Performance analysis of Non Binary LDPC Code over its Binary Counterpart Using Progressive Edge Growth Algorithm

Ambar Bajpai, Muhammad Saadi, Tharathorn Phromsa-ard, Lunchakorn Wuttisittikulkij
Department of Electrical Engineering,
Chulalongkorn University
Bangkok, Thailand
ambarbajpai@gmail.com

Piya Kovintavewat
Data Storage Technology Research Center
Nakhon Pathom Rajabhat University
Nakhon Pathom, Thailand

***Abstract*—Active research has been carried out in the domain of channel coding in order to achieve the Shannon limit. This paper presents the performance analysis of binary and non-binary low-density parity-check (LDPC) codes for various Galois Field. Performance comparison has been made for non-binary LDPC and its binary counterpart by applying Progressive Edge Growth (PEG) algorithm. Decoding is based on belief propagation and Fast Fourier Transform (FFT) based belief propagation for binary and non-binary LDPC codes, respectively. Simulation results indicate that the non-binary LDPC code outperforms its binary counterpart significantly.**

Keywords—Galois filed (GF), Progressive Edge Growth (PEG), Shannon Limit

I. BACKGROUND

In 1948, Claude E. Shannon published his work on a channel capacity limit, which imposed the limit on reliable transmission of data over unreliable channels [1]. Since then various efforts have been made to achieve this limit but not yet realized. Channel codes, which tends to approach the Shannon capacity, are very useful in modern communication engineering but Shannon's theorem is non-constructive and do not give any clue about how to construct such codes. Furthermore, even if an oracle gives a sequence of codes that can achieve the capacity limit for a certain code rate, efficient decoding still remains a big challenge [4]. The fundamental bounds on channel capacity have been known for many years, where only a turbo code [2] and a low-density parity-check (LDPC) code [3][4] have realized a performance close to the capacity with the requirement that the code length (or data size) must approaches infinity. Therefore, it can be safely stated that there is a wide room for the researches in this area, especially on finite length codes and efficient decoding.

II. INTRODUCTION

Many researchers have been carried out on channel coding since Shannon introduced a theory of mathematical constraints for channel capacity. Currently, special focus has been given to a non-binary LDPC code, which is a derivative of a binary LDPC over Galois field GF(q), where $q = p^m$,p is prime number and m is a positive integer [5]. Various standards such as IEEE 802.11n, WiMAX, DVB-S2, and so forth, have adopted LDPC codes. Today, LDPC codes are considered to be the most eligible channel code for next generation high data rate communication and various practical applications. Development of most optimized and efficient constructed LDPC codes have been also studied widely in current decade. LDPC codes can provide lower probability of error than equivalent conventional codes e.g. Turbo codes, RS code etc.

This paper is organized as follows. Section III summarizes the LDPC code followed by the non-binary LDPC code in Section IV. Section V deals with the methods of generating a parity-check matrix based on progressive edge growth (PEG) algorithm. Section VI deals with the decoding technique of non binary LDPC codes. Section VII gives simulation details and results followed by the conclusion in Section VIII.

III. LOW DENSITY PARITY CHECK

An LDPC code, a class of linear block codes, is defined by a sparse parity-check matrix, **H**, of size m ∗ n. The **H** matrix for a regular (j, k) LDPC code is a binary matrix having j ones in each column and k ones in each row, where j and k are small integer numbers if compared to n. An irregular LDPC matrix is also sparse, but in this case not all columns and rows have same number of 1's. Below is an example of regular and irregular matrices.

$$\mathbf{H}_{\text{regular}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{H}_{\text{irregular}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

IV. NON-BINARY LDPC CODES

In 1998, David and Mackay presented an idea of LDPC over finite fields GF(q), where $q > 2$ [6][7]. A non-binary LDPC code is based on a sparse ***H*** matrix over finite field GF(q). We can represent the non-binary LDPC code using a Tanner graph as shown in Figure 1. Recently, regular and irregular non-binary LDPC codes over GF(q) are constructed based on a PEG algorithm [8], which is one of the most promising algorithms. This algorithm is widely used because it provides high code performance and guarantees higher

