Construção de Códigos Matriciais MDS Utilizando Matrizes de Vandermonde

Débora Beatriz Claro Zanitti e Cintya Wink de Oliveira Benedito

***Resumo*— Neste trabalho apresentamos uma construção de códigos MDS, baseado em [1], utilizando matrizes de Vandermonde que são exemplos de matrizes superregulares. Além disso, exemplificamos a codificação e decodificação destes códigos.**

***Palavras-Chave*— Códigos MDS, Codificação, Decodificação.**

***Abstract*— This present study demonstrates a MDS code construction based on [1] using Vandermonde matrices that exemplify superregular matrices. Furthermore, we have exemplified the coding and decoding of these codes.**

***Keywords*— MDS Codes, Coding, Decoding.**

I. Introdução

A teoria de códigos permeia o nosso cotidiano sempre que deseja-se transmitir ou receber uma informação, visto que, por melhor que seja um sistema de comunicação, ele sempre estará sujeito a canais ruidosos ou à falhas. Assim, ao receber um dado ele pode ser diferente daquele transmitido, é então, que faz-se uso dos códigos corretores de erros, que buscam detectar e corrigir possíveis erros que ocorreram durante a transmissão de um dado, [2].

Os códigos matriciais são códigos bidimensionais que podem ser construídos com alfabeto em um corpo ou anel, e possuem várias aplicações em telecomunicações, como por exemplo, em sistemas de armazenamento para proteção de dados contra apagamento. O interesse nos estudos desses códigos está na sua habilidade de corrigir erros em rajada (*burst*), que são erros que ocorrem em bits consecutivos. Além disso eles possuem baixa complexidade de codificação e decodificação, [3]. Este trabalho aborda uma estratégia de codificação e decodificação de códigos matriciais que possuem a propriedade de máxima distância de separação (MDS - *Maximum Distance Separable*), utilizando matrizes de Vandermonde. Códigos MDS são os códigos em que a distância mínima é a máxima possível. Códigos com esta propriedade fornecem proteção máxima contra falhas de um dispositivo, para uma dada quantidade de redundância. Exemplos de códigos MDS não triviais incluem os códigos de Reed–Solomon e suas versões estendidas, [4].

II. Códigos MDS

Códigos de bloco que atingem a igualdade no limitante de Singleton são chamados **códigos MDS**, [5].

Um **código linear** $\mathscr{C}$ é definido como um subespaço vetorial de dimensão k de $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ é um corpo finito com q elementos. Descrevemos o código $\mathscr{C}$ através dos parâmtros $[n, k, d]$, onde n é o comprimento do código, k é a dimensão e d é a distância de Hamming. Um código linear $[n, k, d]$ é dito MDS se, e somente se, $k = n - d + 1$, ou seja, atinge a igualdade no limitante de Singleton, [2]. Códigos MDS, subscritos em $\mathbb{F}_q^b$, podem ser especificados por sua matriz de verificação de paridade H de dimensão $(n-k)b \times nb$ ou por sua matriz geradora G de tamanho $kb \times nb$.

Existem diversas formas de mostrar que um código linear é MDS, a que será utilizada neste trabalho faz uso da seguinte definição: uma matriz A sobre um corpo $\mathbb{F}$ é chamada **superregular** se cada submatriz quadrada em A for não singular, ou seja, com determinante diferente de zero. O resultado a seguir nos garante a equivalência de códigos MDS com matrizes superregulares.

Proposição 1: [5] Seja $\mathscr{C}$ um código linear sobre um corpo $\mathbb{F}$. São equivalentes:

1) $\mathscr{C}$ é MDS.
2) O código $\mathscr{C}$ tem uma matriz geradora na forma sistemática da forma $G = (I|A)$, onde A é uma matriz superregular.

