A Design of Parity-Check Matrix with Maximized Local Girth for Quasi-Cyclic LDPC codes

Gan Srirutchataboon, Ambar Bajpai, Lunchakorn Wuttisittikulkij
Department of electrical Engineering
Chulalongkorn University
Bangkok Thailand

Piya kovintavewat
Faculty of Science and Technology
Nakhon Pathom Rajabhat University
Nakorn Pathom Thailand

***Abstract*— Quasi-Cyclic low-density parity-check (QC-LDPC) codes are an attractive solution to construct a parity-check matrix, H, that offers hardware-friendly architecture and has a satisfactory error-correction performance. In general, a large girth property of LDPC codes ensures a good error-correction performance. Thus, this paper proposes a method to construct the H matrix of QC-LDPC by sequentially maximizing the local girth for each column of the H matrix. The performance of the proposed method will be compared with that of the existing ones. Simulation results show that the proposed method performs better than the existing ones in terms of bit-error rate and provides a higher girth.**

***Keywords*— QC-LDPC, girth, Shannon limit.**

I. INTRODUCTION

An important class of linear block codes known as low-density parity-check (LDPC) codes was originally introduced by Gallager [1] in 1962. Despite its significant impact on recent communication systems and standards, LDPC codes were neglected for almost three decades because of its complexity and hardware unavailability at that time. However, LDPC codes were rediscovered by Mackey and Neal in 1997 [2], and since then many methods for constructing good LDPC codes have been proposed [3, 4] and investigated continuously.

In practice, a quasi-cyclic LDPC codes (QC-LDPC) are widely used in many applications because it is suitable for hardware implementations [5]. Many standards such as IEEE 802.16e and 802.11n also employ QC-LDPC codes. Generally, a parity check matrix **H** of QC-LDPC codes consist of an array of circulant sub-matrices, in which each sub-matrix is a cyclic shift version of the *base* sub-matrix.

A girth is one of important constraints for designing a good LDPC codes because a large girth facilitates an iterative decoding and imposes a respectable minimum distance bound, which can improve the decoding performance at high signal-to-noise ratio (SNR) scenario [3]. Therefore, this work aims at designing good QC-LDPC codes by maximizing the local girth. The **H** matrix is constructed column by column to avoid complexity associated with the exhaust search for appropriate combination of sub-matrices. As can be seen in simulation results, the proposed LDPC codes can perform better than the existing ones in terms of bit-error rate (BER), and also provides a high girth.

This paper is organized as follows. Section II summarizes an LDPC code and a Quasi-Cyclic LDPC code. Section III briefly explains a method to generate a parity-check matrix, **H**, based on circulant matrix algorithms, including the QC-LDPC codes. Section IV explain our proposed method and Section V gives simulation details and results. Finally, Section VI concludes this paper.

II. LDPC CODES

LDPC codes are a class of linear block codes, which can be defined by a sparse parity-check matrix **H** of size $M \times N$, where M is the number of rows and N is the number of columns. In general, the **H** matrix can also be represented by a Tanner graph [6] or bipartite graph, which consists of two sets (V, E), where $V = V_c \cup V_s$, $V_c = \{c_0, c_1, \ldots, c_{M-1}\}$ is a set of check nodes, $V_s = \{s_0, s_1, \ldots, s_{N-1}\}$ is a set of bit nodes (or symbol nodes), E is a set of edges, $(c_m, s_n) \in E$ corresponds to a nonzero element at the m^{th} row and the n^{th} column in the **H** matrix. Below is an example of the **H** matrix, i.e.,

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

whose size is 4×8 with a column weight of $w_c = 2$ and a row weight of $w_r = 4$. Furthermore, if c is a binary codeword, it will satisfy

$$c\mathbf{H}^{\mathrm{T}} = \mathbf{0} \pmod 2, \tag{1}$$

where $(.)^{\mathrm{T}}$ is a transpose matrix operator.

A. Quasi-Cyclic LDPC codes

A QC-LDPC code is a class of cyclic codes, in which each sub-matrix is a shifted version of the base matrix of size $p \times p$.

