

# A Design of Nonprime Block Irregular LDPC Codes via CRT

Chalit Chusin<sup>1</sup>, Chutima Prasartkaew<sup>2</sup>, Sekson Timakul<sup>3</sup>, and Somsak Choomchuay<sup>4</sup>

<sup>1,2,3</sup> College of Data Storage Technology and Applications, King Mongkut's Institute of Technology Ladkrabang  
BKK 10520, Thailand

<sup>1</sup>Tel:/Fax: + 66-3-881-5966, E-mail: [ithonene@hotmail.com](mailto:ithonene@hotmail.com)

<sup>2</sup>Tel: +66-2-329-8345 Ext.114, Fax: +66-2-329-8346, E-mail: [prasartkaew@yahoo.com](mailto:prasartkaew@yahoo.com)

<sup>3</sup>Tel: +66-2-329-8345 Ext.114, Fax: +66-2-329-8346, E-mail: [sekson.timakul@gmail.com](mailto:sekson.timakul@gmail.com)

<sup>4</sup> Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, BKK 10520, Thailand  
Tel: +66-2-329-8345 Ext.114, Fax: +66-2-329-8346, E-mail: [kchsomsa@kmitl.ac.th](mailto:kchsomsa@kmitl.ac.th)

**Abstract**—This paper presents a new design of irregular LDPC codes that supports arbitrary block length. We propose the efficient construction method when nonprime size sub-matrices are used. The problem where  $GCD(L_1, L_2) \neq 1$  that left unsolved has been tackled. We also consider the case  $GCD(L_1, L_2) = 1$  but  $L_1$  or  $L_2$  is a nonprime number. The results show that our designed codes have superior performance compared to MAC. The resulted codes still hold the attractive properties of LDPC codes. The performances of interleaved codes are higher than noninterleaved codes and it goes higher as SNR is increased.

**Index**--- nonprime, CRT, interleave, LDPC codes, irregular

## I. INTRODUCTION

A Low Density Parity Check (LDPC) code was firstly proposed by Gallager in 1962 [1]. According to the good performance of LDPC codes that close to channel limit over AWGN channel [2] and [3], many researchers are interesting in these codes. However, in the case of LDPC codes with random H matrix, big memory size is unavoidable, in particular for the large block length code. Then, it is hard to efficiently access the memory and encoded data. A quasi cyclic structure or QC-LDPC code was taken into consideration to overcome this memory problem. With QC-LDPC codes, the storage memory size can be reduced due to their algebraic structure. The memory can be reduced by either introducing  $L \times L$  circulant permutation matrices or employing zero matrices [4]. QC-LDPC codes with circulant permutation matrices are proposed by [5], [4], [6], and [7]. The performance evaluations were also made respectively.

The improved QC-LDPC codes that made use of the Chinese Remainder Theorem (CRT) has been studied lately by [4], [6] and [7]. The CRT can be used to address the problems of 4-cycle issue and/or girth reduction in case of long block length QC-LDPC coded. Reference [4] has proposed a method for constructing long length QC-LDPC codes from small length QC-LDPC codes using the CRT. And by applying the CRT method to array codes, they presented a family of high-rate regular QC-LDPC codes with no 4-cycles. Reference [6] has proposed a generalization of

CRT combining method to design better QC-LDPC codes. Their results show that a BER of  $10^{-6}$  can be obtained. Such a generalized combining method outperformed 0.5 dB of SNR compared to [4]. Recently, reference [7] has presented the remedy to two problems associated with CRT-based QC-LDPC codes: how to extend the code length code without reducing the girth, and how to design codes with a prescribed girth easily. They have proposed a method of combining QC-LDPC codes via CRT. In contrast to [4] and [6], [7] has constructed  $H_2$  with large girth sub-matrix while  $H_1$  still follows [8]. The resulted codes have flexible length, flexible rates, large girth and suite well iteration decoding.

Based on the prime number parameters of the matrices, [2], [8], [3] and [4] have more focused to regular LDPC codes, whilst [9] and [10] worked on irregular LDPC codes. A limitation of using of prime number parameters is that the designed codes can support only some particular code lengths. With this note, [11] has proposed regular Size Compatible (SC)-array LDPC codes using nonprime number parameters. The sub-matrices are permuted to avoid the cycle of 4. The performance of SC-array is better when compared to [8].

With above regards, the CRT has neither applied to nonprime codes nor irregular structure. In this paper we investigate the application of CRT in designing the irregular LDPC codes with nonprime block length. Although the design cannot cover prescribed girth, it suits well an arbitrary length. The rest of this paper is organized as follows: the literature reviews of the related works are given in section II. The combination of QC-LDPC codes for the longer codes using the CRT proposed by [4] is reviewed in section III. The detailed designed, the highlight of this work, is given in section IV. Examples of 4 cases are also given in this section. In section V, the designed coded are evaluated and their performance are discussed -- also in comparison with some previous works proposed by other authors. Finally, this paper is concluded in section VI.