Um matriz superregular A pode ser gerada através da **matriz de Vandermonde**, que é uma matriz em que os termos de cada linha estão em progressão geométrica. Sendo A uma matriz de dimensões $(n-k) \times k$, sua forma geral é definida por

$$A = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{n-k} \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{n-k}^2 \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_{n-k}^3 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_{n-k}^{k-1} \end{bmatrix}. \quad (1)$$

A seguir apresentamos uma estratégia de codificação e decodificação de códigos matriciais MDS utilizando matrizes de Vandermonde.

III. Codificação e Decodificação

Seja $p(x) = x^b + p_{b-1}x^{b-1} + \dots + p_1 x + p_0 \in \mathbb{F}_q[x]$ um polinômio primitivo. Podemos associar $p(x)$ a seguinte matriz

$$C = \begin{bmatrix} 0 & 0 & \dots & 0 & -p_0 \\ 1 & 0 & \dots & 0 & -p_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & -p_{b-2} \\ 0 & 0 & \dots & 1 & -p_{b-1} \end{bmatrix}. \quad (2)$$

Débora Beatriz Claro Zanitti, e-mail: bia.zanitti@hotmail.com; Cintya Wink de Oliveira Benedito, e-mail:cintya.benedito@unesp.br. Universidade Estadual Paulita "Júlio de Mesquita Filho". Este trabalho foi financiado por FAPESP (2017/17948-8).

Considere $M_{m\times t}(\mathbb{F})$ o espaço das matrizes de ordem $m \times n$ com elementos no corpo $\mathbb{F}$. Pode-se definir um isomorfismo $\psi : M_{m\times t}(\mathbb{F}_{q^b}) \longrightarrow M_{m\times t}(\mathbb{F}_C)$, dado por $\psi(A) = [\psi(\alpha_{ij})] \in M_{m\times t}(\mathbb{F}_q[C])$.

Teorema 1: [1] Se $A = [\alpha_{ij}] \in M_{(n-k)\times k}(\mathbb{F}_{q^b})$ é uma matriz superregular, então $H = [\psi(A)\ I_{(n-k)\times b}]$ é a matriz controle de paridade de um $[n, k, n-k+1]$ código matricial MDS.

Nas condições do Teorema 1, temos que:

$$H = \left[\begin{array}{cccc:c} A_{11} & A_{12} & ... & A_{1k} & \vdots & \\ A_{21} & A_{22} & ... & A_{2k} & \vdots & \\ \vdots & \vdots & \ddots & \vdots & \vdots & I_{(n-k)b} \\ A_{(n-k)1} & A_{(n-k)2} & ... & A_{(n-k)3} & \vdots & \end{array}\right].$$

Agora, assuma que c é uma palavra-código e que v é a mensagem recebida, então $e = v - c$ é o vetor erro.

A síndrome s de v é definida por

$$s^T = Hv^T = \sum_{l=1}^{t} A_{il} v_l^T + v_{t+i}^T = \sum_{l=1}^{t} A_{il} e_l^T + e_{t+i}^T, \quad (3)$$

onde $s = [s_1\ \ s_2\ \ \ldots s_{n-k}]$.

Para códigos com parâmetros $[4+k, k, 5]$ sobre $\mathbb{F}_2^b$, em [1] é apresentado um algoritmo de decodificação para correção de uma ou duas rajada de erros. Devido a limitação de espaço, apresentaremos apenas os passos para correção de 1 erro, e em seguida iremos exemplificá-lo em uma matriz de Vandermonde.

Após efetuar os cálculos da síndromes através da Equação 3, temos que:

Algoritmo: Considere $s = [s_1\ s_2\ s_3\ s_4]$.

1) Caso dois blocos de síndromes sejam zero, o algoritmo para e não há erros no código. Caso contrário, $l_1 = 0$;
2) Seja $l_1 = l_1 + 1$. Se $l_1 = k$, o algoritmo para e declaramos que existem mais de dois erros. Caso contrário, vá para o próximo passo.
3) Calcule os vetores:
$$y_1^T = s_1^T + A_{1l_1} A_{4l_1}^{-1} s_4^T, \quad y_2^T = s_2^T + A_{2l_1} A_{1l_1}^{-1} s_1^T,$$
$$y_3^T = s_3^T + A_{3l_1} A_{2l_1}^{-1} s_2^T, \quad y_4^T = s_4^T + A_{4l_1} A_{3l_1}^{-1} s_3^T.$$
4) Se quaisquer dois valores de y for 0, só existe um erro na posição l_1 dado por $e_{l_1}^T = A_{tl_1}^{-1} s_t^T$ para $t = 1, 2, 3$ e o algoritmo acaba. Caso contrário, mais de um erro ocorreu.

