Construção e Análise de Desempenho de uma Classe de Códigos LDPC Irregulares e Estruturados Definidos sobre Campos Finitos de Inteiros

Pâmela Joyce Silva Melo Dantas e Renato Baldini Filho

***Resumo*— Este artigo apresenta um método de construção e analise de desempenho de uma classe de códigos LDPC (*Low Density Parity Check*) irregulares estruturados definidos sobre os campos finitos de inteiros Z_p, sendo p um número primo maior que 2. A constelação da modulação PSK (*phase-shift keying*) p-ária é utilizada como base para a alocação dos símbolos de Z_p. O desempenho destes códigos LDPC é avaliado em um canal perturbado por ruído aditivo gaussiano branco.**

Palavras-Chave*—*Códigos LDPC não binário, Códigos LDPC sobre campos de inteiros finitos.

Abstract—**This paper presents a method of construction and performance analysis of a class of irregular structured LDPC codes *(Low Density Parity Check)* defined over a finite integer field Z_p, where p is a prime number greater than 2. The symbols of Z_p. are mapped to the symbols of a p-ary PSK *(Phase -shift keying)* constellation. The performance of those LDPC codes is evaluated on an additive white Gaussian noise channel.**

***Keywords*— *non-binary LDPC codes, LDPC defined over finite fields of interger* .**

I. INTRODUÇÃO

Códigos LDPC binários são códigos de bloco lineares longos construídos através da concepção de uma matriz de verificação de paridade **H** esparsa (quantidade de 1's nas linhas e colunas muito pequena quando comparado à quantidade de 0's). Estes códigos associados a um método de decodificação iterativa podem alcançar um desempenho perto do limite ideal de Shannon sobre o canal com ruído gaussiano branco aditivo (*additive white gaussian noise* - *AWGN*)[1] .

É bem conhecido que para melhorar o desempenho da taxa de erro de bit (*bit error rate* - *BER*) de um processo de codificação/descodificação binário é necessário diminuir a taxa de codificação do código, ou de forma equivalente, aumentar o número de bits de redundância da palavra código. Entretanto, existe outra maneira de aumentar a eficiência do processo de codificação/decodificação sem aumentar o comprimento da palavra código. Isto pode ser feito aumentando-se o tamanho do alfabeto utilizado na definição do código.

Códigos LDPC não binários, definidos sobre anéis ou campos (corpos) de inteiros finitos, são candidatos naturais a este papel de alternativa aos códigos LDPC binários. Além disso, estes códigos LDPC apresentam algumas características interessantes, tais como: o perfeito casamento com os símbolos da modulação p-PSK e podem ser feitos facilmente invariantes a rotações de fase da portadora.

Este artigo apresenta um método de construção de uma classe de códigos LDPC definidos sobre campos finitos Z_p, onde p é um número primo maior que 2. Os símbolos de Z_p são mapeados nos símbolos da modulação p-PSK.

Em geral, os códigos de LDPC podem ser definidos como códigos regulares ou irregulares. Um código LDPC é regular, se os pesos de Hamming de todas as linhas e de todas as colunas na sua matriz **H** de verificação de paridade são iguais, respectivamente. Caso contrário, o código é denominado irregular. Os códigos LDPC irregulares apresentam melhor desempenho do que os seus equivalentes regulares [2].

O desempenho dos códigos LDPC propostos são obtidos por simulação de Monte Carlo em um canal com ruído aditivo gaussiano branco (AWGN) e comparados com seus equivalentes binários.

Os algoritmos de decodificação iterativos para códigos LDPC são delimitados por um compromisso entre o desempenho, em termos de taxa de erro de bit (*BER*), e a sua complexidade de decodificação. Além disso, o desempenho do código LDPC varia de acordo com o comprimento das palavras código e o tipo de estrutura da sua matriz de verificação de paridade. O algoritmo de decodificação iterativo utilizado neste artigo é o algoritmo soma-produto (SP) que alcança o melhor desempenho, embora exija uma complexidade mais elevada de implementação.

