A Study of Non-Binary Low-Density Parity-Check Codes and Its Applications

Ambar Bajpai[1] Gan Srirutchataboon[1] Tharathorn Phromsa-ard[1] Suvit Nakpeerayuth[1]
Piya Kovintavewat[2] and Lunchakorn Wuttisittikulkij[1]
[1]Department of Electrical Engineering, Faculty of Engineering, Chulalongkorn University
254 Phayathai Road, Bangkok 10330, Thailand. Email: wlunchak@chula.ac.th
[2] Data Storage Technology Research Center, Nakhon Pathom Rajabhat University, Nakhon Pathom 73000, Thailand.

Abstract

This paper presents a study of non-binary low-density parity-check (LDPC) codes and its applications. Some existing known codes are described. An encoding procedure (based on Reed Solomon codes) and a decoding procedure using fast Fourier transform (based on a belief propagation algorithm) have been discussed. Simulation results illustrate that non-binary LDPC codes can perform better than its binary counterpart. Finally, some interesting applications that exploit non-binary LDPC codes are given.

Keywords: Galois field (GF), low-density parity-check (LDPC), non-binary LDPC.

1. Introduction

An enormous potential research has been carried out on channel coding since the Shannon's theory of mathematical constraints for channel capacity was introduced. This paper focuses on non-binary low-density parity-check (LDPC) codes, which is a derivative of binary LDPC over Galois field GF(q), where $q = 2^m$ and m is a prime number. LDPC codes were first introduced by Gallagar [1] in 1962. Since then these codes were ignored almost next 30 years, due to its complexity and less analytical tools available at that time. Later, these codes were rediscovered by Mackay and Neal in 1996 [2]. Afterward, researchers focused on this potential forward error-correction (FEC) codes in multiple domains of LDPC codes. Various standards such as IEEE 802.11n, WiMAX, DVB-S2, and so forth have adopted LDPC codes. Today, LDPC codes are considered as the most eligible channel codes for future generation high data rate communications and various practical applications. Development of most optimized and efficient constructed LDPC codes have been also studied widely in the current decade.

In practice, the performance of LDPC codes relies on several system parameters and varies accordingly. It is of importance to carefully design LDPC parity-check matrices, which are ultra sparse and avoid low cycle presence and select properly the number of iterations; therefore, fulfilling these constraints leads to significantly optimized performance as stated by Chung *et al*. in 2001 [3]. Result approached to very close to 0.0045 dB from Shannon's limit exists only for a large block length. Clearly, a large block length results in a large parity-check matrix and hence a large generator matrix. Thus, LDPC codes are defined by a sparse matrix, in which most of the entries are zero and only few portions are nonzero values (the smaller the portion of nonzero entries, the less the encoding and decoding complexity). In binary LDPC codes, although a large block length has good performance but it increases a scheduling time.

Non-binary LDPC codes were first investigated by Davey and MacKay in 1998 [4], whose performance is much better than a binary counterpart. A widely used belief propagation (BP) algorithm, used in binary LDPC codes, causes non-binary LDPC codes to increase computation analysis, almost infeasible for a higher order of q. It is shown that complexity can be deduced to $\mathrm{O}\left(q\log_2 q\right)$ if we transfer a BP algorithm for GF(q) into a frequency domain computation [8]. Recently, irregular non-binary LDPC codes over GF(q) are constructed by Hu *et al.* using a progressive-edge-growth (PEG) algorithm [5], popular for next level research due to higher performance.

1.1 Motivation Factor

For small to moderate block length and high code rate, a non-binary LDPC code normally provides better performance than a binary counterpart [2-6]. In addition, non-binary LDPC codes can be combined with a higher order of modulation with ease. Specifically, it can avoid bit to symbol conversion (and vice versa). Such a feature allows an application of radio and underwater communications to combine with higher order modulation and multi-input and multi-output (MIMO) technique [8-12].