## II. RELATED WORKS

Reference [8] has introduced the array structure parity check matrix for regular LDPC codes that can offer code

performance close to a random generated parity check matrix. Other features are: low error floor and no cycle of 4, which are as same as the features of regular LDPC codes originally proposed by [1]. Fan's parity check matrix has regular structure and rewritten herewith in (1) below. This yields the code rate of  $R = 1 - (pj - j + 1) / p^2$ .

$$H(p, j, k) \triangleq \begin{bmatrix} I & I & I & \dots & & & \\ I & P & P^2 & \dots & & & -1 \\ & & P^4 & \dots & & & \vdots \\ \vdots & \vdots & \vdots & \ddots & & & \vdots \\ I & P^{j-1} & P^{2(j-1)} & \dots & & & (k-1) \end{bmatrix} \quad (1)$$

where  $I$  is an  $L \times L$  identity matrix  
 $P$  is a position permutation matrix.

Reference [9] has proposed the modified array codes (MAC) by applying cyclic shifting to the matrix proposed by [8]. In contrast to [8], [9] proposed an irregular LDPC. The parity check matrix of this design is given here again in (2). It offers the code rate of  $R = 1 - (j/k)$ . Modified array codes yields superior performance compared to [8], especially for long block lengths. The reduction of number of "1" in the lower triangle of the matrix leads to simpler encoder while preserving other LDPC's features.

$$H = \begin{bmatrix} I & I & \dots & I & I & \dots & \dots & I \\ 0 & I & P & \dots & P^{(j-2)} & P^{(j-1)} & \dots & P^{(k-2)} \\ 0 & 0 & I & \dots & P^{2(j-3)} & P^{2(j-2)} & \dots & P^{2(k-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix} \quad (2)$$

where  $I$  is an identity matrix  
 $P$  are position permutation matrices.

Reference [4] has proposed a construction method of QC-LDPC codes of large length by combining QC-LDPC codes of small length as their component codes. Such a construction is based on the CRT method given by [12]. The girth of the obtained codes is always larger than or equal to that of each of the component code. By applying the similar method to array codes presented in [8], they presented a family of high-rate regular QC-LDPC codes with no 4-cycles. Simulation results show that [4] have almost the same performance as random regular LDPC codes.

Reference [6] has proposed a generalization of the CRT presented in [4]. The combining method was used to design much more and better QC-LDPC codes for given the parity check matrices of the component codes. The proposed work can be used to design a much larger class of QC-LDPC codes with similar performance by loosening the condition for determining the intermediate parameters. By permuting the block rows of the parity check matrices of the component codes, a lot of QC-LDPC codes with much less 6-cycles and better performance can be designed. At a BER of  $10^{-6}$  some

QC-LDPC codes designed by the generalized combining method outperform those designed by the CRT combining method by 0.5 dB compared to [4].

Reference [7] considered two problems associated with QC-LDPC codes. The first is how to extend the code length of a code without reducing the girth. The second is how to design a code with a prescribed girth easily. The method given in [4] and [6] cannot directly applied to construct low-rate and large girth code. Reference [7] proposed an alternative way to construct sub-matrix and used combining method presented in [4] to build a parity matrix. LDPC codes constructed with such a method have flexible lengths, flexible rates and large girth.

Reference [11] has proposed the SC-Array LDPC codes developed from the array structure of [8]. The  $H$  matrix with nonprime number parameters is given here in (3). The design supports arbitrary lengths achieve good error rate performance compared to [8]. It contains very few or no cycle-4 structure. In their SC-array regular LDPC codes, the permutation sub-matrix is decided to eliminate all cycle-4. The proposed cyclic shift  $\alpha_{sc}(j, k)$  is expressed by (4).

$$H = \begin{bmatrix} I & I & \dots & \dots & \dots & & \\ p^{\alpha_{sc}(2,k)} & I & \dots & \dots & \dots & & -1 \\ p^{\alpha_{sc}(3,k)} & p^{\alpha_{sc}(3,k-1)} & I & \dots & \dots & & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ p^{\alpha_{sc}(j,k)} & p^{\alpha_{sc}(j,k-1)} & \dots & \dots & \dots & \dots & j+1 \end{bmatrix} \quad (3)$$

where

$$\alpha_{sc}(j, k) = (j-1)(k-1) + \left\lfloor \frac{(j-1)(k-1)}{L} \right\rfloor \quad (4)$$

Lately, reference [13] has proposed the design of parity check matrix to support arbitrary code length. It is based on the interleaving method suggested by [14] and the SC-array proposed by [11]. In their design, the constructed rows don't hold the same sub-matrices. The results show that even if the sub-matrix size is a nonprime number, their designed Interleaved Modified Array codes achieve the same error rate performance as the prime size sub-matrices.

The interleave method given by [13] was applied for this study as the following procedure steps.