II. CONSTRUÇÃO DE CÓDIGOS LDPC SOBRE Z_P

Os códigos (n, k) LDPC binários, irregulares e estruturados (IE) são construídos utilizando uma matriz de verificação de paridade **H** de dimensões (n-k, n), onde n e k são o comprimento da palavra código $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ e o do vetor de informação $\mathbf{u} = (u_1, u_2, \ldots, u_k)$, respectivamente. Esta matriz **H** é gerada pelo agrupamento de submatrizes circulantes de dimensão $m \leq n$-k [3],[4]. Submatrizes circulantes são geradas por deslocamentos cíclicos à direita

Pâmela J. S. M. Dantas e Renato Baldini Filho, Departamento de Comunicações, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas-SP. E-mails: pamela@decom.fee.unicamp.br, baldini@decom.fee.unicamp.br. Este trabalho foi parcialmente financiado pela CAPES.

das colunas de uma matriz identidade $\mathbf{I}_m$ de ordem m [5]. O deslocamento das colunas da submatriz circulante em relação a matriz identidade $\mathbf{I}_m$ é definida por um número primo menor que m. Isto permite que a matriz $\mathbf{H}$ gerada não tenha *girths* pequenos.

A Figura 1 mostra dois exemplos de submatrizes circulantes $\mathbf{C}_{8,j}$, obtida a partir da matriz de identidade $\mathbf{I}_8$. O índice j indica o deslocamento inicial para a direita da primeira linha da matriz de identidade.

$$\mathbf{I}_8=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix}\quad \mathbf{C}_{8,3}=\begin{bmatrix}0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\\1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\end{bmatrix}\quad \mathbf{C}_{8,5}=\begin{bmatrix}0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\\1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\end{bmatrix}$$

Fig.1 Submatrizes circulantes obtidas a partir I_8.

Códigos LDPC irregulares estruturados definidos sobre campos finitos de inteiros Z_p são construídos de maneira análoga aos binários, a diferença está nas submatrizes circulantes que, apesar de serem geradas por deslocamentos cíclicos da matriz identidade, são multiplicadas por um símbolo do campo Z_p.

A Figura 2 mostra um exemplo simples de geração de uma matriz $\mathbf{H}(32, 16)$ para um código estruturado irregular definido sobre o campo Z_5. A matriz $\mathbf{H} = [\mathbf{I} \mid \mathbf{P}]$ está na forma sistemática, onde $\mathbf{P}$ é a submatriz de paridade construída por agrupamento de quatro submatrizes $C_{m,j}^{x}$ circulantes definidas por quatro elementos primos j, sem repetição, do conjunto de números primos N_p = {2, 3, 5, 7} menores que m = 8 e $x \in Z_5$. Esta matriz $\mathbf{H}$ proporciona um rápido processo de codificação, o que reduz a complexidade de decodificação [3].

$$\mathbf{H}=\left[\mathbf{I}_{16}\;\middle|\;\begin{matrix}C_{8,2}^{1} & C_{8,3}^{3}\\ C_{8,5}^{2} & C_{8,7}^{2}\end{matrix}\right]$$

$$\mathbf{H}=\left[\begin{array}{c|c|c}
1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,1\,0\,0\,0\,0\,0 & 0\,0\,0\,3\,0\,0\,0\,0\\
0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,0\,0\,0\,0 & 0\,0\,0\,0\,3\,0\,0\,0\\
0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,0\,0 & 0\,0\,0\,0\,0\,3\,0\,0\\
0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,3\,0\\
0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,3\\
0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1 & 3\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,0\,0\,0\,0\,0\,0\,0 & 0\,3\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,1\,0\,0\,0\,0\,0\,0 & 0\,0\,3\,0\,0\,0\,0\,0\\
\hline
0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,2\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,2\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,2\,0 & 2\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,2 & 0\,2\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 & 2\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,2\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0 & 0\,2\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,2\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0 & 0\,0\,2\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,2\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 & 0\,0\,0\,2\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,2\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,2\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,2\,0
\end{array}\right]$$

Fig. 2 Matriz $\mathbf{H}$ (32,16) código LDPC não binário irregular estruturado para um campo Z_5.

Note que existem outras maneiras de estruturar a submatriz $\mathbf{P}$ através do agrupamento de submatrizes $C_{m,j}^{i}$ utilizando diferentes valores para m.

A matriz geradora $\mathbf{G} = [-\mathbf{P}^T \mid \mathbf{I}]$ do código LDPC é obtida através da matriz de verificação de paridade $\mathbf{H}$ na sua forma sistemática, onde o expoente T significa transposta.

Cada um dos símbolos codificados c_i pertencente a Z_p é associado a um dos sinais p-PSK dados pela equação

$$s_i(t) = A\exp j\left(\frac{2\pi}{p}c_i + \varphi\right) \qquad (1)$$

onde $A=\sqrt{E_s}$ é a amplitude do sinal de modulação, E_s é a energia deste sinal e φ é uma fase aleatória da modulação. Para efeitos de análise de desempenho dos códigos, sem perda de generalização, esta fase φ é feita igual a zero.