The most appealing LDPC codes are Quasi-cyclic LDPC (QC-LDPC) for practical systems as the structure of quasi-cyclic matrix allows for linear time encoding using only shift registers and also rendering efficient routing for decoding implementation. Furthermore, it enables the storage of the coding matrix with the requirement of few memory units. One active research on QC-LDPC codes has been on the efficient parity-check matrix construction with large girth, meaning the length of the shortest cycle in the tanner graph representation.

However, this paper only aims to describe the basic concept of non-binary LDPC codes, especially the encoding and the decoding procedures of non-binary LDPC codes. We also provide some interesting applications that exploit non-binary LDPC codes.

This paper is organized as follows. Section 2 introduces parity-check matrix construction algorithms for non-binary LDPC codes. Sections 3 concentrate on the decoding of non-binary LDPC codes. Simulation results are given in Section 4. Section 5 describes various applications of non-binary LDPC codes and the superiority of non-binary LDPC codes over their binary counterpart. Finally, Section 6 concludes this paper.

2. Construction of non-binary LDPC codes

A non-binary LDPC code is basically the same as a binary LDPC code, which consists of a sparse parity-check matrix **H**. The only difference is its elements can be defined over finite fields GF(q), as opposed to GF(2). Although many researchers are working on the topic of non-binary LDPC codes, there is still a lot of works needed to be investigated for non-binary LDPC codes.

A q-ary QC-LDPC code is given by the null space of an array **H** of sparse circular matrices of the same size over the field GF(q). If the array **H** viewed as a matrix has a constant column weight γ and a constant row weight ρ, the code given by the null space of **H** is said to be (γ,ρ)-regular; otherwise, it is said to be irregular. Row-Column (RC) constraint ensures that the Tanner graph of the LDPC code given by the null space of **H** has a girth of at least 6 and that the minimum distance of the code, if (γ,ρ)-regular, is at least $\gamma+1$ [12-13]. The distance bound is tight for regular LDPC codes whose parity-check matrices have large column weights and row redundancies, such as the algebraic LDPC codes constructed using finite fields, finite geometries, and combinatorial designs. Fig. 1 shows the Tanner graph for non-binary LDPC codes.

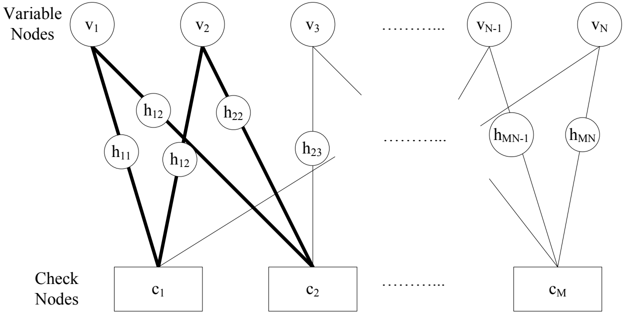

Fig. 1 A Tanner graph showing non-binary LDPC codes [28].

2.1 Construction of non-binary LDPC codes from Reed Solomon Codes

Shu Lin *at el.* [18-22] investigated several structural methods to construct non-binary LDPC codes (with good performance) using array dispersion methods [14], which use tools such as Euclidian distances and finite geometries. Specifically, array dispersion operation is applied to each nonzero element in a matrix form of size $(q-1)\times(q-1)$. In the context of non-binary LDPC codes defined over GF(q), an element $\alpha^i \in \mathrm{GF}(q)$ for $0 \le i \le q-2$ will be placed the i-th indexed of the location vector length $(q-1)$.

For example, an α^4 element in GF(8) would be placed in the 4-th index of the location vector. This element is shifted on right cyclically to build an array of size $(q-1)\times(q-1)$. Performing array dispersion on an $m\times n$ matrix would result in a larger sparse matrix with size of $m(q-1)\times n(q-1)$. Thus, for this example, one obtains

$$\mathbf{W} = \begin{bmatrix} 0 & 0 & 0 & 0 & \alpha^4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^6 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 \end{bmatrix}, \qquad (1)$$

where the top row in **W** is the original location vector. In **W** matrix, for zero elements, array dispersion will result in a $(q-1)\times(q-1)$ zero matrix and array dispersion of 1 will also yield a $(q-1)\times(q-1)$ array with each row defined as the previous row cyclically shifted to the right and multiplied by the primitive element in GF(q). Same is true for the rest of the primitive GF field elements. Performing array dispersion leads to a parity-check matrix **H**.

