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

Extensão de Galois $GF(2^5)$ aplicada na Obtenção de um Polinômio Gerador em um Código BCH

Bianca Lapa Ribeiro[1]
Discente do Curso de Matemática-Licenciatura, UNIFAL-MG, Alfenas-MG
Maria Flávia Maciel Santiago[2]
Discente do Curso de Matemática-Licenciatura, UNIFAL-MG, Alfenas-MG
Letícia Ribeiro Pereira[3]
Discente do Curso de Matemática-Licenciatura, UNIFAL-MG, Alfenas-MG
Anderson José de Oliveira[4]
Docente do Curso de Matemática-Licenciatura, UNIFAL-MG, Alfenas-MG

Em um processo de transmissão da informação podem ocorrer uma série de interferências que dificultam o entendimento dos dados enviados. Podemos considerar que um sistema de comunicação é um conjunto de mecanismos que possibilita a transmissão da informação de um transmissor para um determinado receptor, por meio de um canal de comunicação, sendo desejável que essa transmissão seja efetuada com alta confiabilidade, permitindo que a mensagem recebida seja igual a original, portanto, existe uma grande preocupação em relação ao controle de perturbações.

Os códigos corretores de erros (CCE's) são capazes de detectar e corrigir erros que podem surgir durante os processos de transmissão ou armazenamento de informações, a fim de garantir sua confiabilidade. Pode-se destacar uma classe importante dos CCE's, que são os códigos BCH (Bose, Chaudhuri e Hocquenghem) [2]. Eles são uma extensa família de códigos cíclicos com uma alta capacidade de correção de erros. Esses códigos são uma extensão dos códigos de Hamming para correção de erros múltiplos. Por ser uma classe dos códigos cíclicos permite uma representação em termos de polinômios, o que simplifica os processos de codificação e decodificação dos códigos BCH [2].

Além da sua simplicidade nos processos de codificação e decodificação, possuem forte estrutura matemática em sua construção, onde são utilizados corpos finitos e admitem uma representação em termos de polinômios sobre extensões de $\mathbb{Z}_2$ [3]. Podem ser utilizados no contexto biológico, pois são eficientes na detecção e correção de possíveis erros (mutações) que podem surgir no processo de transmissão e/ou armazenamento de informações genéticas, conforme apontado nos trabalhos de [1] e [4].

Em [4] propõe-se a análise de sequências de DNA, utilizando os códigos BCH, por meio de dois algoritmos e suas implementações em dois programas computacionais distintos. Esses programas calculam polinômios geradores, identificam palavras-códigos em sequências de DNA e realizam o processo de decodificação, sendo capazes de encontrar mutações na estrutura do DNA.

O objetivo deste trabalho é apresentar a construção do polinômio gerador de um código BCH com capacidade de correção de cinco erros a partir da extensão $GF(2^5)$, gerada pelo polinômio primitivo $p(X) = 1 + X^2 + X^5$.

[1]bianca.ribeiro@sou.unifal-mg.edu.br
[2]maria.santiago@sou.unifal-mg.edu.br
[3]leticia.pereira@sou.unifal-mg.edu.br
[4]anderson.oliveira@unifal-mg.edu.br

Os resultados apresentados neste trabalho foram desenvolvidos em um projeto de iniciação científica, que ainda está em desenvolvimento, realizado por meio de seminários virtuais, devido à pandemia de Covid-19.

Em um código BCH, os corpos de Galois representam a estrutura básica em seu processo de construção [3]. Efetuamos o cálculo de um polinômio gerador do código BCH com capacidade de correção de cinco erros a partir da extensão $GF(2^5)$, gerada pelo polinômio primitivo $p(X) = 1 + X^2 + X^5$. Primeiramente, admitindo que α seja uma raíz desse polinômio, determinamos todos elementos de $GF(2^5)$ gerados por $p(X) = 1 + X^2 + X^5$. Em seguida, encontramos as raízes conjugadas, através de β^{2^l}, com $l \geq 0$ e construímos os polinômios mínimos referentes à essas raízes conjugadas, por meio de um produtório. Para obter o polinômio gerador, dado por $g(X) = MMC\{\phi_1(X), \phi_3(X), ..., \phi_{2t-1}(X)\}$, efetuamos o produto dos polinômios mínimos $\phi_1(X)$, $\phi_3(X)$, ..., $\phi_{2t-1}(X)$, encontrados anteriormente.

Neste caso, o polinômio gerador pode ser descrito da seguinte forma:

$$g(X) = MMC\{\phi_1(X), \phi_3(X), \phi_5(X), \phi_7(X)\} \tag{1}$$

$$g(X) = (X^5+X^2+1)\cdot(X^5+X^4+X^3+X^2+1)\cdot(X^5+X^4+X^2+X+1)\cdot(X^5+X^3+X^2+X+1) \tag{2}$$

Então, obtemos:

$$g(X) = X^{20} + X^{18} + X^{17} + X^{13} + X^{10} + X^9 + X^7 + X^6 + X^4 + X^2 + 1 \tag{3}$$

gerando um código BCH cíclico com $d_{min} \geq 11$, onde d_{min} representa a distância mínima do código. Conseguimos estabelecer uma relação entre o grau do polinômio gerador e os parâmetros do código BCH. Dado o polinômio gerador $g(X)$ e sendo seu grau $gr(g(X)) = 20$, podemos encontrar os parâmetros do código BCH com capacidade de correção de cinco erros através da seguinte igualdade: $gr(g(X)) = n - k$. O parâmetro n de um código BCH (n, k) é dado por $n = 2^m - 1$. Sabemos que $m = 5$, pois o código é gerado por $p(x) = 1+X^2+X^5$ a partir de $GF(2^5)$. Com isso, $n = 2^m-1 \Rightarrow n = 2^5-1 \Rightarrow n = 31$. Como $gr(g(X)) = n-k \Rightarrow 20 = n-k \Rightarrow 20 = 31-k \Rightarrow k = 11$. Portanto, o código em questão é o código BCH$(31, 11)$.

Agradecimentos

Agradecemos à Unifal-MG pela oportunidade de desenvolvimento deste trabalho.

Referências

[1] Faria, L. C. B. Existências de Códigos Corretores de Erros e Protocolos de Comunicação em Sequências de DNA, Tese de Doutorado, Faculdade de Engenharia Elétrica e de Computação, Unicamp, 2011.

[2] Lin, S. and Costello Jr., D. J. *Error Control Coding. 2nd ed.* Prentice Hall, 2004.

[3] Marcet, A. P. Códigos Corretores de Erros BCH: Uma Aplicação de Polinômios em Corpos Finitos, Dissertação de Mestrado, Faculdade de Formação de Professores,Universidade do Estado do Rio de Janeiro, São Gonçalo, 2019.

[4] Pereira, D. G. Uma Abordagem Computacional para a Análise de Sequências de DNA por meio dos Códigos Corretores de Erros, Dissertação de Mestrado, Faculdade de Engenharia Elétrica e de Computação, Unicamp, 2014.