Exemplos de Códigos de Bloco Lineares 5 e 7-ários com Máxima Distância Euclidiana

Raissa Andrade Oliveira e Rodrigo Gusmão Cavalcante

***Resumo*— Neste trabalho apresentamos alguns exemplos de códigos de bloco lineares 5 e 7-ários com máxima distância Euclidiana entre as palavras-código. Tais códigos foram obtidos de um problema de otimização linear inteira derivada da representação modular de códigos de blocos lineares.**

***Palavras-Chave*— Código de bloco linear, distância mínima Euclidiana, representação modular, programação linear inteira.**

***Abstract*— In this work we present some examples of 5 and 7-ario linear codes of block with maximum Euclidian distance between code words. These codes were obtained from an integer linear optimization problem derived from the modular representation of linear codes of block.**

***Keywords*— Linear codes of block, Euclidian minimal distance, modular representation, integer linear programming.**

I. INTRODUÇÃO

A classe de códigos corretores de erro denominada códigos de bloco lineares tem grande aplicação nos principais sistemas de codificação digital. Em geral, quando o canal é binário simétrico (BSC) tanto a codificação quanto a decodificação são realizadas usando a distância de Hamming. Entretanto, em determinadas situações outras medidas de distância como a de Lee ou a Euclidiana podem ser mais adequadas para o projeto do sistema de comunicações.

O desempenho dos códigos corretores de erro pode ser medido em função do quanto uma palavra-código se difere de qualquer outra palavra-código. Neste caso, quanto maior for essa diferença menor será a probabilidade do decodificador decidir erroneamente, isto é, decidir por uma palavra-código não transmitida. Essa diferença entre palavras-código é quantificada, geralmente, em termos da distância mínima (d_{min}) do código, que é definida como sendo a menor das distâncias entre quaisquer duas palavras-código. Neste trabalho, consideramos que a d_{min} seja medida em função da distância Euclidiana.

Em [4], um método para a construção de códigos de bloco lineares sobre $\mathbb{F}_q$, q primo, com máxima d_{min} usando programação linear inteira [2] foi descrito em função da representação modular [3] para códigos de bloco lineares. Neste trabalho usamos tal método para construir códigos de bloco lineares sobre $\mathbb{F}_5$ com taxas $r = 1/n, 2/3, 2/4, 2/5$ e $2/6$ e sobre $\mathbb{F}_7$ com taxas $r = 2/3$ e $2/4$ com máxima d_{min} Euclidiana.

Este trabalho está organizado da seguinte forma. Na Seção II apresentamos a representação modular exemplificando seu cálculo para a distância Euclidiana. Na Seção III descrevemos o problema de otimização a ser resolvido e apresentamos uma possível técnica para solucioná-lo. Na Seção IV alguns códigos são apresentados. Finalmente, na Seção V as conclusões são apresentadas.

Raissa Andrade Oliveira e Rodrigo Gusmão Cavalcante, Graduação em Engenharia Elétrica, Centro Federal de Educação Tecnológica da Bahia, Unidade de Ensino de Vitória da Conquista, Bahia, Brasil, emails: raissa_engenharia@yahoo.com.br e rodgcav@cefetba.br.

II. REPRESENTAÇÃO MODULAR

De acordo com [3] e [4] um código de bloco linear q-ário de taxa $r = k/n$ pode ter sua matriz geradora $\mathbf{G}$ representada por um vetor

$$\mathbf{N} = [n_1, n_2, \cdots, n_m], \quad \text{(representação modular)} \quad (1)$$

onde $m = q^k - 1$ e $n_i \in \mathbb{N}$ é a quantidade de colunas de $\mathbf{G}$ do tipo i na forma q-ária. Por exemplo, se $k = 2$, $q = 5$ e $n_{17} = 1$ então existe uma coluna em $\mathbf{G}$ igual a $[2\ 3]^T$, pois $17_{10} = 23_5$.

Usando a representação modular (1), o espectro de distâncias $\mathbf{W}$ do código pode ser obtido por $\mathbf{W} = \mathbf{N} \cdot \mathbf{C}$, onde $\mathbf{C}$ pode ser obtida usando a matriz $\mathbf{M}_{k \times m}$ que possui como colunas todas as possíveis combinações de k elementos de $\mathbb{F}_q$, exceto a combinação toda nula. Por exemplo, caso $q = 5$, $k = 1$ e $\mathbf{G} = \mathbf{M} = [1\ 2\ 3\ 4]$, então as palavras-código são dadas por $\{c_0 = 0000,\ c_1 = 1234,\ c_2 = 2413,\ c_3 = 3142,\ c_4 = 4321\}$ e a matriz $\mathbf{C}$, cujas colunas representam a distância Euclidiana entre cada uma das palavras-código, é dada por

$$\mathbf{C} = \begin{bmatrix} 1 & 2 & 3 & 4 & 1 & 2 & 3 & 1 & 2 & 1 \\ 2 & 4 & 1 & 3 & 2 & 1 & 1 & 3 & 1 & 2 \\ 3 & 1 & 4 & 2 & 2 & 1 & 1 & 3 & 1 & 2 \\ 4 & 3 & 2 & 1 & 1 & 2 & 3 & 1 & 2 & 1 \end{bmatrix}. \quad (2)$$