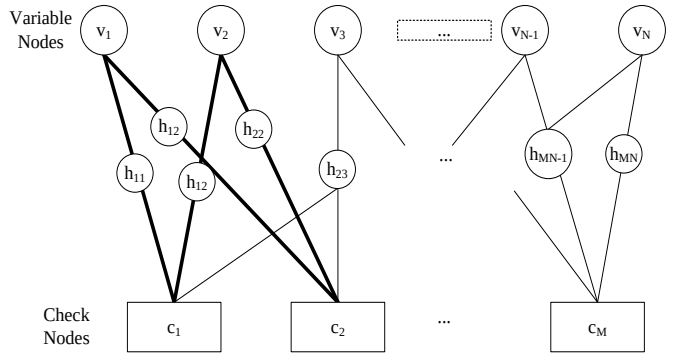

Figure 1. H matrix representation using a Tanner graph.

girth. Another popular way to construct an **H** matrix is based on a Quasi-Cyclic (QC) LDPC method proposed by Lin *et al*. [9]. There are some interesting potential applications discussed so far in research associated with non-binary LDPC codes [10].

V. A METHOD OF CONSTRUCTING **H** MATRIX

The structure of **H** has a significant effect on encoding, decoding, and code performance in terms of bit-error rate (BER). In general, **H** can be designed based on structured or non-structured method. For instance, Fan [11] presented an array structure of **H**, which offers a comparable performance to a random generated parity-check matrix. Eleftheriou and Olcer [12] proposed a modified array structure (MAC) by applying a cyclic shift to Fan's array, which offered higher performance than Fan's array matrix. Next, Singhaudom *et al*. [13] introduced an interleaved modified array structure (IMAC) by applying a QC matrix into to the cyclic shift of Fan's array [8]. This IMAC is suitable for a large block length LDPC codes. After this, Prasartkaew and Choomchuay [14] proposed a variant of **H** matrix for short and moderate block length codes, which has comparable performance than IMAC.

Another very useful method for generating **H** matrix is through a PEG algorithm because it can guarantee high girth bound. Accordingly, we focus on the PEG algorithm in this paper to investigate the performance of a non-binary LDPC code over its binary counterpart. However PEG algorithm legs of special structural property, ongoing research literature found on QC -PEG based **H** matrix and strictly concentrated check nodes LDPC codes for high efficient and less complex encoding [9].

A. *Progressive Edge Growth Algorithm*

PEG is an algorithm used for constructing an **H** matrix and suitable for encoding and decoding of the LDPC code with a large girth. It is considered as most successful approaches for construction of finite length LDPC codes. For an edge, the connections between variable nodes and check nodes by an edge connection algorithm. This algorithm is valid for both regular and irregular **H** matrix construction. In practice, a low cycle free Tanner graph provides optimum decoding and PEG try to maximize the girth cycle. We employed same notations as used in [8] for describing a tanner graph with n variable nodes and m check nodes. The PEG algorithm can be summarized as follows.

for $j = 0$ to $n - 1$ **do**
begin
  for $k = 0$ to $d_{s_j} - 1$ **do**
  begin
  if $k = 0$
  $E_{s_j}^0 \longleftarrow$ edge (c_i, s_j), where $E_{s_j}^k$ is the first edge incident to symbol node s_j, and c_j is the check node such that it has the minimum check node degree under the current graph setting $E_{s_0} \bigcup E_{s_1} \bigcup \cdots \bigcup E_{s_{j-1}}$
  else
  expand a sub-graph from symbol node s_j up to depth l under the current graph setting such that the cardinality of $N_{s_j}^l$ stops increasing but is less than m, or $\overline{N_{s_j}^l} = \emptyset$ but $\overline{N_{s_j}^{l+1}} = \emptyset$, then $E_{s_j}^k \longleftarrow$ edge (c_i, s_j) where $E_{s_j}^k$ is the k^{th} edge incident to s_j and c_i is a check node picked from set $\overline{N_{sj}^l}$ having minimum check node degree.
  end
end

In the above algorithm both symbol nodes and check nodes are ordered according to their degrees in non-decreasing order, where d_{s_j} is the degree of symbol nodes s_j, and $N_{s_j}^l$ and $\overline{N_{s_j}^l}$ are the set of every check node reached by a sub-graph starting from symbol node s_j within depth l and its complement, respectively. PEG creates a lower bound girth of length $2(l + 2)$.