Exemplo 1: Considerando o polinômio primitivo $p(x) = x^4 + x + 1 \in F_2[x]$, têm-se que a matriz C é dada por:

$$C = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Seja α um elemento primitivo tal que $\alpha^4 + \alpha + 1 = 0$. Então a matriz de Vandermonde em α será

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 \\ \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix},$$

que é uma matriz superregular. Então

$$H = \left[\begin{array}{cccc:c} I_4 & I_4 & I_4 & I_4 & \vdots & \\ C & C^2 & C^3 & C^4 & \vdots & I_{16} \\ C^2 & C^4 & C^6 & C^8 & \vdots & \\ C^3 & C^6 & C^9 & C^{12} & \vdots & \end{array}\right],$$

é a matriz de verificação de paridade de um código matricial MDS de parâmetros $[8, 4, 5]$. Assumindo que a palavra recebida foi

$$v = [0110\ \ 1011\ \ 1101\ \ 1001\ \ 0110\ \ 1111\ \ 0000\ \ 1101].$$

Através da Equação (3), é possível encontrar as síndromes:

$$s_1^T = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix},\ s_2^T = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, s_3^T = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} s_4^T = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

e como são todas diferentes de zero, encontra-se

$$y_1^T = s_1^T + A_{11}A_{41}^{-1}s_4^T = 0^T, \quad y_2^T = s_2^T + A_{21}A_{11}^{-1}s_1^T = 0^T,$$
$$y_3^T = s_3^T + A_{31}A_{21}^{-1}s_2^T = 0^T, \quad y_4^T = s_4^T + A_{41}A_{31}^{-1}s_3^T = 0^T.$$

Como todos são zero, significa que ocorreu um erro na posição $l_1 = 1$ dado por:

$$e_1^T = A_{11}^{-1} s_1^T = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Então, a palavra corrigida é:

$$c = v - e = [1001\ \ 1011\ \ 1101\ \ 1001\ \ 0110\ \ 1111\ \ 0000\ \ 1101].$$

IV. Conclusões

Neste trabalho foi apresentado uma construção de códigos matriciais MDS utilizando matrizes superregulares. Na referência [1] estas matrizes são aleatórias, aqui introduzimos a utilização de matrizes de Vandermonde na concepção dos códigos, as quais são de fácil manipulação e implementação. Tal construção pode ser utilizada em diversas aplicações em telecomunicações, como em sistemas de armazenamento distribuído para proteger dados contra apagamentos, onde erros em rajada ocorrem.

Agradecimentos

Os autores agradecem ao SBrT pela oportunidade e o apoio financeiro da FAPESP Processo 2017/17948-8.

Referências

[1] S. D. Cardell, J. J. Climent, V. Requena. A construction of MDS array codes. *WIT Transactions on Information and Communication Technologies*, 2013.
[2] W. C. Huffman and V. Pless. *Fundamentals of Error Correting Codes*, Cambridge University Press, 2003.
[3] M. Blaum, P.G. Farrell, H.C.A. Van Tilborg, Array codes. Chapter 22 in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman (Eds.), Elsevier Science B.V, 1998.
[4] F. Tosato and M. Sandell. *Irregular MDS Array Codes,* in IEEE Transactions on Information Theory, vol. 60, no. 9, pp. 5304-5314, Sept. 2014. doi: 10.1109/TIT.2014.2336656
[5] R. M. Roth. *Introduction to Coding Theory*, Cambridge University Press, 2006.