The non-binary LDPC codes are constructed from Reed Solomon (RS) codes with a message length equal to k. In general, RS codes defined over GF(q) with a block length of $n = q-1$ will be represented by $(q-1, k, q-k)$, and they are maximum distance separable codes with minimum distance $d = n-k+1$. It can be demonstrated that a vector containing all ones $\left[1,1,1,\ldots,1\right]$ and the vector $\left[1,\alpha,\alpha^2,\ldots,\alpha^{q-k}\right]$ are both valid code words. Since RS code is linear codes, adding these two code words will result in other linear code words. This added code word is then used to build an $m(q-1)\times n(q-1)$ matrix.

In general, QC-LDPC codes have a quasi-cyclic structure of the parity-check matrix **H**. Either binary or non-binary LDPC codes can be classified into two categories, i.e., random-like method and structured method. In random-like method, the shift offset values for component circulant permutation sub-matrices are obtained via random methods [15-17], whereas in structural methods, a special algebraic and a structural method [18-24] are used for computing circulant permutation sub-matrices. Using these methods, we can achieve high girth while the code block length can also be varied to meet the requirement of any specific application.

Consider an $m\times n$ matrix **B**(**H**), which is called the base matrix. With cyclic expansion, that is, replacing elements "0" and "1" in **B**(**H**) with zero sub-matrices of size $L\times L$ and circulant permutation sub-matrices of size $L\times L$, respectively, one can obtain a **H** matrix of size $mL\times nL$, which defines a binary QC-LDPC code. Specifically, let **P** be an $L\times L$ permutation matrix as

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \qquad (2)$$

For a finite, $0 \le a < L$, $\mathbf{P}^a$ denotes a circulant permutation sub-matrix of size $L \times L$, which is obtained by cyclically shifting an identity matrix $\mathbf{I}_L$ to the right by a times. For simple notation, $\mathbf{P}^\infty$ denotes a zero matrix of size $L{\times}L$. By applying cyclic expansion to the base matrix **B**(**H**), the **H** matrix of size $mL \times nL$ for a binary QC-LDPC code can be obtained according to [17], [25]

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}^{a_{11}} & \mathbf{P}^{a_{12}} & \cdots & \mathbf{P}^{a_{1n}} \\ \mathbf{P}^{a_{21}} & \mathbf{P}^{a_{22}} & \cdots & \mathbf{P}^{a_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}^{a_{m1}} & \mathbf{P}^{a_{m2}} & \cdots & \mathbf{P}^{a_{mn}} \end{bmatrix} \tag{3}$$

where the shift offset value $a_{ij} \in \{0, 1, \ldots, L-1, \infty\}$ for $i = 1, 2, \ldots, m$; $j = 1, 2, \ldots, n$; and $a_{ij} = \infty$ when the corresponding element in **B**(**H**) is "0."

It is given a binary H matrix as in (3), a non-binary $\mathbf{H_q}$ matrix can be obtained by replacing each nonzero element in **H** with a nonzero element from GF(q). Nonetheless, generally speaking, the obtained code is not qualified as a quasi-cyclic code over GF(q). Below is a summary of a design algorithm:

- Step 1: Construct a base matrix **B**(**H**).
- Step 2: Specify the shift offset value a_{ij} in (3) for each nonzero element of **B**(**H**). After cyclic expansion, we obtain a binary **H** matrix as in (3).
- Step 3: Specify the nonzero elements of $\mathbf{H_q}$ over GF(q) by replacing each "1" element in **H** by an element from GF(q), excluding 0 element.

3. Decoding of Non-Binary LDPC

There are number of decoding algorithm discussed in literature [33] for binary and non-binary LDPC codes as we can briefly summarize as follows.