A Figura 3 apresenta dois exemplos de modulação p-PSK utilizadas para transmitir os códigos LDPC definidos sobre campos não binários [6]. Como geralmente a saída da fonte de informação é binária, seus bits são mapeados em símbolos de Z_p utilizando codificação de Gray. A codificação de Gray associada à modulação minimiza a probabilidade de erro de bit no processo de decodificação, pois um erro em um símbolo de informação para seu adjacente produz um único bit errado. O mapeamento da sequência binária (representada entre parênteses) em símbolos de Z_p é apresentado para as modulações 3-PSK e 5-PSK. Note que alguns símbolos de Z_p não possuem bits atribuídos. Estes símbolos são usados apenas como redundância no processo de codificação [7].

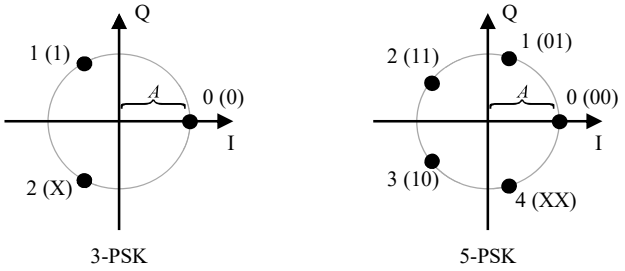

Fig. 3 Modulação p-PSK, p = 3 e 5, com mapeamento de binário para Z_p utilizando código de Gray.

Note que, devido ao mapeamento de Gray das sequências binárias da fonte em símbolos do campo Z_p, um ou mais símbolos de Z_p não são gerados na entrada no codificador, mas são utilizados na geração dos símbolos de paridade. Então, na entrada do codificador temos q (uma potência de 2 imediatamente menor que número primo p) possibilidades de símbolos a cada instante. Assim, podemos definir a taxa R_c de codificação de um código LDPC (n, k) irregular estruturado sobre Z_p por

$$R_c = \frac{\log q^k}{\log q^k + \log p^{n-k}} = \frac{k\log q}{k\log q + (n-k)\log p}. \qquad (2)$$

O processo de decodificação iterativo é baseado numa generalização do algoritmo soma-produto binário para operar com símbolos de Z_p. A diferença é que a cada transição de um nó de paridade para um nó de variável e vice-versa, existe uma probabilidade associada para cada elemento de Z_p. No final de

uma iteração, uma possível palavra de código $\hat{\mathbf{c}}$ é estimada e a sua síndrome é avaliada. Se a síndrome é nula a palavra código estimada $\hat{\mathbf{c}}$ é decodificada. Caso contrário, os passos vertical e horizontal do algoritmo são repetidos. O processo é interrompido, quando uma palavra de código é detectada, ou quando o número máximo de iterações é alcançado.

III. Modelo do Sistema de Comunicação

A Figura 4 apresenta o modelo de comunicação utilizado para analisar o desempenho dos códigos LDPC irregulares estruturados sistemáticos construídos sobre campos de inteiros finitos Z_p. A sequência de informação **u** q-ária é modulada por um modulador q-PSK e enviada ao canal, sendo que ao mesmo tempo, ela é codificada por um código LDPC onde só a parte de paridade **p** p-ária é gerada e modulada por um modulador p-PSK, que em seguida, é concatenada a **u**.

Por exemplo, para p = 5, os símbolos de informação são mapeados na modulação 4-PSK e os símbolos de paridade na modulação 5-PSK, dessa forma, obtemos um melhor desempenho dos códigos LDPC sobre Z_5.

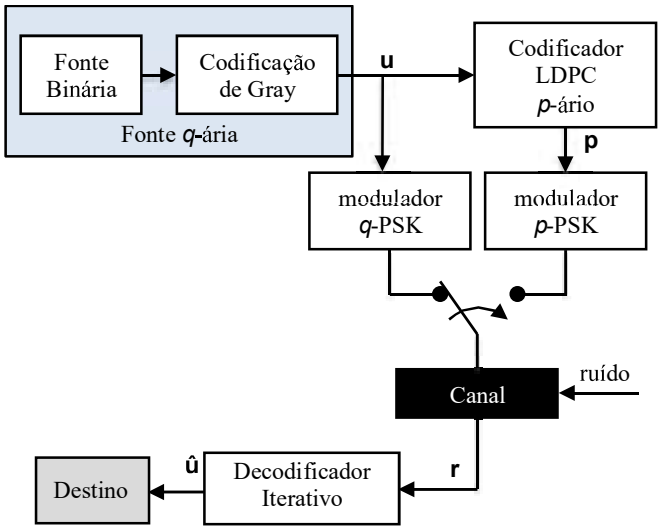

Fig. 4 Diagrama de Blocos do Modelo de Comunicação utilizado para avaliar o desempenho dos Códigos LDPC p-ário.

