

CONSTRUÇÃO DE CÓDIGOS DE BLOCO LINEARES COM MÁXIMA DISTÂNCIA EUCLIDIANA

Raissa Andrade OLIVEIRA (1); Rodrigo Gusmão CAVALCANTE (2)

(1) CEFET-BA, Unidade de Ensino de Vitória da Conquista, Av. Amazonas, 3150. Bairro Zabelê. Vitória da Conquista, Bahia. Fone: (77) 3426-2271, e-mail: raissa_engenharia@yahoo.com.br

(2) CEFET-BA, Unidade de Ensino de Vitória da Conquista, Av. Amazonas, 3150. Bairro Zabelê. Vitória da Conquista, Bahia. Fone: (77) 3426-2271, e-mail: rodgcav@cefetba.br

RESUMO

A classe de códigos de blocos lineares é muito utilizada em sistemas de comunicações digitais cuja informação é transmitida em canais ruidosos, como, por exemplo, na comunicação sem fio. Neste caso, o uso de códigos de bloco lineares permite a detecção e a correção dos possíveis erros ocorridos durante o processo de transmissão. Neste trabalho, construímos uma classe de códigos de bloco lineares sobre o corpo de Galois q -ário (F_q), com q primo e máxima distância Euclidiana entre as palavras-código, de forma que sua capacidade de correção fosse máxima para uma determinada taxa de transmissão. Para tanto, utilizamos uma representação modular de códigos de bloco sobre F_q para formular um problema de otimização linear inteira, cujas soluções fossem códigos de blocos lineares ótimos. O método utilizado para resolver esse problema de otimização linear inteira foi o método do plano de cortes (*cutting plane*), que foi implementado computacionalmente com o auxílio do programa *Octave* e *SciLab*. Usando essas rotinas computacionais desenvolvidas, alguns exemplos de códigos de bloco lineares q -ários com máxima distância Euclidiana entre as palavras-código foram obtidos e apresentaram valores de distâncias Euclidiana entre as palavras-código maiores do que os códigos tradicionais que usam a distância de *Hamming* como parâmetro de desempenho, isto é, maior correção de erros. Além disso, usando simulação computacional e o método de Monte Carlo, curvas de probabilidade média de erro *versus* energia média de transmissão foram construídas para analisar o desempenho dos códigos de bloco propostos. Neste caso, verificamos que os códigos de bloco obtidos apresentam bons desempenhos e são de interesse prático para a correção de erros na transmissão de informação digital.

Palavras-chave: código de bloco linear, máxima distância Euclidiana, representação modular.

1. INTRODUÇÃO

Um dos principais problemas nos sistemas de comunicações digitais é que as informações a serem transmitidas estão sempre sujeitas a ação de ruídos. Em canais binários simétricos (BSC) existem, geralmente, a presença de um ruído denominado ruído Aditivo Gaussiano Branco (AWGN) que ocasiona erros de transmissão.

Elaboradas técnicas de codificação estão sendo desenvolvidas com o intuito de identificar e quando possível corrigir os erros na transmissão da informação, a classe de códigos corretores de erro denominada códigos de bloco lineares é de grande aplicação nos principais sistemas de codificação digital e utiliza a distância de *Hamming* para a codificação e a decodificação em canais binários simétricos. 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 comunicação.

O desempenho dos códigos corretores de erro pode ser medido em função da diferença entre duas palavras-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 o número de símbolos em posições correspondentes que diferem entre si, e é quantificada 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, como visto em [5].

Em [4], um método para a construção de códigos de bloco lineares sobre 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 F_5 com taxas $r = 1/n, 2/3, 2/4, 2/5$ e $2/6$ e sobre F_7 com taxas $r = 2/3$ e $2/4$ com máxima d_{min} Euclidiana. A teoria de Shannon é aplicada com o intuito de comparar os resultados das taxas dos códigos de blocos lineares com o limite de quantidade máxima de dados de um canal estabelecido por Shannon.