Thus, the $M \times N$ **H** matrix of QC-LDPC codes can be constructed as

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}^{a(0,0)} & \mathbf{I}^{a(0,1)} & . \; . & \mathbf{I}^{a(0,k-1)} \\ \mathbf{I}^{a(1,0)} & \mathbf{I}^{a(1,1)} & . \; . & \mathbf{I}^{a(1,k-1)} \\ . & . & . \; . & . \\ . & . & . \; . & . \\ \mathbf{I}^{a(j-1,0)} & \mathbf{I}^{a(j-1,1)} & . \; . & \mathbf{I}^{a(j-1,k-1)} \end{bmatrix}_{M \times N}, \qquad (2)$$

where j is the number of block-rows, k is the number of block-columns, $\mathbf{I}^0$ is an $p \times p$ identity matrix, $a(j,k)$ is a number of cyclic shifts $M = pj$, and $N = pk$. Specifically, $\mathbf{I}^{a(j,k)}$ is a $p \times p$ circulant permutation matrix obtained by cyclically shifting the rows of the identity matrix $\mathbf{I}^0$ to the right by $a(j,k)$ times.

It should be noted that any sub-matrix inside **H** can also be represented by its first column. For example, if $p = 3$, we obtain $\mathbf{I}^0 = [1\ 0\ 0]^T$ and $\mathbf{I}^1 = [0\ 1\ 0]^T$, i.e.,

$$\mathbf{I}^0 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } \mathbf{I}^1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \qquad (3)$$

where the x^{th} column is obtained by cyclically shifting the 1^{st} column $(x-1)$ places to the bottom, and $1 < x \leq p$ is an integer.

B. Existing Method for Generating LDPC codes

In this Section, we mention about some existing methods for constructing the **H** matrix. For example, Fan [7] proposed an array code. Then, Eleftheriou and Olcer [8] introduced a modified array code (MAC), which yielded higher performance than the array code. However, Singhaudom [9] presented an interleaved modified array code (IMAC), which was suitable for a large block length code and eased an encoding process. Then, Prasartkaew and Choomchuay [10] proposed a method for constructing the IMAC suitable for short and moderate block length codes, whose performance is comparable to IMAC. Moreover, Prasartkaew and Choomchuay also presented a method to construct a short-block irregular LDPC code by using magic square theorem [11]. Another useful method for generating the **H** matrix is a Sidara-Fuja-Tanner (SFT) technique [12], which suits for a regular QC-LDPC code. This paper will compare our proposed LDPC code with the codes based on IMAC, SFT, and magic square.

III. PROPOSED METHOED

This section explains how to construct the **H** matrix based on our proposed method. Let us consider the case where $j = 3$ and $k = 9$. Assuming that $p \geq jk$, the procedure for constructing the proposed **H** matrix is as follows.

1) Construct a $j \times k$ index matrix, $\bar{\mathbf{H}}$, as shown in Table I (a), where R is a random number, and Z stands for a designed shifting order for the $p \times p$ circulant permutation matrix. Note that the **H** matrix will have a size of $jp \times kp$.

Table I. An example of the 3×9 index matrix.

block-column index

block-row index $\bar{\mathbf{H}}$	1	2	3	4	5	6	7	8	9
1	*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*	*R*
2	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*
3	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*

(a)

block-column index

block-row index $\bar{\mathbf{H}}$	1	2	3	4	5	6	7	8	9
1	19	9	44	17	28	8	31	13	32
2	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*
3	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*

(b)

2) Construct a $j \times k$ index matrix, $\bar{\mathbf{H}}$, as shown in Table I (a), where R is a random number, and Z stands for a designed shifting order for the $p \times p$ circulant permutation matrix. Note that the **H** matrix will have a size of $jp \times kp$.
3) Assign a random number R between 0 and $p-1$ to all elements in the first row of $\bar{\mathbf{H}}$, as depicted in Table I (b) for example.
4) For each column, replace Z in all block-rows using a number between 0 to $p-1$. To do so, we find all possible data patterns of each column[1], P_{fc}. In practice, it can be demonstrated that the total number of data patterns in P_{fc} is equal to

$$\text{\# data patterns} = \binom{p}{1}^{j-1} \qquad (4)$$

   3.1) We place each 2-block-row data pattern in the column and compute its local girth, g, resulting from this column[2]. The data pattern that yields a maximum girth will be used in this column. Note that when finding a local girth for each data pattern, if we cannot find the local girth (i.e., no cycle), we will assume that this data pattern has a girth of infinity, i.e., $g = \infty$.

