Algoritmo de Decodificação para Correção de até Duas Rajadas de Erros em Códigos Matriciais MDS

Débora Beatriz Claro Zanitti, Carina Alves, Cintya Wink de Oliveira Benedito

***Resumo*— Este trabalho apresenta um algoritmo de decodificação de até duas rajadas de erros para códigos matriciais MDS com parâmetros $(m+k, k, m+1)$, para todo $m \geq 4$, utilizando matrizes superregulares, tais como as matrizes de Vandermonde. Este algoritmo é uma generalização do algoritmo proposto em [1], onde o caso $m = 4$ é apresentado. Também será apresentado um exemplo de decodificação de três rajadas de erros, o que nos leva a conjecturar que o algoritmo proposto pode ser utilizado para correção de mais rajadas de erros.**

***Palavras-Chave*— Códigos Matriciais, Códigos MDS, Matrizes Superregulares, Erros em Rajada.**

***Abstract*— This work presents a decoding algorithm for up to two burst errors for MDS matrix codes with parameters $(m+k, k, m+1)$, for all $m \geq 4$, using superregular matrices, such as Vandermonde matrices. This algorithm is a generalization of the algorithm proposed in [1], where the case $m = 4$ is presented. An example of decoding three burst errors will also be presented, which leads us to conjecture that the proposed algorithm can be used to correct more burst of errors.**

***Keywords*— Matrix Codes, MDS Codes, Superregular Matrices, Burst of Errors.**

I. INTRODUÇÃO

Os códigos corretores de erros são utilizados para transmitir ou armazenar informações de modo confiável e seguro, uma vez que a mensagem transmitida pode ter seu conteúdo comprometido devido a interferências no canal. A ideia básica de um código corretor de erros é de codificar uma informação acrescentando a esta, de maneira organizada, bits de redundâncias permitindo assim, ao receber tal informação, detectar e corrigir erros, [2]. Para obter bons códigos corretores de erros é desejável obter códigos com a maior distância mínima possível. Códigos que possuem a propriedade de máxima distância de separação, ou seja, códigos em que a distância mínima é a máxima possível, são chamados de códigos MDS (*Maximum Distance Separable*), [3]. Códigos com esta propriedade fornece proteção máxima contra falhas de um dispositivo para uma dada quantidade de redundância.

Códigos matriciais são códigos corretores de erros bidimensionais que possuem como principal característica a habilidade de corrigir erros em rajada (*burst of errors*), ou seja, erros que ocorrem em bits consecutivos, [4]. Estes códigos são conhecidos pela sua flexibilidade e facilidade de codificação e decodificação. Inicialmente, códigos matriciais MDS foram utilizados para correção de erros de apagamento como em gravações magnéticas [4]. Porém devido a sua capacidade de correção de rajadas de erros, estes códigos também têm se mostrado eficiente em aplicações recentes como em sistemas de armazenamento distribuído [5], para reparação eficiente de nós com falhas (apagamentos) [6] e também em reparos cooperativos [7].

Neste trabalho será apresentado um algoritmo de decodificação para correção de até duas rajadas de erros de códigos matriciais MDS construídos a partir de matrizes superregulares. Inicialmente na Seção II serão apresentados conceitos que serão utilizados no decorrer do trabalho, tal como a definição de códigos lineares, códigos matriciais, códigos MDS, de matrizes superregulares e do logaritmo de Zech. Na Seção III será apresentada a construção de códigos matriciais MDS através de matrizes superregulares e da matriz de Frobenius, ambas essenciais para construção da matriz verificação de paridade. Na Seção IV será apresentado um algoritmo de decodificação para códigos matriciais MDS construídos a partir dos conceitos apresentados na Seção III, com capacidade de correção de até duas rajadas de erros. Ainda nessa seção será apresentado um exemplo de correção de três rajadas de erros. Finalmente, na Seção V serão apresentadas as conclusões deste trabalho e perspectivas de trabalhos futuros.

II. PRELIMINARES

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 parâmetros $[N, K, D]$, onde N é o comprimento do código, K é a dimensão e D é a distância mínima de Hamming. Para um código linear $\mathscr{C}$ podemos calcular um limitante para o número de palavras códigos, o qual é dado pelo teorema a seguir.