VI. DECODING OF NON-BINARY LDPC

Several decoding algorithms have been discussed in the literature [15] for binary and non-binary LDPC codes, which can be summarized as the following steps.

1. Initialization: By using a received vector **r**, variable nodes are initially assigned with the likelihoods of channel reliability.

2. Check node update: This step is also called as a horizontal step, where each check node is updated using the likelihood message from adjacent variable nodes except the considering updated check node. A matrix generated based on updated check node information to corresponding location in **H** matrix known as Q matrix [16].

3. Variable node update: This step is known as a vertical update, where the variable nodes receive the message from adjacent check nodes to update its information and construct R matrix [16].

4. Iterative decoding: Most likelihood value of code word $\widehat{c_n}$ is computed with the step 1 and variable nodes messages. Decoded code word is valid only if it satisfies$cH^T = 0$. In case of no valid code word produced, decoding process stopped after certain number of iterations.

A. FFT Based Belief Propagation Decoding for GF(q)

Generally, the belief propagation algorithm is used for decoding a binary LDPC; however, it can also be extended to decode a non-binary LDPC code with the expense of increased complexity as q increases. The construction of Q matrix for GF(q) becomes more complicated in the horizontal step, as more possible non-binary sequences need to satisfy the parity-check equations, similarly R vertical matrix from Q matrix becomes even much more complicated. Permutation and de-permutation steps are also necessary for a non-binary LDPC. Specifically, the cyclic shift of likelihoods in downwards is referred to as permutation and that in upwards is called de-permutation.

FFT used in [17][18] to reduce the complexity in horizontal step in the belief propagation algorithm perform the computation of the check nodes update. In the frequency domain for simple product form transforms from convolution mathematical implications. By using this method, the complexity in the horizontal step for check node update can be significantly reduced. In general, the parity check equations must satisfy (1)

$$\sum_{j=1}^{n} h_{ij} c_j = 0 , \qquad (1)$$

where $h_{ij} \in$ GF(q) is an element in **H**, $c_j \in$ GF(q), $i = 1, 2, \ldots, m$, and $j = 1,2, \ldots, n$.

Algorithm can be summarized in Figure. 2, known as a factor graph of non-binary LDPC. Factor graph is used to decode non-binary LDPC codes. It requires two additional blocks 1) permutation block; 2) re-ordering block; as compared to binary factor graph [16].

In factor graph the number of **H** matrix elements connected to coded symbol c_j's is the column weight of code and the number of connections to each parity check is the row weight of the code. Likelihoods of each coded symbol f_j are the column vectors containing q likelihoods of coded symbol. A block labeled as $\prod$ function as reordering block connects non-binary element in each row to parity check matrix.

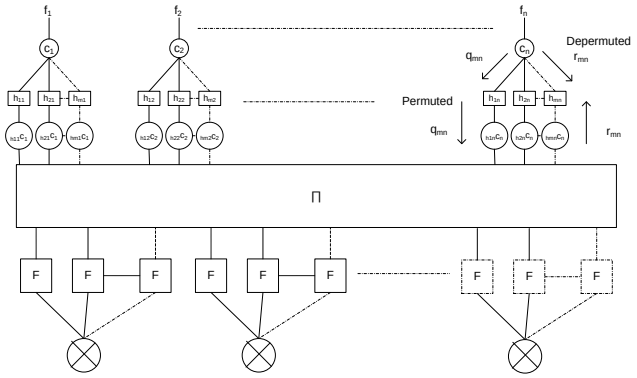

Figure 2 Generalized factor graph using FFTs operations for non-binary LDPC decoding.