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

2. FUNDAMENTAÇÃO TEÓRICA

O presente trabalho trata da construção de códigos corretores de erro, geralmente, utilizados em sistemas de comunicações digitais como o apresentado na Figura 1. Neste sistema, a informação a ser transmitida está sujeita a ação de um ruído, normalmente, AWGN (ruído branco gaussiano aditivo), que em geral ocasiona erros na transmissão da informação (*bits*). Neste caso, o objetivo do sistema de codificação, composto pelos blocos codificador e decodificador da Figura 1, é identificar e corrigir erros na transmissão da mensagem. Portanto, seu principal objetivo é diminuir a probabilidade média de erro de transmissão em sistemas de comunicações.

Neste trabalho, abordaremos apenas o processo de codificação, o qual insere redundância na palavra-código, objetivando a identificação correta da informação transmitida, mesmo que existam alguns erros na transmissão. Mais especificamente, foi considerada a classe de códigos corretores de erro denominada códigos bloco lineares, que é bastante utilizada nos sistemas de codificação convencionais, principalmente, àqueles que usam códigos Turbo para que seus desempenhos se aproximem do limitante de Shannon da capacidade de canal, [1].

O processo de codificação de canal consiste em transformar um bloco de informação com um tamanho de k símbolos em um bloco codificado com n símbolos, adicionando redundância de acordo com uma regra predefinida.

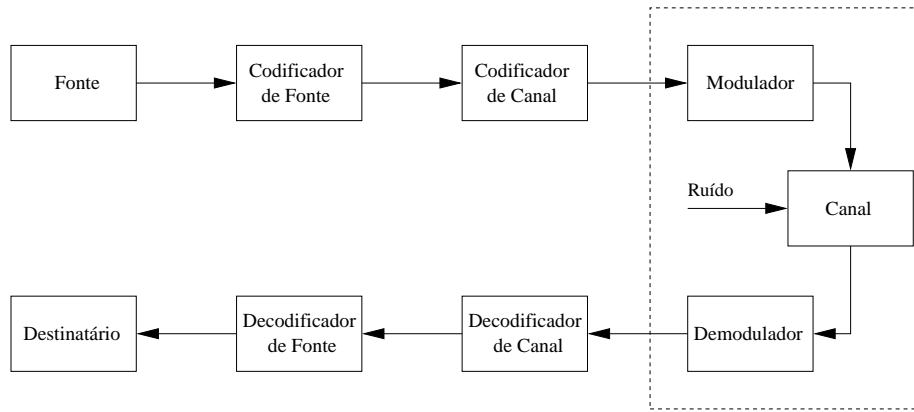


Figura 1. Diagrama de blocos de um sistema de comunicações digitais.

Para gerar um código de bloco (n, k) , por exemplo, o codificador de canal aceita informação em blocos sucessivos de k símbolos; para cada bloco o codificador adiciona $n - k$ símbolos redundantes que se relacionam algebricamente com os k símbolos de mensagem, produzindo assim um bloco codificado com n símbolos, onde $n > k$. O bloco de n símbolos denomina-se palavra-código e n , tamanho de bloco do código, onde a taxa de codificação $r = k/n$, com $0 < r < 1$.

Assim, para que o código possua uma estrutura sistemática, uma palavra código é dividida em duas partes, uma é constituída pelos símbolos de mensagem e a outra pelos símbolos de paridade.

Um código linear é gerado com base numa matriz geradora G . Neste caso, sendo \mathbf{m} o vetor que representa a mensagem a codificar, então as palavras-código, \mathbf{c} , podem ser obtidas por

$$\mathbf{c} = (\mathbf{m} * \mathbf{G}) \bmod q \quad (1)$$

No processo de decodificação usa-se uma matriz de verificação da paridade do código, \mathbf{H} , que permite verificar se existem erros na palavra recebida $\mathbf{r} = \mathbf{c} + \mathbf{e}$, através do cálculo da síndrome

$$\mathbf{s} = (\mathbf{r} * \mathbf{H}^T) \bmod q = (\mathbf{c} * \mathbf{H}^T + \mathbf{e} * \mathbf{H}^T) \bmod q = (\mathbf{e} * \mathbf{H}^T) \bmod q, \quad (2)$$

onde \mathbf{e} é o erro de transmissão no canal ruidoso.