1) Initialization: By using the received vector **r**, variable nodes are initially assigned with the likelihoods of channel reliability.
2) Check node update: This step is called a horizontal step to construct a **Q** matrix. Each check node is updated using the likelihood message from adjacent variable nodes, except the considering updated check nodes.
3) Variable node update: This step is known as a vertical update to construct an **R** matrix. Each variable node is updated using messages received from its adjacent check nodes.
4) Iterative decoding: The most likelihood value of codeword **c** is computed with the step 1 and variable nodes messages. A decoded codeword is valid only if it satisfies $\mathbf{cH}^{\mathrm{T}} = \mathbf{0}$. In case of no valid codeword produced, a decoding process will stop after certain number of iterations.

3.1 FFT Based belief propagation (BP) decoding for GF(*q*)

Practically, the BP algorithm for binary LDPC codes can be extended to decode non-binary LDPC codes, with the cost of increased decoding complexity as a value of q increases. Thus, the **Q** matrix for GF(q) becomes more complicated. In the horizontal step, as more possible non-binary sequences are needed to satisfy parity check equations; this leads to much more computation. Similarly, in the vertical step, since **R** matrix is computed from **Q** matrix, it certainly becomes much more complicated. Permutation and depermutation are required in case of non-binary LDPC codes. Cyclic shift of the likelihoods in downwards direction is called permutation whereas the inverse operation is called depermutations. The fast Fourier transform (FFT) used in [34] allows the computation of the check node update in the frequency domain in a product form, instead of performing a more complicated convolution done in the time domain. By this method, the complexity in horizontal step for check node update is significantly reduced [35]. In general, parity check equations satisfy (4).

$$\sum_{j=1}^{n} h_{ij} c_j = 0 \ , \tag{4}$$

where a parity check matrix h_{ij} and $c_j \in \mathrm{GF}(q)$ for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. Algorithm can be summarized in Fig. 2 known as a factor graph of non-binary LDPC [35]. Coded symbol likelihoods c_j are the column weight of codes. Likelihoods of each coded symbols f_j are column vectors containing q likelihoods of coded symbol. A block labeled $\prod$ connects non-binary elements in each row to parity check matrix.

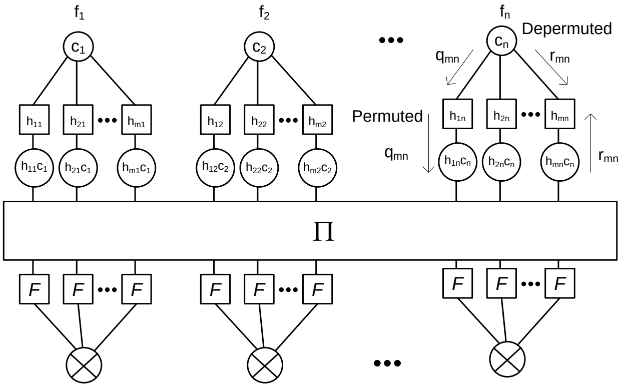

Fig. 2 Generalized factor graph of a non-binary LDPC code using FFTs operations [35].

4. Simulation Results

This section shows an example through simulation on how non-binary LDPC codes can perform. For simplicity, we consider a rate-1/2 coded additive white Gaussian noise (AWGN) channel. A block of 9 message symbols $x_k \in \mathrm{GF}(q)$ is encoded by a regular $(j, k) = (2, 4)$ non-binary LDPC code, resulting in a coded block length of 18 symbols $a_k \in \mathrm{GF}(q)$. The parity-check matrix **H** has 2 nonzero elements in each column and 4 nonzero elements in each row. The received signal can then be expressed as in (5).

$$y_k = a_k + n_k \ , \tag{5}$$

where n_k is an AWGN with variance $\sigma^2 = N_0/2$. The SNR per bit (or 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 and 1000 error bits.

Fig. 3 compares the performance of different LDPC codes over GF(q) at the 10-th iteration in terms of bit-error rate (BER), where q = 2, 4, 8, 16 and 32. Note that q = 2 represent a binary LDPC code. We also plot the BER performance of a conventional binary phase shift keying (BPSK) system for the sake of 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.