Teorema 1: [2] Se $\mathscr{C}$ um código linear $[N, K, D]$ sobre $\mathbb{F}_q$ então o número máximo de palavras-código possíveis é q^K e o limite Singleton afirma que

$$q^K \leq q^{N-D+1}, \tag{1}$$

ou seja, $K \leq N - D + 1$ ou ainda, $D \leq N - K + 1$.

Um código no qual a igualdade é alcançada no limitante de Singleton é chamado de **código com distância máxima separável - MDS** (*Maximum Distance Separable*), o que significa que nenhum código de comprimento N e distância mínima D tem mais palavras-código que um código MDS com os mesmos parâmetros.

Agora, se tomarmos $b > 0$ um inteiro positivo tal que b divide K, então podemos construir um **código matricial**

Débora Beatriz Claro Zanitti, Universidade Estadual Paulita "Júlio de Mesquita Filho", Campus São João da Boa Vista-SP, e-mail: debora.zanitti@unesp.com; Carina Alves, Universidade Estadual Paulita "Júlio de Mesquita Filho", Campus Rio Claro-SP, e-mail: carina.alves@unesp.br; Cintya Wink de Oliveira Benedito, Universidade Estadual Paulita "Júlio de Mesquita Filho", Campus São João da Boa Vista-SP,e-mail:cintya.benedito@unesp.br. Este trabalho foi financiado por FAPESP (2017/17948-8).

linear sobre $\mathbb{F}_q^b$, com parâmetros $[n, k, d]$, onde $k = K/b$, $n = N/b$ e a distância mínima d é calculada considerando o código sobre $\mathbb{F}_q^b$. Tais códigos podem ser especificados por sua matriz verificação de paridade H de dimensão $(n-k)b \times nb$, gerando palavras-código de comprimento nb, onde b torna-se o comprimento da rajada de erro. O limitante de Singleton continua válido, ou seja, temos $d \leq n-k-1$. E, se a igualdade é alcançada temos um **código matricial linear MDS**.

No contexto da teoria de códigos, as matrizes superregulares com entradas no corpo finito $\mathbb{F}_q$ podem ser usadas para gerarem códigos lineares e códigos matriciais com boas propriedades de distância.

Definição 1: Uma matriz retangular A com elementos em $\mathbb{F}_q$ é chamada **superregular** se toda submatriz de A não for singular, ou seja, todos seus determinantes são diferentes de zero.

Proposição 1: [8] Seja $\mathscr{C}$ um código linear $[N, K, D]$ sobre um corpo finito $\mathbb{F}_q$. São necessárias as seguintes condições para que o código seja MDS:

1) Todo conjunto de $n-k$ colunas em qualquer matriz de verificação de paridade H de $\mathscr{C}$ é linearmente independente.
2) Todo conjunto de k colunas em qualquer matriz geradora de $\mathscr{C}$ é linearmente independente.
3) O código dual $\mathscr{C}^{\perp}$ é MDS.
4) O código $\mathscr{C}$ tem uma matriz geradora na forma sistemática da forma $G = (I|A)$, onde A é uma matriz superregular.

A partir da Proposição 1, também é possível obter códigos matriciais lineares MDS utilizando matrizes superregulares. Neste trabalho iremos considerar exemplos particulares de matrizes superregulares, especificamente as matrizes de Vandermonde.

Definição 2: Uma matriz A é dita **matriz de Vandermonde** se todas as suas linhas estão em progressão geométrica.

Sejam $\alpha_1, ..., \alpha_{n-k}$ elementos não nulos em um corpo $\mathbb{F}$ e A uma matriz de dimensões $(n-k) \times k$. Uma matriz de Vandermonde é dada por

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

A transposta desta matriz também é uma matriz de Vandermonde.

Um outro conceito que será utilizado neste trabalho é o de logaritmo de Zech, o qual definiremos a seguir. Algumas propriedades deste logaritmo podem ser encontradas em [9].