Códigos poderosos exigem uma redundância elevada e, portanto, a taxa de transmissão de dados cai excessivamente. Assim, existe um compromisso entre a correção de erro e a taxa de transmissão.

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

$$\mathbf{N} = [n_1, n_2, \dots, n_m], \quad (\text{representação modular}) \quad (3)$$

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

Usando a representação modular (3), 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 \mathbf{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

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

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 $[(c_1, c_2), (c_1, c_3), (c_2, c_3) \text{ e } (c_3, c_4)]$ com distância Euclidiana 6, 2 combinações $[(c_1, c_4) \text{ e } (c_2, c_3)]$ com distância 8 e 4 combinações $[(c_0, c_1), (c_0, c_2), (c_0, c_3) \text{ e } (c_0, c_4)]$ com distância 10.

3. METODOLOGIA

Segundo [4] e [5], usando a representação modular (3) pode-se formular o problema de otimização linear inteira descrito por (5), cujas soluções fornecem o vetor \mathbf{N} de um código de bloco de taxa $r = k/n$ com d_{\min} máxima.

$$\begin{aligned} \text{Maximizar: } & z = w \\ \text{Sujeito a: } & \mathbf{N} \cdot \mathbf{C} \geq w\mathbf{1} \\ & \sum n_i = n \\ & n_i \geq 0, \text{ inteiros,} \end{aligned} \quad (5)$$

onde $\mathbf{1} = [1, 1, \dots, 1]^T$ 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 (5), como as colunas 5 e 10 e as colunas 6 e 9 em (4).

Neste trabalho, o problema de otimização (5) 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

$$\sum (a_i - \lfloor a_i \rfloor) n_i \geq b_k - \lfloor b_k \rfloor. \quad (6)$$

O Teorema Fundamental de Shannon demonstra a possibilidade do uso de codificação para controlar com eficiência a taxa de erro de um sistema de comunicação digital. A expressão 7 é utilizada.

$$\frac{E_b}{N_0} = \frac{2^{\frac{C}{B}} - 1}{\frac{C}{B}}, \quad (7)$$

onde, E_b/N_0 representa a relação entre a energia média por bit e a densidade de potência de ruído e C/B a eficiência de largura de faixa máxima. Um diagrama de eficiência de largura de faixa para vários valores de R/B em função de E_b/N_0 é utilizado. O limite de Shannon é uma espécie de parâmetro e tem como intuito, mostrar a capacidade de um canal de largura B tendendo ao infinito (bps) na presença do ruído Gaussiano aditivo branco com densidade espectral de potência $N_0/2$ (W/Hz).

4. ANÁLISE E INTERPRETAÇÃO DOS RESULTADOS

Inicialmente consideramos os códigos bloco lineares 5-ário com taxa $r = 1/n$ que foram obtidos com o auxílio de (4) e (5), como apresentado na Tabela 1.

Ainda considerando códigos sobre D_5 foram obtidos os seguintes códigos para $k = 2$:

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

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

- $r = 2/3, d_{min} = 2, \mathcal{D}(t) = 16t^2 + 60t^3 + 61t^4 + \dots e$

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

- $r = 2/4, d_{min} = 4, \mathcal{D}(t) = 48t^4 + 56t^5 + 48t^6 + \dots e$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 3 & 4 \end{bmatrix}.$$

- $r = 2/5, d_{min} = 5, \mathcal{D}(t) = 80t^5 + 40t^6 + 60t^7 + \dots e$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 4 & 3 & 2 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}. \quad (8)$$

- $r = 2/6, d_{min} = 6, \mathcal{D}(t) = 11t^6 + 36t^7 + 53t^8 + \dots e$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 2 & 4 & 3 \\ 0 & 1 & 3 & 3 & 3 & 4 \end{bmatrix}.$$