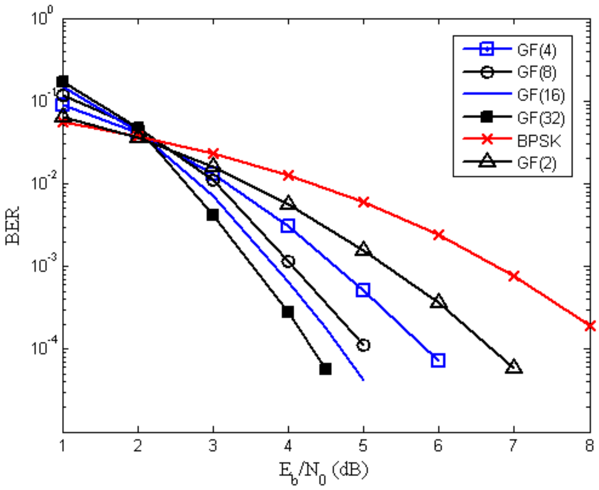

Fig. 3 BER performance of different LDPC codes over GF(q) at the 10-th iteration.

We also compare the performance of different schemes by plotting the BER as a function of the number of iterations in Fig. 4. It is obvious that the LDPC iteration can help increase the performance of the system up to 6 iterations, and then it seems to encounter an error floor. Again, a non-binary LDPC code with large q is superior to that with small q.

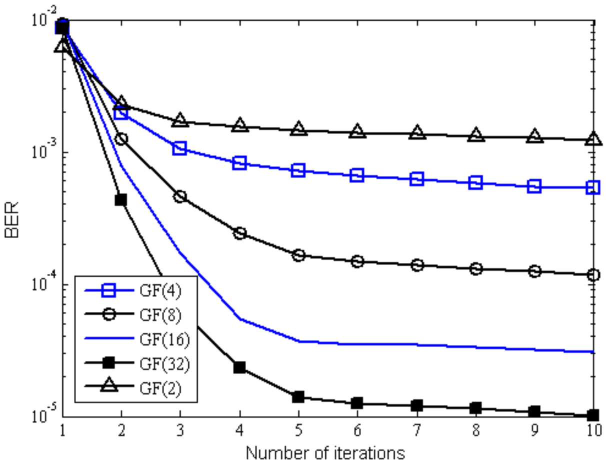

Fig. 4 BER versus the number of iterations at E_b/N_0 = 5 dB.

5. Applications of Non-Binary LDPC

In this section, we briefly summarize some interesting applications that exploit the non-binary LDPC codes as follows.

5.1 Multiple-Antenna Transmissions

In recent years, the multiple-input multiple-output (MIMO) transmission system has been identified as significant potential to minimize fading and increase the capacity of wireless channels. In Fig. 5, we show an example of the design of irregular binary LDPC codes which has been investigated for MIMO channels as proposed in [10]. Most research focuses however on binary LDPC codes for MIMO channels. It is shown that LDPC codes with higher order GF(q) give best performance if compared to binary LDPC code [6]. Thus, in recent works, non-binary LDPC codes have been applied to the non-binary AWGN channel [8] and MIMO channels [26]. Non-Binary LDPC codes when concatenated with MLC (multi-level) codes [27] leads to better performance.

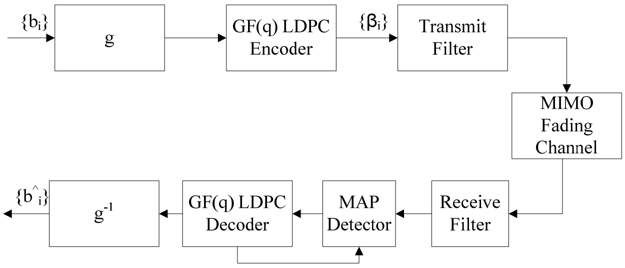

Fig. 5 A schematic block diagram of iterative system [10].