A sequência **r** formada pela justaposição de **u** e **p** somada ao ruído **w**, chega ao receptor, onde é decodificada iterativamente e uma estimação **û** da sequência de informação é obtida e entregue ao usuário.

IV. Resultados

Nesta seção é apresentada uma análise comparativa do desempenho de códigos LDPC-IE definidos sobre Z_3 e Z_5, em relação aos códigos LDPC-IE binários equivalentes. Foram utilizadas matrizes de verificação de paridade dos códigos para comprimentos n = 500 e n = 1000 símbolos e dimensões $m = (n\text{-}k)/2$ e $m = (n\text{-}k)/5$, o limite no número de iterações para a decodificação iterativa foi fixado em 5, as simulações foram feitas em um canal AWGN.

A Figura 5 mostra o desempenho, em termos de taxa de erro de bit (*BER*) pela razão energia de bit (E_b) pela densidade espectral de potência unilateral de ruído (N_0), dos códigos LDPC-IE binário, sobre Z_3 e sobre Z_5. Os dois primeiros códigos possuem n =1000 e k = 500 símbolos e a dimensão das submatrizes circulantes igual a 250. O código LDPC-IE definido sobre Z_5 possui n = 500 e k = 250 símbolos e dimensão das submatrizes circulantes igual a 125. Estes parâmetros foram escolhidos para que os três códigos sejam equivalentes.

A matriz **H** (500, 250), gerada a partir de submatrizes $C_{125,j}^{i}$ para o código LDPC-IE sobre Z_5, é definida da seguinte maneira:

$$\mathbf{H} = \left[\mathbf{I}_{250} \;\middle|\; \begin{matrix} C_{125,2}^{1} & C_{125,3}^{3} \\ C_{125,5}^{3} & C_{125,7}^{1} \end{matrix}\right]. \tag{3}$$

Enquanto que a matriz **H** para o código LDPC-IE (1000, 500) sobre Z_3 é gerada utilizando submatrizes circulantes $C_{250,j}^{i}$,

$$\mathbf{H} = \left[\mathbf{I}_{500} \;\middle|\; \begin{matrix} C_{250,2}^{1} & C_{250,3}^{1} \\ C_{250,5}^{1} & C_{250,7}^{1} \end{matrix}\right]. \tag{4}$$

O desempenho do código LDPC-IE definido sobre Z_5 para uma *BER* igual a 5×10^{-5}, apresenta E_b/N_0, em torno de 1 dB pior que o código binário equivalente. Enquanto que, o código LDPC-IE definido sobre Z_3, para uma *BER* igual a 3×10^{-3}, tem um desempenho em termos de Eb/N_0 de 3,5 dB pior que o equivalente binário.

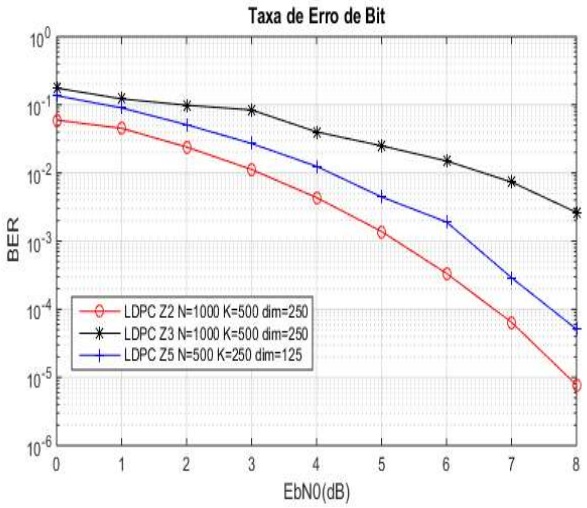

Fig. 5 Desempenho dos códigos LDPC-IE (500, 250, 125) para código Z_5 e LDPC-IE (1000, 500, 250) para o código binário e Z_3.