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 $\mathcal{D}(t) = 16t^2 + 14t^3 + 2t^5 + \dots e \mathcal{D}(t) = 8t^4 + 44t^6 + 4t^7 + \dots$, respectivamente. Entretanto, quando a taxa é igual a $2/5$ os seguintes parâmetros foram obtidos: $d_{min} = 7, \mathcal{D}(t) = 37t^7 + 10t^8 + 5t^9 + \dots e$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 4 & 2 & 4 \\ 0 & 1 & 2 & 4 & 4 \end{bmatrix}. \quad (9)$$

Por fim, os seguintes códigos sobre F_7 com máxima d_{min} euclidiana foram construídos para $k = 2$:

- $r = 2/3, d_{min} = 3, \mathcal{D}(t) = 120t^3 + 150t^4 + \dots e$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 3 \end{bmatrix}.$$

- $r = 2/4, d_{min} = 5, \mathcal{D}(t) = 88t^5 + 207t^6 + \dots e$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 4 & 5 \end{bmatrix}.$$

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 $\mathcal{D}(t) = 30t^3 + 3t^4 + 93t^5 + \dots$ para $r = 2/3$ e $\mathcal{D}(t) = 3t^6 + 91t^7 + t^8 + \dots$ 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 três erros.

Na etapa de simulação computacional consideramos um esquema de modulação 5-ASK sujeito a ação de um ruído AWGN como ilustra a Figura 2(a). Neste caso, utilizamos o modelo de um canal discreto sem memória 5-ário, como apresentado na Figura 2(b).

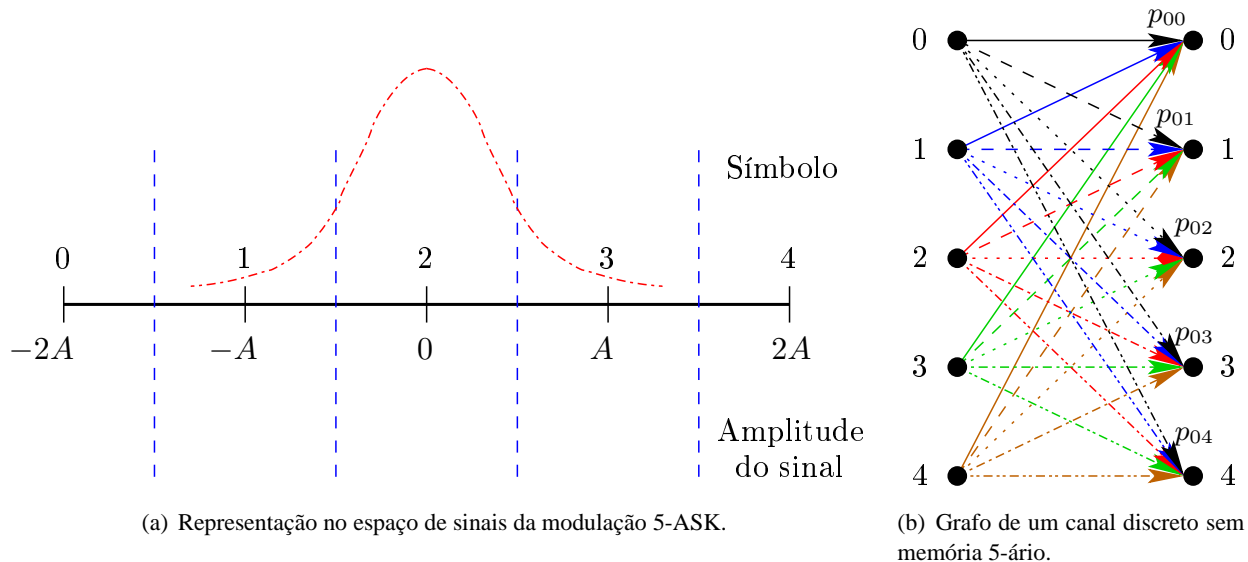


Figura 2. Representação do canal e do esquema de modulação do sistema de comunicações utilizado na simulação computacional.