Definição 3: Se α é um elemento primitivo de um corpo finito $\mathbb{F}_q$, então o **logaritmo de Zech** de um número inteiro n em relação à base α é definida pela equação

$$Z_\alpha(n) = log_\alpha(1+\alpha^n) \iff \alpha^{Z_\alpha(n)} = 1+\alpha^n, \quad (3)$$

onde o resultado do logaritmo é limitado ao corpo, uma vez que para $\mathbb{F}_q$ temos que $\alpha^{q-1} = 1$.

III. Construção de Códigos MDS

Seja $p(x) = x^b + p_{b-1}x^{b-1} + ... + p_1x + p_0 \in \mathbb{F}_q[x]$ um polinômio primitivo. Podemos associar a $p(x)$ uma matriz chamada **matriz de Frobenius** (*Frobenius companion matrix*), que é uma matriz que contém 1's (uns) na subdiagonal e a última coluna é dada pelos coeficientes de $p(x)$, sendo os demais elementos todos nulos, como segue

$$C = \begin{bmatrix} 0 & 0 & \dots & 0 & -p_0 \\ 1 & 0 & \dots & 0 & -p_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & -p_{b-2} \\ 0 & 0 & \dots & 1 & -p_{b-1} \end{bmatrix}. \quad (4)$$

Considere $M_{m\times n}(\mathbb{F}_q)$ o espaço das matrizes de ordem $m \times n$ com elementos no corpo finito $\mathbb{F}_q$. A partir do isomorfismo $\phi : \mathbb{F}_{q^b} \longrightarrow \mathbb{F}_q[C]$, dado por $\phi(\alpha) = C$, em [1], é definido o isomorfismo $\psi : M_{m\times n}(\mathbb{F}_{q^b}) \longrightarrow M_{m\times n}(\mathbb{F}_q[C])$, dado por $\psi(A) = [\phi(\alpha_{ij})] \in M_{m\times n}(\mathbb{F}_q[C])$. Nestas condições, o seguinte resultado que nos fornece uma matriz controle de paridade de um código matricial linear MDS.

Teorema 2: [1] Se $A = [\alpha_{ij}] \in M_{(n-k)\times k}(\mathbb{F}_{q^b})$ é uma matriz superregular, então $H = [\psi(A) \mid I_{(n-k)\times b}]$ é uma matriz controle de paridade de um $[n, k, n-k+1]$ código matricial linear MDS $\mathscr{C}$.

IV. Decodificação de Códigos Matriciais MDS

Considere um código matricial MDS $\mathscr{C}$ sobre $\mathbb{F}_2^b$, com b um inteiro positivo, construído nas condições do Teorema 2. Os parâmetros deste código são $[n, k, n-k+1] = [m+k, k, m+1]$, ou seja, $m = n-k$, e a matriz controle de paridade será dada por

$$H = \left[\begin{array}{cccc|c} A_{11} & A_{12} & \dots & A_{1k} & \\ A_{21} & A_{22} & \dots & A_{2k} & \\ \vdots & \vdots & \ddots & \vdots & I_{mb} \\ A_{m1} & A_{m2} & \dots & A_{mk} & \end{array}\right], \quad (5)$$

com $A_{ij} = C^{\sigma(i,j)}$, onde $C \in M_{b\times b}(\mathbb{F}_2)$ é como em (4) e $\sigma(i,j)$ é a potência de cada elemento (i,j) da matriz superregular A.

Sejam $c = [c_1\ c_2\ \dots\ c_n]$ a palavra-código enviada, $v = [v_1\ v_2\ \dots\ v_n]$ o vetor recebido e $e = [e_1\ e_2\ \dots\ e_n]$ o vetor erro, onde $e = v - c$ e $c_j, v_j, e_j \in \mathbb{F}_2^b$, para todo $j = 1, \dots, n$.

A **síndrome** s de v é definida por

$$s^T = Hv^T = [s_1\ \ s_2\ \ \dots s_m], \quad (6)$$

onde $s_i \in \mathbb{F}_2^b$ e pode ser calculada por

$$s_i^T = \sum_{j=1}^{k} A_{ij}v_j^T + \sum_{j=k+1}^{n} v_j^T = \sum_{j=1}^{k} A_{ij}e_j^T + \sum_{j=k+1}^{n} e_j^T, \quad (7)$$

para cada $i = 1, \dots, m$.