5.2 Small Packet Transmission in Vehicle Communications

Vehicle communication systems require small and moderate size packet transmission in order to optimize overall system capacity. Fast moving vehicles needs better forward error-correction (FEC) techniques for most reliable communication. For higher rate packet communications, it is also useful to apply the higher order modulation such as 8PSK and 16QAM. The block diagram for non-binary LDPC codes based transmission as shown in Fig. 6 was introduced for vehicle communication using small size of packets. As results shown in [28], for small and medium sized packet transmission in vehicle communication, non-binary LDPC codes are very useful and outperform its binary counterpart.

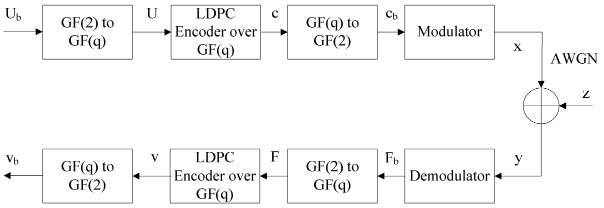

Fig. 6 A block diagram of non-binary LDPC codes based transmission as introduced in [28] for vehicle communication.

5.3 Communications over Fading Channels for higher order modulations

Various standards like 802.11n, Wimax, DVB-S2 employ higher order modulation and these standards officially stated LDPC codes for channel coding. A proposed non-binary system in [9] is illustrated in Fig. 7. Also, a low complexity decoding algorithm for the non-binary LDPC codes based on log domain sum product algorithm has been developed in [9].

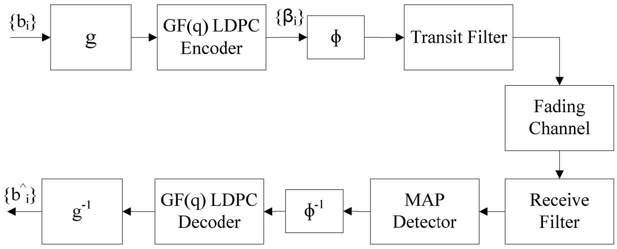

Fig. 7 A schematic block diagram of a non-binary system proposed in [9].

5.4 Distributed file storage system

In today's electronic and computerized world, growing demands of grid and cluster computing. In computer cluster, CPU power is readily available through batch or grid computing systems. Most often considerable amount of disk space on the computer nodes is not useful for long term storage. Research targeted to use this idle storage for higher performance and reliable file storage targeted mainly at workstations. An LDPC code provides solution to this problem because it can reconstruct original message relatively less complex and efficient algorithm unlike erasure coding [29-30]. Read Solomon coding [31] suitability of LDPC codes can be used for storage application [32].

5.5 Other Applications

Recently, non-binary LDPC codes have been standardized in IEEE 802.11n, Digital Video Broadcasting (DVB-S2), and Wimax. Furthermore, applications of these codes can also be extended to high data rate optical communication system, rate adaptive schemes in communication systems and under water acoustic communication, and so on.

6. Conclusion

In this paper, we have presented a study on non-binary LDPC codes from associated open literature related to LDPC. Through our study, we discussed motivation factors behind enormous potential of non-binary QC-LDPC codes in various standards and applications. Moreover, we presented code construction methods and a decoding procedure of non-binary LDPC codes. Section 4 showed performance comparison of our tested simulation for a given regular parity-check matrix. We take into account of a higher order of Galois fields, which outperforms binary LDPC for small to medium sized data packets. We also compare BER as a function of the number of iterations for a fixed SNR, which concludes that non-binary LDPC codes perform better than a binary LDPC counterpart, especially when an order of Galois fields is high. Consequently, we summarized some potential applications discussed so far in research associated with non-binary LDPC codes.

References

[1] R. Gallager, "Low density parity-check codes," Ph.D. dissertation, 1962.

[2] D. J. MacKay and R. Neal, "Near Shannon-limit performance of low-density parity-check codes," vol. 32, 1996, pp. 645–1646.

[3] S.-Y. Chung, G. F. Jr., T. Richardson, and R. Urbanke,"On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," vol. 47, Feb. 2001, pp. 58 – 60.