Na simulação utilizamos a matriz de probabilidade de transição P para representar o canal discreto sem memória 5-ário, dada por

$$P = \begin{bmatrix} p_{00} & p_{01} & p_{02} & p_{03} & p_{04} \\ p_{10} & p_{11} & p_{12} & p_{13} & p_{14} \\ p_{20} & p_{21} & p_{22} & p_{23} & p_{24} \\ p_{30} & p_{31} & p_{32} & p_{33} & p_{34} \\ p_{40} & p_{41} & p_{42} & p_{43} & p_{44} \end{bmatrix} \quad (\text{Simétrica}).$$

Como o ruído no canal de transmissão é AWGN, alguns exemplos de probabilidades de transição podem ser determinadas por

$$p_{00} = \frac{1}{2} + \int_0^{A/2} \frac{1}{\sqrt{2\pi}\sigma} e^{-x^2/2\sigma^2} dx = \frac{1}{2} + \frac{1}{2} \text{erf} \left(\frac{\sqrt{2}A}{4\sigma} \right)$$

$$p_{01} = \frac{1}{2} + \int_{A/2}^{3A/2} \frac{1}{\sqrt{2\pi}\sigma} e^{-x^2/2\sigma^2} dx = \frac{1}{2} \text{erf} \left(\frac{3\sqrt{2}A}{4\sigma} \right) - \frac{1}{2} \text{erf} \left(\frac{\sqrt{2}A}{4\sigma} \right)$$

$$p_{11} = \frac{1}{2} + \int_{-A/2}^{A/2} \frac{1}{\sqrt{2\pi}\sigma} e^{-x^2/2\sigma^2} dx = \text{erf}\left(\frac{\sqrt{2}A}{4\sigma}\right),$$

onde $\text{erf}(z)$ é a função erro definida como

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt.$$

No caso, os códigos utilizados para a simulação foram os códigos (8) e (9) com $d_{\min} = 5$ (Euclidiana) e $d_{\min} = 7$ (Euclidiana ao quadrado), respectivamente. Com isso, a probabilidade média erro de símbolo transmitido para o código 1 é dado por

$$P_{e1} = p^5 - 5p^4q - 10p^3q^2 - 10p^2q^3,$$

onde os valores de p e q são obtidos das probabilidades de transição como segue

$$p = \frac{1}{5} + \frac{4}{5}\text{erf}\left(\frac{\sqrt{2}A}{4\sigma}\right) \quad \text{e} \quad q = \frac{4}{5} \left[\text{erf}\left(\frac{3\sqrt{2}A}{4\sigma}\right) - \text{erf}\left(\frac{\sqrt{2}A}{4\sigma}\right) \right].$$

Além disso, a probabilidade média erro de símbolo transmitido para o código 2 é dado por

$$P_{e1} = p^5 - 5p^4q - 10p^3q^2 - 5p^4s,$$

onde os valores de p e q foram obtidos anteriormente e s é dado por

$$s = \frac{3}{5} \left[\text{erf}\left(\frac{5\sqrt{2}A}{4\sigma}\right) - \text{erf}\left(3\frac{\sqrt{2}A}{4\sigma}\right) \right].$$

A Figura 3 apresenta as curvas de desempenho do sistema de comunicação usando os códigos 1 e 2. Neste caso, utilizamos a relação sinal ruído $\text{SNR} = 10 \log_{10}(\overline{E}_m/\mathcal{N})$, onde $E_m = 2A^2$ é a energia média da transmissão e $\mathcal{N} = \sigma^2$ é a energia média de ruído. Com isso, note que o código 2 é que apresenta o melhor desempenho para uma determinada SNR, ou equivalente, um ganho de 2.3 dB para uma probabilidade média de erro de símbolo fixa. Tal resultado era esperado, visto que a distância mínima desse código é maior do que a do código 1.