A seguir apresentamos o algoritmo proposto, sendo ele uma generalização de [1], que corrige até duas rajadas de erros de comprimento b em um código matricial MDS sobre $\mathbb{F}_2^b$ com parâmetros $[m+k, k, m+1]$ para $m \geq 4$, pois a capacidade de correção de erros de um código de bloco linear

é $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{m}{2} \rfloor$. Observamos que para $m = 2$ e 3 o código é capaz de corrigir até um erro e um algoritmo similar pode ser apresentado. **Algoritmo 1:** Iniciamos com os valores de m e k, parâmetros do código, e com a matriz controle de paridade H correspondente como em (5). Seja $v = [v_1, \ldots, v_n]$ o vetor recebido, onde $n = m + k$.

1) Calcule a síndrome $s = [s_1 \;\; s_2 \;\; \ldots s_m]$ de v, utilizando a Equação 7, para cada $i = 1, \ldots, m$.
2) Se $s_j \neq 0$ e $s_i = 0$, para todo $i \neq j$ e $i = 1, \ldots, m$, então faça $e_{k+j} = s_j$ e dizemos que o erro ocorreu na posição $k + j$.
3) Se $s_{j_1} \neq 0$, $s_{j_2} \neq 0$ e $s_i = 0$ para todo $i \neq j_1 \neq j_2$ e $i = 1, \ldots, m$, então faça $e_{k+j_1} = s_{j_1}$ e $e_{k+j_2} = s_{j_2}$. Neste caso, dizemos que os erros ocorreram nas posições $k + j_1$ e $k + j_2$. Caso contrário, seja $l_1 = 0$
4) Faça $l_1 = l_1 + 1$. Se $l_1 = k$, então o algoritmo finaliza pois mais de dois erros ocorreram. Caso contrário, vá para o próximo passo.
5) Calcule os seguintes vetores

$$\begin{aligned} y_1^T &= s_1^T + A_{1l_1} A_{ml_1}^{-1} s_m^T, \\ y_2^T &= s_2^T + A_{2l_1} A_{1l_1}^{-1} s_1^T, \\ y_3^T &= s_3^T + A_{3l_1} A_{2l_1}^{-1} s_2^T, \\ &\vdots \\ y_m^T &= s_m^T + A_{ml_1} A_{(m-1)l_1}^{-1} s_{m-1}^T. \end{aligned} \tag{8}$$

6) Se tivermos $(y_i, y_{i+1}) = (0, 0)$, para algum $i = 1, \ldots, m-1$ ou $(y_m, y_1) = (0, 0)$, então existe uma rajada de erros de comprimento b na posição l_1 dada por

$$e_{l_1}^T = A_{il_1}^{-1} s_i, \tag{9}$$

para todo $i = 1, \ldots, m$. Caso contrário, vá para o próximo passo.
7) Para $l_2 \in \{l_1 + 1, l_1 + 2, \ldots, k\}$, se

$$y_i^T = C^{r_{i-2}} y_{i-1}^T, \tag{10}$$

para todo $i = 3, 4, \ldots, m$ com

$$\begin{aligned} r_{i-2} = \sigma(i, l_2) - \sigma(i-1, l_2) + Z(\sigma(i, l_1) \\ - \sigma(i, l_2) - \sigma(i-1, l_1) + \sigma(i-1, l_2)) \\ - Z(\sigma(i-1, l_1) - \sigma(i-1, l_2) \\ - \sigma(i-2, l_1) + \sigma(i-2, l_2)) \end{aligned}, \tag{11}$$

declara-se que ocorreram dois erros, um na posição l_1 e outro na posição l_2. Caso contrário, volte ao Passo 4.

Se o algoritmo declarar que os erros ocorreram nas posições l_1 e l_2, para obter a magnitude dos erros basta resolver o seguinte sistema linear

$$\begin{cases} A_{il_1} e_{l_1}^T + A_{il_2} e_{l_2}^T = s_i^T \\ A_{jl_1} e_{l_1}^T + A_{jl_2} e_{l_2}^T = s_j^T \end{cases}, \tag{12}$$

para $i, j = 1, 2, \ldots, m$ e $i \neq j$.