Neste caso, $\mathbf{N} = [1\ 1\ 1\ 1]$ e $\mathbf{W} = [10\ 10\ 10\ 10\ 6\ 6\ 8\ 8\ 6\ 6]$ ou, equivalentemente, $\mathcal{D}(t) = 4t^6 + 2t^8 + 4t^{10}$, o que significa que existem 4 combinações de palavras-código ((c_1, c_2), (c_1, c_3), (c_2, c_3) e (c_3, c_4)) com distância Euclidiana 6, 2 combinações ((c_1, c_4) e (c_2, c_3)) com distância 8 e 4 combinações ((c_0, c_1), (c_0, c_2), (c_0, c_3) e (c_0, c_3)) com distância 10.

III. FORMULAÇÃO DO PROBLEMA DE OTIMIZAÇÃO

Segundo [4], usando a representação modular (1) pode-se formular o problema de otimização linear inteira descrito por (3), cujas soluções fornecem o vetor $\mathbf{N}$ de um código de bloco de taxa $r = k/n$ com d_{min} máxima.

$$\begin{array}{ll} \text{Maximizar:} & z = w \\ \text{Sujeito a:} & \mathbf{N} \cdot \mathbf{C} \geq w\mathbf{1} \\ & \sum n_i = n \\ & n_i \geq 0, \text{ inteiros,} \end{array} \quad (3)$$

onde $\mathbf{1} = [1, 1, \ldots, 1]^T$ e w é igual a distância mínima do código. Observe que esse problema foi formulado de maneira geral, pois caso a medida de distância seja alterada, então basta apenas modificar a matriz $\mathbf{C}$ para determinar o código nesse novo contexto. Por exemplo, caso a distância seja a euclidiana ao quadrado, então é suficiente elevar os termos de $\mathbf{C}$ ao quadrado. Além disso, algumas colunas de $\mathbf{C}$ que se repetem podem ser retiradas para simplificar o problema (3), como as colunas 5 e 10 e as colunas 6 e 9 em (2).

Neste trabalho, o problema de otimização (3) foi resolvido para alguns valores de q, k e n usando o método plano de corte (*cutting plane*) descrito em [2]. A idéia deste método é adicionar novas restrições ao problema com o objetivo de forçar que a solução ótima do problema seja inteira.

Uma maneira eficiente de gerar planos de corte é usar o corte de *Gomory*. Tal corte é obtido de uma das restrições gerada pelo método simplex para a solução corrente ótima da relaxação linear, isto é, se tivermos a restrição

$$n_k + \sum a_i n_i = b_k,$$

sendo b_k um número não inteiro, então o corte para essa restrição é dada por

$$\sum (a_i - \lfloor a_i \rfloor) n_i \geq b_k - \lfloor b_k \rfloor. \qquad (4)$$

IV. Exemplos de Códigos de bloco lineares q-ários

Inicialmente consideramos os códigos bloco lineares 5-ário com taxa $r = 1/n$ que foram obtidos com o auxílio de (2) e (3), como apresentado na Tabela I.

n	$\mathbf{N}$	d_{min}	$\mathcal{D}(t)$ para $i = 1$
$4i-2$	$[i, i, i-1, i-1]$	$6i-3$	$5t^3 + 3t^4 + t^6 + t^7$
$4i-1$	$[i, i, i, i-1]$	$6i-2$	$2t^4 + 3t^5 + t^6 + 2t^7 + t^8 + t^9$
$4i$	$[i, i, i, i]$	$6i$	$4t^6 + 2t^8 + 4t^{10}$
$4i+1$	$[i+1, i, i, i]$	$6i+1$	$2t^7 + 2t^8 + t^9 + 2t^{11} + 2t^{12} + t^{13} + t^{14}$

TABELA I

Códigos de bloco lineares 5-ários com taxa $r = 1/n$.