[4] N. Wiberg, "Codes and decoding on general graphs," Ph.D. dissertation, Department of electrical engineering, Linkping University, 1996.

[5] C. Poulliat and D. Declercq, "Using binary images of non binary LDPC codes to improve overall performance," in 4th International Symposium on Turbo-codes and related topics, Apr. 2006.

[6] M. C. Davey and D. Mackay, "Low-density parity-check codes over GF(q)," IEEE Comm. Letters, vol. 2, pp. 165-167, June 1998.

[7] X. Y Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," IEEE Trans. Inform. Theory, vol. 51, pp. 386-398, Jan. 2005.

[8] J. Huang, S. Zhou, and P. Willett, "Non binary LDPC coding for multicarrier underwater acoustic communication," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 9, pp. 1684–1696, Dec. 2008.

[9] R.-H. Peng and R.-R. Chen, "Application of non binary LDPC codes for communication over fading channels using higher order modulations," in *Proc. IEEE Globecom*, Nov. /Dec. 2006.

[10] R.-H. Peng and R.-R. Chen, "Design of non binary LDPC codes over GF(q) for multiple-antenna transmission," in *Proc. IEEE MILCOM*, Oct. 2006.

[11] R.-H. Peng and R.-R. Chen, "Application of non binary LDPC cycle codes to MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2020–2026, 2008.

[12] B. Li, J. Huang, S. Zhou, K. Ball, M. Stojanovic, L. Freitag, and P. Willett, "MIMO-OFDM for high rate underwater acoustic communications," *IEEE J. Ocean. Engr.*, vol. 34, no. 4, pp. 634–644, Oct. 2009.

[11] Davey, M.C. and Mackay, D.J. (1998) Low density parity-check codes over GF(q). IEEE Information Theory Workshop, Killarney, Ireland, pp. 70–1.

[12] Y. Kou, S. 1, and M. P. C. Fossorier,"Low density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

[13] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2004.

[14] Lin, S., Song, S., Zhou, B. *et al.* (2007) Algebraic constructions of non binary quasi-cyclic LDPC codes: array masking and dispersion.9th International Symposium on Communication Theory and Applications (ISCTA), Ambleside, Lake District, UK.

[15] R.-H. Peng and R.-R. Chen, “Design of non binary quasi-cyclic LDPC cycle codes,” in *Proc. IEEE Inform. Theory Workshop*, Sep. 2007.

[16] B. Li, J. Huang, S. Zhou, K. Ball, M. Stojanovic, L. Freitag, and P. Willett, “MIMO-OFDM for high rate underwater acoustic communications,” *IEEE J. Ocean. Engr.*, vol. 34, no. 4, pp. 634–644, Oct. 2009.

[17] M. Fossorier, “Quasi-cyclic low-density parity-check codes from circulant permutation matrices,” *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, 2004.

[18] 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.

[19] S. Song, L. Zeng, S. Lin, and K. Abdel-Ghaffar, “Algebraic constructions of nonbinary quasi-cyclic LDPC codes,” in *Proc. IEEE Intern. Symp. Inform. Theory*, July 2006.

[20] B. Zhou, Y.-Y. Tai, L. Lan, S. Song, L. Zeng, and S. Lin, “Construction of high performance and efficiently encodable nonbinary quasi-cyclic LDPC codes,” in *Proc. IEEE Globecom*, Nov./Dec. 2006.

[21] S. Lin, S. Song, B. Zhou, J. Kang, Y.-Y. Tai, and Q. Huang, “Algebraic constructions of nonbinary quasi-cyclic LDPC codes: array masking and dispersion,” in *Proc. Inform. Theory Applications Workshop*, 2007.

[22] B. Zhou, J. Kang, Y.-Y. Tai, Q. Huang, and S. Lin, “High performance nonbinary quasi-cyclic LDPC codes on Euclidean geometries,” in *Proc. IEEE MILCOM*, Oct. 2007.