O teorema a seguir demonstra que o algoritmo proposto de fato corrige até duas rajadas de erros de comprimento b.

Teorema 3: Se $\mathscr{C}$ é um código matricial linear MDS sobre $\mathbb{F}_2^b$ com parâmetros $[m + k, k, m + 1]$, com $m \geq 4$, $k, b \in \mathbb{N}$ e matriz controle de paridade H dada como em (5), então o Algoritmo 1 corrige até duas rajadas de erros de comprimento b.

Prova 1: Como $n = m + k$, os erros na palavra recebida $v = [v_1, \ldots, v_n]$ podem ocorrer nos k símbolos de informação ou nos m símbolos de paridade. Iremos analisar cada uma das possibilidades.

- *Caso1: Um ou dois erros nos símbolos de paridade.* Se 1 ou 2 erros ocorreram nos símbolos de paridade, então $m - 1$ ou $m - 2$ síndromes são zeros, respectivamente. Se os erros ocorreram nas posições $k + j_1$ e $k + j_2$ então as síndromes não nulas serão respectivamente s_{j_1} e s_{j_2}, e as magnitudes dos erros serão

$$e_{k+j_1} = s_{j_1} \;\; e \;\; e_{k+j_2} = s_{j_2}. \tag{13}$$

- *Caso 2: Um erro no símbolo de informação.* Suponhamos que um único erro ocorreu em um símbolo de informação na posição l_1. Então por (7), as síndromes serão dadas por

$$s_i^T = A_{il_1} e_{l_1}^T, \;\; \forall i = 1, \ldots, m. \tag{14}$$

Substituindo em (8), temos $y_i^T = 0$, para todo $i = 1, .., m$ pois

$$e_{l_1}^T = A_{1l_1}^{-1} s_1^T = A_{2l_1}^{-1} = \ldots = A_{ml_1}^{-1} s_m^T, \tag{15}$$

e a magnitude do erro é obtida utilizando qualquer igualdade da Equação 15.
- *Caso 3: Um erro no símbolo de informação e um erro no símbolo de paridade.* Suponhamos que o erro no símbolo de informação ocorreu na posição l_1 e, sem perda de generalidade, que o erro no símbolo de paridade ocorreu na posição $k+1$. Então por (7), as síndromes serão dadas por

$$s_1^T = A_{1l_1} e_{l_1}^T + e_{k+1} \quad e \quad s_i^T = A_{il_1} e_{l_1}^T, \tag{16}$$

para todo $i = 2, \ldots, m$. Neste caso teremos $y_1, y_2 \neq 0$, pois s_1 está presente no cálculo destes vetores, e $y_3 = \ldots = y_m = 0$. Dessa forma a magnitude dos erros serão

$$e_{k+1} = s_1^T \quad e \quad e_{l_1}^T = A_{3l_1}^{-1} s_3^T = \ldots = A_{ml_1}^{-1} s_m^T. \tag{17}$$

- *Caso 4: Dois erros nos símbolos de informação.* Suponhamos que os erros nos símbolos de informação estejam nas posições l_1 e l_2. Por (7) as síndromes são calculadas por

$$s_i^T = A_{il_1} e_{l_1}^T + A_{il_2} e_{l_2}^T, \tag{18}$$

para $i = 1, ..., m$. Substituindo (18) nos vetores y_i dados em (8), teremos $y_i^T \neq 0$, para todo $i = 1, \ldots, m$. Para y_2, temos

$$\begin{aligned} y_2^T &= s_2^T + A_{2l_1} A_{1l_1}^{-1} s_1^T \\ &= (A_{2l_1} e_{l_1}^T + A_{2l_2} e_{l_2}^T) + A_{2l_1} A_{1l_1}^{-1} (A_{1l_1} e_{l_1}^T + A_{1l_2} e_{l_2}^T) \\ &= A_{2l_1} e_{l_1}^T + A_{2l_2} e_{l_2}^T + A_{2l_1} A_{1l_1}^{-1} A_{1l_1} e_{l_1}^T + A_{2l_1} A_{1l_1}^{-1} A_{1l_2} e_{l_2}^T \\ &= A_{2l_2} e_{l_2}^T + A_{2l_1} A_{1l_1}^{-1} A_{1l_2} e_{l_2}^T \\ &= (A_{2l_1} A_{1l_1}^{-1} A_{1l_2}) e_{l_2}^T. \end{aligned} \tag{19}$$