   3.2) Once we obtain a data pattern for the first column, we perform the same procedure for the second column. This process continues until all columns are filled with the chosen number.

Table II illustrates an example of the index matrix $\bar{\mathbf{H}}$, after obtaining all Z's.

[1] For example, there are two block-rows in Table I (b), which are the 2^{nd} and 3^{rd} rows. If we assume that $p = 3$, there will then be 9 data patterns of the first column as given in Fig. 1.

[2] When finding a local girth for each data pattern, we will assume that all sub-matrices labeled as Z are zero matrices.

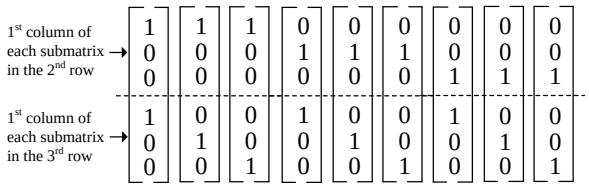

Fig. 1. An example of data patterns of the first column of the 2nd and 3rd block-rows for $p = 3$.

Table II. A designed 3×9 index matrix.

	block-column index								
block-row index	$\bar{\mathbf{H}}$	1	2	3	4	5	6	7	8	9
	1	19	9	44	17	28	8	31	13	32
	2	0	2	3	5	10	7	29	20	18
	3	0	3	5	14	20	12	36	23	45

IV. SIMULATION RESULTS

Consider an $M \times N$ **H** matrix, where N is the length of a codeword, and M is the number of parity bits. To evaluate the performance of the proposed algorithm, we simulate the system based on an additive white Gaussian noise (AWGN) channel model, where a binary input sequence $a_k \in \{0, 1\}$ of length $N - M$ bits is encoded by an LDPC encoder and is mapped to an N-bit coded sequence $b_k \in \{\pm 1\}$. Then, the received sequence is given by $y_k = b_k + n_k$, where n_k is AWGN with zero mean and variance σ^2. At the receiver, the received sequence y_k is decoded by an LDPC decoder implemented based on a message passing algorithm [1] with 10 iterations. In simulation, the signal-to-noise ratio is defined as

$$\mathrm{SNR} = 10\log_{10}\left(\frac{1}{\sigma^2}\right), \tag{5}$$

in decibel (dB). Each BER point is computed based on a minimum number of 50000 data packets and 500 error bits, and all LDPC codes use the **H** matrix of size 171×513.

Fig. 2 compares the BER performance of the proposed algorithm with other existing methods, where "Magic 1," "Magic 2" and "Magic 3" are the codes from [11], "SFT" is the codes from [12], and "IMAC" is the codes from [10]. We also show the performance of a binary phase shift keying (BPSK) system as a benchmark so as to see how big the performance gain can be obtained from using the LDPC codes. Clearly, the proposed algorithm is superior to other algorithms when SNR is high. Furthermore, we also investigate the local girth of each algorithm as given in Table III. Again, the proposed algorithm offers the largest girth if compared to other algorithms.

We also compare the BER performance of different schemes as a function of the number of iterations at SNR = 4.5 dB in Fig. 3. It is apparent that the proposed algorithm converges faster than other algorithms.

Table III. A minimum girth from different **H** matrices.

Parameter	Minimum Girth			
	Magic	SFT	IMAC	Proposed
$p = 57, j = 3, k = 9$	6	6	6	8
$p = 61, j = 3, k = 10$	6	6	6	8

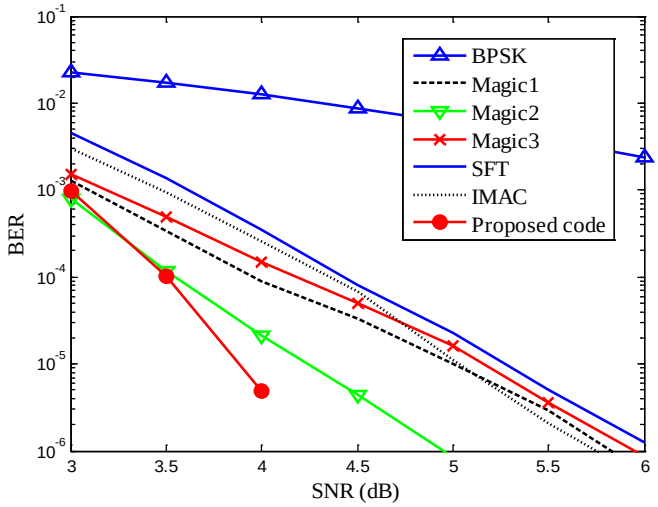

Fig. 2. BER performance of different 171×513 **H** matrices.

