbb{Q}(i), K = \mathbb{Q}(i, \sqrt{5})$ e σ é o gerador $Gal(K/F)$ e $\gamma = i$.

Considerando o código C da forma

$$X = \tfrac{1}{\sqrt{5}} \cdot \begin{bmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ \gamma\overline{\alpha}(c + d\overline{\theta}) & \overline{\alpha}(c + d\overline{\theta}) \end{bmatrix}.$$

onde $\alpha = (1 + i - i\theta), a, b, c, d \in \mathbb{Z}[i]$ e $det(X) = (N_{K/\mathbb{Q}(i)}(z_1) - \gamma N_{K/\mathbb{Q}(i)}(z_2)) \in \mathbb{Z}[i]$.

Mas, $det(X) \neq 0 \Leftrightarrow i \neq N_{rd}(x), \forall x \in \mathcal{A}$ [1]. Como $\mathbb{Z}[i]$ é um conjunto discreto, segue $det(X) \nrightarrow 0, \forall X \in C$. De fato, se $|\gamma| = |i|$, temos que a energia média por antena é uniforme.

Agradecimentos

À FAPESP, pelo apoio financeiro n° 2019/22368 − 6.

Referências

[1] Berdy, G., Oggier F. On the existence of perfect space-time codes, *IEEE Transaction on Information Theory*, 55:(5), 2078 - 2082, 2009. DOI: 10.11.05.2016.033.

[2] Oggier, F. Rekaya, G.. Befiore, J.C.. Viterbo, E.. Perfect space time block codes, *IEEE Transaction on Information Theory* 52(9), 3885 - 3902, 2006. DOI: 10.11.05. 2006. 880010.