Como $A_{ij} = C^{\sigma(i,j)}$, então

$$y_2^T = (C^{\sigma(2,l_2)} + C^{\sigma(2,l_1) - \sigma(1,l_1) + \sigma(1,l_1)}) e_{l_2}^T. \tag{20}$$

Utilizando o logaritmo de Zech e suas propriedades temos que

$$y_2^T = C^{\sigma(2,l_2)+Z(\sigma(2,l_1)-\sigma(1,l_1)+\sigma(1,l_2)-\sigma(2,l_2))}e_{l_2}^T, \quad (21)$$

ou seja,

$$e_{l_2}^T = C^{-\sigma(2,l_2)-Z(\sigma(2,l_1)-\sigma(1,l_1)+\sigma(1,l_2)-\sigma(2,l_2))}y_2^T. \quad (22)$$

Da mesma forma

$$y_3^T = C^{\sigma(3,l_2)+Z(\sigma(3,l_1)-\sigma(2,l_1)+\sigma(2,l_2)-\sigma(3,l_2))}e_{l_2}^T. \quad (23)$$

Substituindo (22) em (23) temos

$$y_3^T = C^{r_1}y_2^T, \quad (24)$$

onde

$$\begin{aligned} r_1 &= \sigma(3,l_2) - \sigma(2,l_2) \\ &+ Z(\sigma(3,l_1) - \sigma(3,l_2) - \sigma(2,l_1) + \sigma(2,l_2)) \\ &- Z(\sigma(2,l_1) - \sigma(2,l_2) - \sigma(1,l_1) + \sigma(1,l_2)). \end{aligned} \quad (25)$$

De modo análogo, podemos obter para todo $i = 3, \ldots, m$ que

$$y_i^T = C^{r_{i-2}}y_{i-1}^T, \quad (26)$$

onde

$$\begin{aligned} r_{i-2} &= \sigma(i,l_2) - \sigma(i-1,l_2) + Z(\sigma(i,l_1) - \sigma(i,l_2) \\ &- \sigma(i-1,l_1) + \sigma(i-1,l_2)) - Z(\sigma(i-1,l_1) \\ &- \sigma(i-1,l_2) - \sigma(i-2,l_1) + \sigma(i-2,l_2)). \end{aligned} \quad (27)$$

Garantindo as igualdades das Equações 24 e 26, segue que são válidas as expressões s_i, ou seja, os erros de fato ocorreram nas posições l_1 e l_2. Para encontrar a magnitude dos erros, basta resolver o sistema linear com duas equações e duas incógnitas tomando quaisquer duas equações de síndromes como apresentado na Equação 12.

■

A seguir apresentamos um exemplo da utilização do algoritmo proposto.

Exemplo 1: Um código matricial MDS $\mathscr{C}$ com parâmetros $[10, 5, 6]$, ou seja, $m = k = 5$, pode ser obtido a partir do Teorema 2 da seguinte forma. Seja $p(x) = x^5+x^4+x^2+x+1$ um polinômio primitivo. Temos que a matriz de Frobenius C e a matriz superregular de Vandermonde A são dadas por

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

e

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} \\ \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} \end{bmatrix}.$$

Assim, obtêm-se a matriz verificação de paridade para o código $\mathscr{C}$

$$H = \left[\begin{array}{ccccc|c} I_5 & I_5 & I_5 & I_5 & I_5 & \\ C & C^2 & C^3 & C^4 & C^5 & \\ C^2 & C^4 & C^6 & C^8 & C^{10} & I_{25} \\ C^3 & C^6 & C^9 & C^{12} & C^{15} & \\ C^4 & C^8 & C^{12} & C^{16} & C^{20} & \end{array}\right].$$