A Figura 6 apresenta uma comparação de desempenho dos códigos LDPC-IE equivalentes binário, definido sobre Z_3 e sobre Z_5. A matriz de verificação de paridade **H** do código LDPC-IE (500, 250) definido sobre Z_5 é gerada a partir de submatrizes circulantes de dimensão 50. As matrizes **H** dos códigos LDPC-IE (1000, 500) binário e definido sobre Z_3 são geradas a partir de submatrizes circulantes de dimensão igual a 100. Note que o desempenho do código LDPC-IE definido sobre Z_5 se torna melhor que o equivalente binário a partir de uma *BER* igual a 6×10^{-4}.

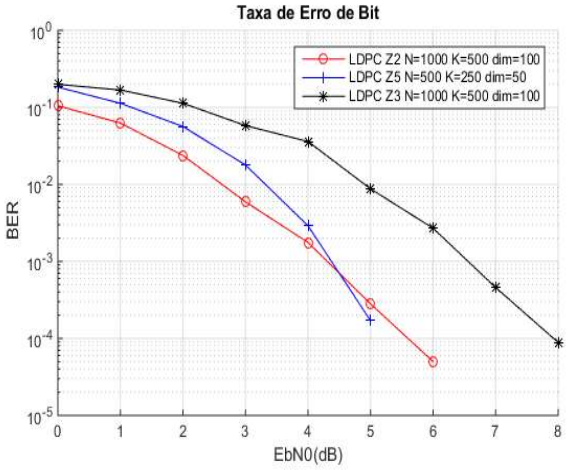

Fig. 6 Desempenho dos códigos LDPC-IE (500, 250, 50) para código Z_5 e LDPC-IE (1000, 500, 100) para o código binário e Z_3.

Note que, em ambas as Figuras 5 e 6, o desempenho do código LDPC-IE definido sobre Z_3 não apresenta desempenho melhor que seu binário equivalente. Entretanto, à medida que o número de submatrizes circulantes aumenta na matriz **H**, o código definido sobre Z_3 se aproxima do binário equivalente. Esta aproximação é mais evidente para a constelação Z_5.

V. Conclusão

Neste artigo apresentamos um método de construção de códigos LDPC-IE definidos sobre campos finitos de inteiros e uma análise do desempenho desses códigos com relação aos códigos LDPC binários equivalentes.

Dentre os códigos LDPC-IE analisados, o que apresentou melhor desempenho em comparação com o código LDPC binário equivalente foi o código definido sobre o campo Z_5 LDPC-IE (500, 250) gerado a partir de submatrizes circulantes de ordem igual a 50. Isso se deve ao fato de que quanto menor a ordem das submatrizes, maior é o número de submatrizes e consequentemente maior é a quantidade de elementos não nulos por linha e coluna, dessa forma, a quantidade de nós de variavel e nós de paridade aumentam. Entretanto, o processo de decodificação do códigos LDPC não binários apresentam uma complexidade maior devido ao maior número de operações que eles realizam. Por outro lado, os códigos LDPC-IE definidos sobre Z_5 apresentam menor comprimento das palavras código que seus equivalentes binários. Assim, os códigos LDPC definidos sobre campos finitos de inteiros podem ser uma alternativa aos códigos binários.

Referências

[1] Shannon, C. E., *A Mathematical Theory of Communications.* BSTJ, 27:379-423, Sep. 1948.

[2] Richardson, T. J. and Urbanke R. L., *"The capacity of low-density parity-check codes under message-passing decoding",* IEEE Trans. Inf. Theory, vol. 47, pp. 559-618, Feb. 2001.

[3] Jobes, M., *A VLSI Architecture and the FPGA Implementation for multi-rate LDPC Decoding,* MSc thesis, Mcmaster University, 2009.

[4] Karkooti, M., *Semi-Parallel Architectures for Real-Time LDPC Coding,* MSC thesis, rice University, 2004.

[5] de Lucena, A. U. *A Study on VHDL Implementation of a Class of Irregular Structured LDPC Codes applied to 100 GBPS Optical Networks,* 7th Latin American Workshop on Communications – Arequipa-Peru, 2015.

[6] Baldini F., R. and Farrell P. G., *"Coded modulation based on rings of integers modulo-q, Part I: block codes"*, *IEE Proc.-Commun*., vol. 141, no. 3, pp. 129–136, Jun.1994.

[7] Dantas, P. J. S. M. *Códigos LDPC definidos sobre corpos de inteiros finitos,* Dissertação de Mestrado, Unicamp, Campinas, 2014.

[8] Sridhara and Fuja T. E., *"LDPC codes over rings for PSK modulation"*, *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3209-3220, Sep. 2005.

[9] Ryan, W. E. and Lin., S., *Channel Codes Classical and Modern.* Cambridge University Press, 2009.