[23] Y.-Y. Tai, L. Lan, L. Zeng, S. Lin, and K. Abdel-Ghaffar, “Algebraic construction of quasi-cyclic LDPC codes for the AWGN and erasure channels,” *IEEE Trans. Commun.*, vol. 54, no. 10, pp. 1765–1774, Oct. 2006.

[24] R. Tanner, D. Sridhara, and T. Fuja, “A class of group-structured LDPC codes,” in *Proc. Commun. Theory Applications*, July 2001.

[25] S. Myung, K. Yang, and J. Kim, “Quasi-cyclic LDPC codes for fast encoding,” *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2894–2901, Aug. 2005.

[26] A. Bennatan and D. Burshtein, "Design and analysis of non binary LDPC codes for arbitrary discrete-memoryless channels," IEEE Trans. Inform. Theory, vol. 52, pp. 549-583, Feb. 2006.

[27] J. Hou, P. H. Siegel, L. B. Milstein, and H. D. Pfister, Capacity approaching bandwidth-efficient coded modulation schemes based on low-density parity-check codes," IEEE Trans. Inform. Theory, vol. 49, pp. 2141-2155, Sept. 2003.

[28] K. Dai, g. Frederic and p. Ramesh, “Application of non-binary LDPC codes for small packet transmission in vehicle communications” 5th international conference on its telecommunications, June 27-29, Brest, France, 2005, pp. 109-112.

[29] W. K. Lin, D. M. Chiu, Y. B. Lee, Erasure Code Replication Revisited, in: 4th International Conference on Peer-to-Peer Computing (P2P 2004), IEEE, Zurich, Switzerland, 2004, pp. 90–97.

[30] H. Weatherspoon, J. Kubiatowicz, Erasure coding vs. replication: A quantitative comparison, in: International Workshop on Peer-to-Peer Systems (IPTPS), Vol. 1, 2002.

[31] J. S. Plank, A tutorial on Reed-Solomon coding for fault-tolerance in RAID-like systems, Software – Practice & Experience 27 (9) (1997) 995–1012.

[32] B. Gaidioz, B.Koblitz, Nuno Santos, “Exploring high performance distributed file storage using LDPC codes” Elsevier Science Publishers B. V., Parallel Computing, Volume 33 Issue 4-5, pp.264-274, May 2007.

[33] 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.

[34] D. J. C. MacKay and M. Davey, “Evaluation of Gallager codes for short block length and high rate applications”, Proc. IMA Workshop Codes, Syst., Graphical Models, 1999

[35] L. Barnault and D. Declercq, “Fast decoding algorithm for LDPC over GF”, Proc. Inf. Theory Workshop Paris, France, Mar. 2003, p. 70.

Ambar Bajpai He has done his M.E. (Communication Systems) from BITS Pilani, India in 2007. Presently he is pusuing Ph.D in chulalongkorn university, Bangkok Thailand. In addition, he worked with ST Microelectronics, Bangalore with hands on experience in live projects of video codec H.264 & integrate BlueZ stack on ST nomadic development board. His area of interest is wireless technologies, wireless security & Bluetooth.

Gan Srirutchataboon He received a B.Eng from Bangkok University. He is currently a Master student of Electrical Engineering at Chulalongkorn university.

Tharathorn Phromsa-ard He is currently a Master student of Electrical Engineering at Chulalongkorn University under the scholarship of TGIST.

Suvit Nakpeerayuth He is a lecturer in Electrical Engineering at Chulalongkorn University. His research interests include digital signal processing technology, advanced communication techniques for unmanned aerial vehicle.

Piya Kovintavewat He received the B.Eng. summa cum laude from Thammasat University, Thailand (1994), the M.S. degree from Chalmers University of Technology, Sweden (1998), and the Ph.D. degree from Georgia Institute of Technology (2004), all in Electrical Engineering. His thesis work titled "Timing Recovery Based on Per-Survivor Processing" was awarded second prize for new Ph.D. thesis in the field of information technology by the National Research Council of Thailand in 2005.

Lunchakorn Wuttisittikulkij He is an Associated Professor in Electrical Engineering at Chulalongkorn University.