Supondo que a palavra recebida foi $v = [11000\ 10011\ 01010\ 01011\ 11111\ 10100\ 00110\ 01101\ 00000\ 00000]$. Ao calcular as síndromes obtêm-se

$$s_1^T = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} s_2^T = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} s_3^T = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} s_4^T = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} s_5^T = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Como todas são diferentes de zero, então os erros ocorreram nos símbolos de informação. Considerando $l_1 = 1$, segue-se o algoritmo calculando os vetores

$$y_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} y_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} y_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} y_4 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} y_5 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Uma vez que todos y_i's são diferentes de zero. Para $l_2 = 2$, testa-se a Equação 10 através dos cálculos de r_{i-2} como (11), para $i = 3, 4, 5$. Temos

$$\begin{aligned} r_1 &= \sigma(3,2) - \sigma(2,2) + Z(\sigma(3,1) - \sigma(3,2) - \sigma(2,1) + \sigma(2,2)) \\ &- Z(\sigma(2,1) - \sigma(2,2) - \sigma(1,1) + \sigma(1,2)) \\ &= 4 - 2 + Z(-1) - Z(-1) = 2 \end{aligned},$$

$$\begin{aligned} r_2 &= \sigma(4,2) - \sigma(3,2) + Z(\sigma(4,1) - \sigma(4,2) - \sigma(3,1) + \sigma(3,2)) \\ &- Z(\sigma(3,1) - \sigma(3,2) - \sigma(2,1) + \sigma(2,2)) \\ &= 6 - 4 + Z(-1) - Z(-1) = 2 \end{aligned}$$

e

$$\begin{aligned} r_3 &= \sigma(5,2) - \sigma(4,2) + Z(\sigma(5,1) - \sigma(5,2) - \sigma(4,1) + \sigma(4,2)) \\ &- Z(\sigma(4,1) - \sigma(4,2) - \sigma(3,1) + \sigma(3,2)) \\ &= 8 - 6 + Z(-1) - Z(-1) = 2 \end{aligned}.$$

Logo,

$$y_3^T = c^2y_2^T \quad , \quad y_4^T = c^2y_3^T \quad \text{e} \quad y_5^T = c^2y_4^T.$$

Assim, por (12) obtemos a magnitude dos erros

$$e_1 = [01111] \quad \text{e} \quad e_2 = [01110].$$

Portanto, a palavra-código corrigida é $c = v - e = [10111\ 11101\ 01010\ 01011\ 11111\ 10100\ 00110\ 01101\ 00000\ 00000]$.

A seguir apresentaremos um exemplo de correção de três rajadas de erros de comprimento b em um código matricial MDS de parâmetros $[12, 6, 7]$. Podemos observar que os passos da decodificação são os mesmos do algoritmo proposto, porém as potências r_{i-2} de C, para garantir as igualdades (24) e (26), foram obtidas computacionalmente, pois até o momento não temos uma fórmula fechada para mais de duas rajadas de erros como as apresentadas nas Equações 25 e 27.

Exemplo 2: Para obtermos um código matricial MDS $\mathscr{C}$ com parâmetros $[12, 6, 7]$ utilizando o Teorema 2, considere

o polinômio primitivo $p(x) = x^6 + x^4 + x^3 + x + 1$. Têm-se que a matriz de Frobenius C e a matriz superregular de Vandermonde são dadas por

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

e

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \\ \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \\ \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} & \alpha^{24} \\ \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} & \alpha^{30} \end{bmatrix}$$

Assim,

$$H = \left[\begin{array}{cccccc|c} I_6 & I_6 & I_6 & I_6 & I_6 & I_6 & \vdots \\ C & C^2 & C^3 & C^4 & C^5 & C^6 & \vdots \\ C^2 & C^4 & C^6 & C^8 & C^{10} & C^{12} & \vdots \\ C^3 & C^6 & C^9 & C^{12} & C^{15} & C^{18} & \vdots \\ C^4 & C^8 & C^{12} & C^{16} & C^{20} & C^{24} & \vdots \\ C^5 & C^{10} & C^{15} & C^{20} & C^{25} & C^{30} & \vdots \end{array} \quad I_{36}\right]$$