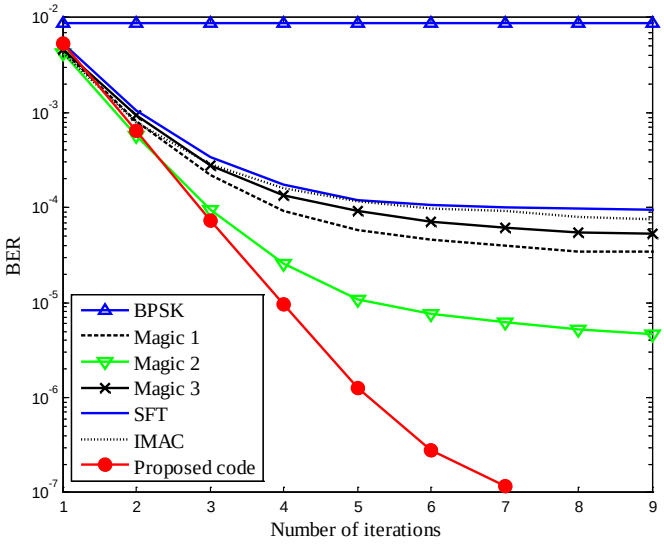

Fig. 3. BER performance as a function of the number of iterations for different 171×513 **H** matrices at SNR = 4.5 dB.

V. CONCLUTION

In this paper, we propose a new algorithm for constructing the **H** matrix of QC-LDPC codes that aims to maximize the local girth by sequentially assigning proper sub-matrix for each column of the **H** matrix one by one. As shown in simulation results, the proposed algorithm outperforms the

existing algorithms in terms of BER and converges faster than the others. In addition, we found that the proposed algorithm requires more complexity than other algorithms. There exists a trade-off between performance and complexity.

REFERENCES

[1] R. Gallager, "Low-density parity-check codes," *IRE Trans. on Inform. Theory*, vol. 8, no. 1, pp. 21–28, January 1962.

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, pp. 1645–1646, August. 1996.

[3] Hu, Xiao-Yu, Evangelos Eleftheriou, and Dieter-Michael Arnold. "Regular and irregular progressive edge-growth tanner graphs." *Information Theory, IEEE Transactions on* 51.1 (2005): 386-398.

[4] J. Xueqin, X. Xiang-Gen, and L. Moon Ho, "Efficient progressive edge-growth algorithm based on Chinese remainder theorem," IEEE Trans. On Comm., vol. 62, no. 2, pp. 442–451, February 2014.

[5] Chen, Yanni, and Keshab K. Parhi. "Overlapped message passing for quasi-cyclic low-density parity check codes." *Circuits and Systems I: Regular Papers, IEEE Transactions on* 51.6 (2004): 1106-1113.

[6] Tanner, Robert Michael. "A recursive approach to low complexity codes."*Information Theory, IEEE Transactions on* 27.5 (1981): 533-547.

[7] J. L. Fan, "Array codes as low-density pqrity-check codes," *in Proc. of the 2nd Int. Symp. Turbo Codes*, France, pp. 543-546, Sep 2000.

[8] E. Eleftheriou and S. Olcer," low-density parity-check codes for digital subscriber line," in *Proc. of ICC'02*, pp. 1752-1757, April-May, 2002.

[9] W. Singhaudom, S. Noppankeepong, and P. Supnithi, "Design of high-rate modified array codes for magnetic recording system," in *Proc. of ECTI-CON*, May 2007.

[10] C. Prasartkaew and S. Choomchuay, "Parity check matrix construction via magic square based algorithm," in *Proc. of ISCIT*, October 2-5, 2012.

[11] C. Prasartkaew and S. Choomchuay, "Parity check matrix construction via Magic Square Based Algorithm," *Communications and Information Technologies (ISCIT), 2012 International Symposium on* , vol., no., pp.54,59, 2-5 Oct. 2012.

[12] S. Timakul and S. Choomchuay, "Construction of quasi-cyclic LDPC codes form SFT structure and cyclic shift," in *Proc. of ISPAC*, December 7-9, 2011.