VII. SIMULATION DETAILS AND RESULTS

This section shows an example through simulation on how binary and non-binary LDPC codes perform. For simplicity, we consider a code rate of 1/2 for an additive white Gaussian noise (AWGN) channel. Each of 9 message symbols $x_k \in$ GF(q) is encoded by a regular non-binary LDPC code, resulting in a coded block length of 18 symbols, $a_k \in$ GF(q). The parity-check matrix **H** has been constructed using PEG algorithm. We have taken degree 2 of each variable node, hence 2 nonzero elements in each column..The girth of **H** matrix is 6 The received signal can then be expressed as in (2).

$$y_k = a_k + n_k , \qquad (2)$$

Where n_k is AWGN with zero mean and variance $\sigma^2 = N_o/2$. The per-bit signal-to-noise ratio (E_b/N_0) is defined as $10\log_{10}(1/\sigma^2)$ in decibel (dB). We compute the BER based on a minimum number of 50000 data packets.

To compare the performance between binary and non-binary LDPC codes, we use the LDPC decoder with 10 iterations and plot the BER performance. Figure 3 compares the performance of different LDPC codes over GF(q) at the 10^{th} iteration in terms of BER, where q = 2, 4, 8, 16, 32, 64 and 128. Note that $q = 2$ represents a binary LDPC code. Here, we also plot the BER performance of uncoded bits under the influence of same channel conditions and theoretical BER for BPSK for fair comparison.

As expected, a non-binary LDPC code with large q performs better than that with small q. As the decoding complexity of a non-binary LDPC code with large q is high, all advantages gained by this non-binary LDPC code need to be balanced against the increased implementation cost.

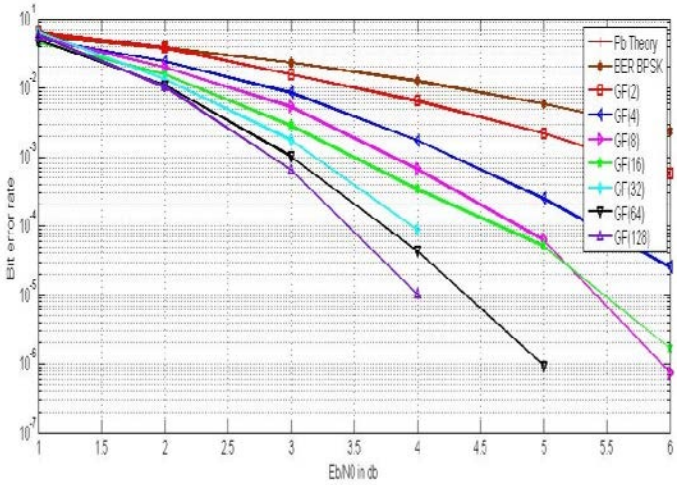

Figure 3BER performance of different LDPC codes over GF(q) at 10th iteration

It could be observed that there is indeed a significant performance gain in moving to higher order field reaching towards the Shannon's limit.

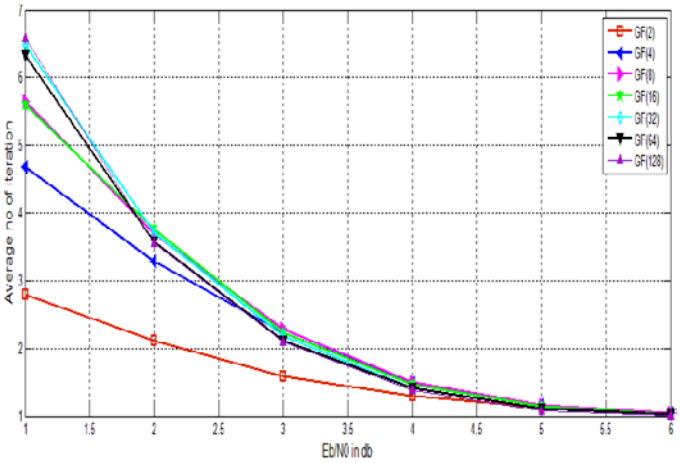

Figure 4Average number of iterations required for decoding different LDPC codes over GF (q)

We also compare the performance of different schemes by plotting the average number of iterations needed to decode all codeword of finite GF (q) LDPC codes as a function of E_b/N_0 as shown in Figure. 4 based on our example. It is obvious that the LDPC codes iteration can help to increase the performance of the system. Again, a non-binary LDPC codes with large q is superior to that with small q.