Ainda considerando códigos sobre $\mathbb{F}_5$ foram obtidos os seguintes códigos para $k = 2$:

- $r = 2/3$, $d_{min} = 2$, $\mathcal{D}(t) = 16t^2 + 60t^3 + 61t^4 + \cdots$ e
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \end{bmatrix}.$$
- $r = 2/4$, $d_{min} = 4$, $\mathcal{D}(t) = 48t^4 + 56t^5 + 48t^6 + \cdots$ e
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 3 & 4 \end{bmatrix}.$$
- $r = 2/5$, $d_{min} = 5$, $\mathcal{D}(t) = 80t^5 + 40t^6 + 60t^7 + \cdots$ e
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 4 & 3 & 2 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}.$$
- $r = 2/6$, $d_{min} = 6$, $\mathcal{D}(t) = 11t^6 + 36t^7 + 53t^8 + \cdots$ e
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 2 & 4 & 3 \\ 0 & 1 & 3 & 3 & 3 & 4 \end{bmatrix}.$$

Além disso, a distância euclidiana ao quadrado também foi considerada nos códigos 5-ários. Neste caso, não foi observado alterações nos valores de d_{min} e nas matrizes geradoras para as taxas $r = 2/3$ e $2/4$, mas apenas em $\mathcal{D}(t)$, que no caso valem $\mathcal{D}(t) = 16t^2 + 14t^3 + 2t^5 + \cdots$ e $\mathcal{D}(t) = 8t^4 + 44t^6 + 4t^7 + \cdots$, respectivamente. Entretanto, quando a taxa é igual a $2/5$ os seguintes parâmetros foram obtidos: $d_{min} = 7$, $\mathcal{D}(t) = 37t^7 + 10t^8 + 5t^9 + \cdots$ e

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 4 & 2 & 4 \\ 0 & 1 & 2 & 4 & 4 \end{bmatrix}.$$

Por fim, os seguintes códigos sobre $\mathbb{F}_7$ com máxima d_{min} euclidiana foram construídos para $k = 2$:

- $r = 2/3$, $d_{min} = 3$, $\mathcal{D}(t) = 120t^3 + 150t^4 + \cdots$ e
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 3 \end{bmatrix}.$$
- $r = 2/4$, $d_{min} = 5$, $\mathcal{D}(t) = 88t^5 + 207t^6 + \cdots$ e
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 4 & 5 \end{bmatrix}.$$

Da mesma forma que foi realizado no caso em que $q = 5$, também foram construídos códigos 7-ários considerando a distância euclidiana ao quadrado. No caso, novamente a matriz geradora permaneceu inalterada, mas foi obtido $\mathcal{D}(t) = 30t^3 + 3t^4 + 93t^5 + \cdots$ para $r = 2/3$ e $\mathcal{D}(t) = 3t^6 + 91t^7 + t^8 + \cdots$ para $r = 2/4$, cujo d_{min} é maior.

Observe que em alguns dos códigos apresentados anteriormente $d_{min} > n$, fato que não poderia ocorrer caso fosse considerada a distância de Hamming. Neste caso, quando os símbolos do alfabeto q-ário do código são associado aos sinais de uma modulação q-ASK, então a probabilidade de se transmitir, por exemplo, o símbolo 2 e se receber 4 é muito menor que a probabilidade de se receber 3. Tal fato, nos induz a pensar que em geral os erros de transmissão ocorrem com uma distância Euclidiana igual a 1. Neste caso, é como se um código usando a distância Euclidiana ao quadrado, por exemplo, com $d_{min} = 7$, em geral corrigisse até 3 erros.

V. Conclusões

Códigos com máxima distância d_{min} Euclidiana e Euclidiana ao quadrado foram construídos para $\mathbb{F}_5$ e $\mathbb{F}_7$. Como esperado, tais códigos apresentam valores de d_{min} maiores do que se a medida de distância fosse por exemplo a distância de Hamming. Tal fato, propicia maior correção de erros. Além disso, o método do plano de corte aplicado na resolução do problema de otimização demostrou ser adequado.

Agradecimentos

Os autores agradecem a FAPESB e ao CNPq pela bolsa de iniciação científica fornecida no período de desenvolvimento desse trabalho.

Referências

[1] S. Haykin, *Sistemas de Comunicações: Analógicos e Digitais*, Porto Alegre: Bookman, 4.ed., 2004.

[2] L. A. Wolsey, *Integer Programming*. New York: John Wileyand Sons, 1998.

[3] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd. ed. Cambridge: MIT Press, 1972.

[4] R.G. Cavalcante, e R. Palazzo Jr., "Construção de códigos de bloco lineares sobre $\mathbb{F}_q$ com d_{min} máxima usando programação linear inteira", *XXII Simpósio Brasileiro de Telecomunicações-SBrT'05*, Campinas, 2005.