5. CONCLUSÃO

Os códigos com máxima distância d_{\min} Euclidiana e Euclidiana ao quadrado construídos apresentaram probabilidade de erro de bit menor e valores de d_{\min} maiores do que se a medida de distância fosse por exemplo a distância de *Hamming*. O método do plano de corte aplicado na resolução do problema de otimização demonstrou ser adequado além de que a elaborada técnica de codificação permitiu uma aproximação maior do limite estabelecido por Shannon.

AGRADECIMENTOS

Os autores agradecem a FAPESB e ao CNPq pela bolsa de iniciação científica fornecida no período de desenvolvimento desse trabalho, e ao Centro Federal de Educação Tecnológica que proporcionou a apresentação deste artigo.

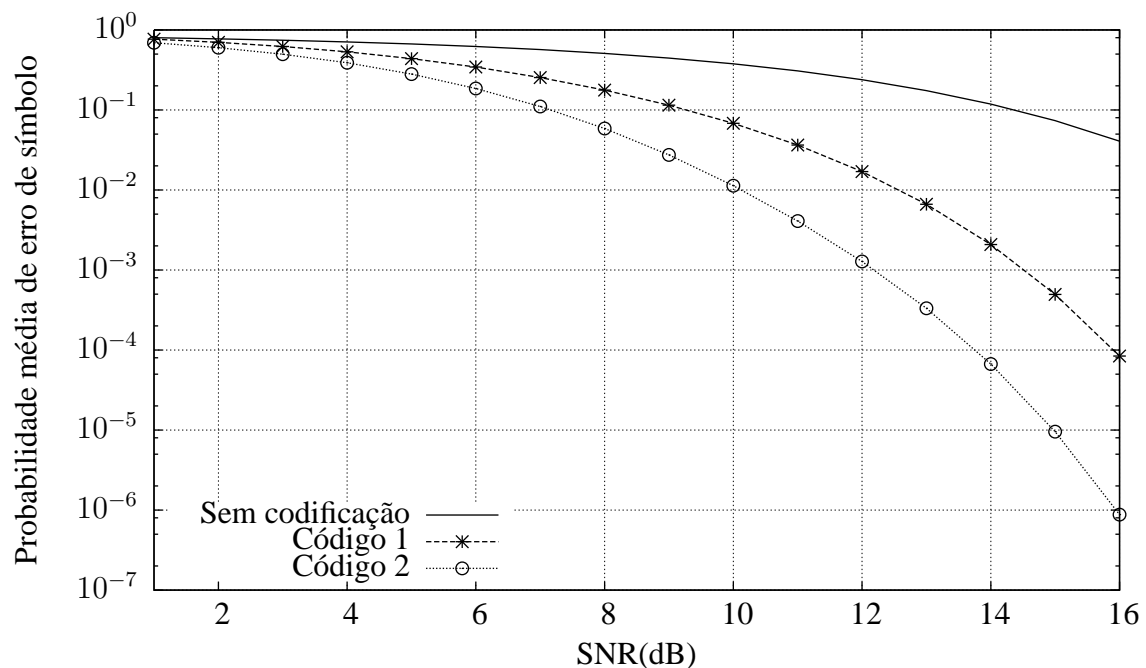


Figura 3. Curvas de desempenho de sistemas de codificação usando códigos de taxa $r = 2/5$ em F_5 , sendo que o código 1 possui distância mínima Euclidiana igual a 5 e o código 2 possui distância mínima Euclidiana ao quadrado igual a 7.

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 Wiley and 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 F_q com d_{min} máxima usando programação linear inteira", *XXII Simpósio Brasileiro de Telecomunicações-SBrT'05*, Campinas, 2005.
- [5] R. A. Oliveira, e R.G. Cavalcante, "Exemplos de códigos de Bloco Lineares 5 e 7-ários com máxima distância euclidiana", *XXVI Simpósio Brasileiro de Telecomunicações-SBrT'08*, Rio de Janeiro, RJ 2008.