VIII. CONCLUSION

In this paper, we have presented a study on non-binary LDPC codes from associated open literature and its performance related to **H**. matrix construction. We analyzed PEG based construction of **H** matrix for binary and non-binary LDPC codes Decoding procedure based on FFT-belief propagation for non-binary LDPC codes. Section VII showed performance and comparisons of our tested simulation for a PEG based regular **H** matrix. We take into account of higher order of GF(q), which outperforms binary LDPC for small to medium sized data packets.

REFERENCES

1. C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal,vol. 27, pp. 379-423, 1948.
2. Berrou, Claude, Alain Glavieux, and Punya Thitimajshima. "Near Shannon limit error-correcting coding and decoding: Turbo-codes.1." *Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record, IEEE International Conference on*. Vol. 2. IEEE, 1993.
3. Gallager, Robert. "Low-density parity-check codes." *Information Theory, IRE Transactions on* 8.1 (1962): 21-28.
4. MacKay, David JC, and Radford M. Neal. "Near Shannon limit performance of low density parity check codes." *Electronics letters* 32.18 (1996): 1645.
5. Davey, Matthew C., and David JC MacKay. "Low density parity check codes over GF (q)." *Information Theory Workshop, 1998*. IEEE, 1998.
6. MacKay, David JC, and Matthew C. Davey. "Evaluation of Gallager codes for short block length and high rate applications." *Codes, Systems, and Graphical Models*. Springer New York, 2001. 113-130.
7. Davey, M. C., & MacKay, D. J. (1998, June). Low density parity check codes over GF (q). In *Information Theory Workshop, 1998* (pp. 70-71). IEEE.
8. Hu, X. Y., Eleftheriou, E., & Arnold, D. M. (2005). Regular and irregular progressive edge-growth tanner graphs. *Information Theory, IEEE Transactions on*, *51*(1), 386-398.
9. S. Lin, S. Song, L. Lan, L. Zeng, and Y.-Y. Tai, "Constructions of nonbinary quasi-cyclic LDPC codes: a finite field approach," in *Proc. Inform. Theory Applications Workshop*, 2006.
10. A. Bajpai, G. Srirutchataboon, T. Phromsa-ard, L. Kovintavewat and P. Kovintavewat, "A Study of Non-Binary Low-Density Parity-Check Codes and Its Applications." *Proceedings of Thailand's Electrical Engineering Conference (EECON-35)* 2012.
11. J.L. Fan, "Array Codes as low-density parity-check codes," *Proc. 2nd Int. Symp. Turbo Code*, Beit, France, pp. 543-546, Sep. 2000.
12. E. Eleftheriou and S. Olcer, "Low-density parity-Check Codes for Digital Subscriber Lines," *Proc. 2002 Int. Conf. on Comm.*, pp.1752-1757, April-May 2002.
13. W. Singhaudom, S. Noppankeepong, P. Suphithi**, "**Design of Hign-Rate Modified Array Codes for Magnetic Recording System," *ECTI International Conference***,** May 2007.
14. Chutima Prasartkaew and Somsak Choomchuay. "A design of parity check matrix for Irregular LDPC codes." *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*. IEEE, 2009.
15. D. Declercq and M. Fossorier, "Decoding algorithm for non-binary LDPC codes over GF (2^m) ". *IEEE Transactions on Communication vol.* 55, no. 4 pp. 633-643, April 2007.
16. Carrasco, R. A. and Johnston, M. (2008) Information, Channel Capacity and Channel Modeling, in Non-Binary Error Control Coding for Wireless Communication and Data Storage, John Wiley & Sons, Ltd, Chichester, UK. doi: 10.1002/9780470740415.ch1
17. MacKay, David JC, and Matthew C. Davey. "Evaluation of Gallager codes for short block length and high rate applications." *Codes, Systems, and Graphical Models*. Springer New York, 2001. 113-130.
18. Voicila, A., Declercq, D., Verdier, F., Fossorier, M., & Urard, P. (2010). Low-complexity decoding for non-binary LDPC codes in high order fields.*Communications, IEEE Transactions on*, *58*(5), 1365-1375.