é a matriz de verificação de paridade de $\mathscr{C}$. Assumindo que a palavra recebida foi $v = [100101\ 100001\ 110000\ 000000\ 000000\ 000000\ 000000\ 000000\ 000000\ 000000\ 000000\ 000000]$, as síndromes por (7) são dadas por

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

$$s_4^T = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} s_5^T = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} s_6^T = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Como todas diferentes de zero, calculamos y_i para $i = 1, 2, \ldots, 6$

$$y_1^T = [110111]^T \quad y_2^T = [101011]^T \quad y_3^T = [111000]^T$$
$$y_4^T = [011011]^T \quad y_5^T = [100100]^T \quad y_6^T = [011110]^T$$

O próximo passo é verificar em quais posições ocorreram os erros, ou seja, encontrar os valores r_j tais que $y_i^T = C^{r_j} y_{i-1}^T$, para $j = 1, 2, 3, 4$. Computacionalmente, obtemos que existem tais potências para as posições $l_1 = 1$, $l_2 = 2$ e $l_3 = 3$, sendo elas

$$y_3^T = c^{11} y_2^T \quad , \quad y_4^T = c^{50} y_3^T \quad , \quad y_5^T = c^6 y_4^T \quad \text{e} \quad y_6^T = c^{30} y_5^T.$$

Para encontrar a magnitude dos erros, basta resolver o seguinte sistema linear

$$\begin{cases} A_{11} e_1^T + A_{12} e_2^T + A_{13} e_3^T = s_1^T, \\ A_{21} e_1^T + A_{22} e_2^T + A_{23} e_3^T = s_2^T. \\ A_{31} e_1^T + A_{32} e_2^T + A_{33} e_3^T = s_3^T. \end{cases}$$

obtendo-se

$$e_1 = [100101], \quad e_2 = [100001] \quad \text{e} \quad e_3 = [110000].$$

V. Conclusões

Neste trabalho foi apresentado um algoritmo de decodificação de códigos matriciais MDS capaz de corrigir até duas rajadas de erros de comprimento b com parâmetros $[m+k, k, m+1]$, para todo $m \geq 4$. Também foi apresentando um exemplo para a decodificação de três rajadas de erros. Como continuidade pretendemos aprimorar o algoritmo para que ele seja capaz de corrigir todos os $\lfloor \frac{d-1}{2} \rfloor$ erros de um código matricial MDS. Pretendemos também verificar se a construção de códigos matriciais MDS utilizando matrizes superregulares e o algortimo de decodificação apresentado são eficientes em aplicações de sistemas de armazenamento distribuído para recuperação de nós com falhas.

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 and V. Requena, "A Construction Of MDS Array Codes", in *WIT Transactions on Information and Communication Technologies*, v.45, pp. 47 - 58, May 2013, doi:10.2495/DATA130051.

[2] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Nova York, 1977.

[3] S. Roman, *Coding and Information Theory*, Springer-Verlag, 1992.

[4] 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

[5] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright and K. Ramchandran, "Network Coding for Distributed Storage Systems,"in *IEEE Transactions on Information Theory*, v. 56, no. 9, pp. 4539-4551, Sept. 2010, doi:10.1109/TIT.2010.2054295.

[6] M. Ye and A. Barg, "Explicit Constructions of High-Rate MDS Array Codes With Optimal Repair Bandwidth,"in *IEEE Transactions on Information Theory*, v. 63, no. 4, pp. 2001-2014, April 2017, doi: 10.1109/TIT.2017.2661313.

[7] M. Ye and A. Barg, "Cooperative Repair: Constructions of Optimal MDS Codes for All Admissible Parameters,"in *IEEE Transactions on Information Theory*, v. 65, no. 3, pp. 1639-1656, March 2019, doi: 10.1109/TIT.2018.2856206.

[8] R. M. Roth. *Introduction to Coding Theory*, Cambridge University Press, 2006.

[9] K. Huber, "Some Comments on Zech's logarithms", in *IEEE Transactions on Information Theory*, v. 31, no. 4, pp. 1314-1319, Jul. 1990, doi: 10.1109/18.53764.