1) The sub-matrix for interleaving can be either  $T$  or  $\omega$ , where sizes of  $T$  and  $\omega$  can be nonprime or prime number. The  $\omega$  matrix was designed by locating '1' in the position as shown in the following matrices. Because of there are two 1's in each alternative column, then the  $\omega$  matrix can be modified by a lower half left shifting and the  $T$  matrix is obtained.

$$\omega = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{6 \times 6} \rightarrow T = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{6 \times 6}$$

2) The sub-matrix,  $T^d$  or  $T^2$  can be obtained by right shifting the sub-matrix,  $T$ .

$$T^1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{6 \times 6} \rightarrow T^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{6 \times 6}, T^n = T$$

3) The interleaving is performed similar to that mentioned in [13] where the maximum exponent number of sub-matrix,  $T^2$  (or  $\omega^2$ ) must be less than or equal to  $j$ .

4) Matrix element  $\alpha$ , can be computed using CRT method given in [4]. The achieved matrix is shown in (5).

$$H = \begin{bmatrix} I & I & IT & IT^2 & \dots & \dots & j \\ 0 & I & P^{\alpha_T(2,3)}T & \dots & \dots & \dots & \\ 0 & 0 & I & P^{\alpha_T(3,4)}T^2 & P^{\alpha_T(3,i)}T^{j-1} & \dots & 3, k-2)T^j \\ \vdots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \dots & \dots & \dots & \dots \end{bmatrix} \quad (5)$$

where

$$\alpha_T(j, k) = (j-1)(k-1) + \left\lfloor \frac{(j-1)(K-j)}{L} \right\rfloor \quad (6)$$

### III. THE COMBINATION OF QC-LDPC CODES VIA CRT

The parity check matrix of QC-LDPC codes shown in (7) consists of small square blocks of  $L \times L$  zero matrix or circulant permutation matrices.

$$H = \begin{bmatrix} P^{\alpha_{11}} & P^{\alpha_{12}} & \dots & P^{1(k-1)} & P^{\alpha_{1k}} \\ P^{\alpha_{21}} & P^{\alpha_{22}} & \dots & P^{2(k-1)} & P^{\alpha_{2k}} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ P^{\alpha_{j1}} & P^{\alpha_{j2}} & \dots & P^{j(k-1)} & P^{\alpha_{jk}} \end{bmatrix}_{j \times k} \quad (7)$$

Where  $P^{\alpha_{mn}}; (1 \leq m \leq j, 1 \leq n \leq k)$  represents an  $L \times L$  circulant permutation matrix obtained by cyclically right-shifting the identity matrix,  $I$  to the right by  $\alpha_{mn}$  times, and  $\alpha \in \{0, 1, \dots, \infty\}$ . The zero matrix of size  $L \times L$  is denoted by  $I^0$ . The exponent matrix,  $E(H)$  of the given  $H$  in (7) is defined as

$$E(H) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & 1) & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & \dots & 1) & \alpha_{2k} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ \alpha_{j1} & \alpha_{j2} & \dots & 1) & \alpha_{jk} \end{bmatrix} \quad (8)$$

The check matrix  $H$  can be obtained by replacing each  $\alpha_{mn}$  entry of  $E(H)$  with  $P^{\alpha_{mn}}$ . The mother matrix,  $M(H)$  of the given  $H$  is obtained by replacing zero matrix and circulant permutation matrix in  $H$  with "0" and "I", respectively.  $\alpha_{mn}^q$  notes the exponent  $(mn)^{th}$  of the matrix  $q$ .

Let  $L_1, L_2, \dots, L_t$  be pair-wise relatively prime positive integers. Let  $C_q$  be a QC-LDPC code whose binary parity check matrix,  $H_q$  with dimension of  $jL_q \times kL_q$ . A combining method proposed in [4] was used to construct a QC-LDPC code as the following procedures.

Step1: If  $GCD(L_q, L_r) = 1$  for all  $q, r \leq t$  and  $(q \neq r)$

- If  $\alpha_{mn}^q \neq \infty$  for  $1 \leq q \leq t$ , then

$$\alpha_{mn} = \sum_{q=1}^t \alpha_{mn}^q b_q L'_q \text{ mod } L \quad (9)$$

Where

$$L = L_1 L_2 \dots L_t, \quad L'_q = \frac{L}{L_q} \quad (10)$$

and  $b_q L'_q \equiv 1 \text{ mod } L_q$ . Otherwise,  $\alpha_{mn} = \infty$ .

Step2: The exponent matrix  $E(H)$  for  $H$  is defined by  $E(H) = (a_{mn})$ .

Step3: The parity check matrix  $H$  can be obtained by replacing each exponent coupling of  $E(H)$  with  $P^{\alpha_{mn}}$ .

For example, consider two QC-LDPC codes that have parity check matrices,  $H_1$  and  $H_2$  that  $GCD(L_1, L_2) = 1$ ,  $E(H_1) = (a_{mn}^1)$ ,  $E(H_2) = (a_{mn}^2)$  and  $M(H_1) = M(H_2)$ . When they are combined using CRT, the exponent matrix  $E(H) = (c_{mn})$  is given by

$$c_{mn} = \{a_{mn}^1 b_1 L'_1 + a_{mn}^2 b_2 L'_2\} \text{ mod } L \quad (11)$$

where  $b_1$  and  $b_2$  are two integers such that  $b_1 L_2 \equiv 1 \text{ mod } L_1$  and  $b_2 L_1 \equiv 1 \text{ mod } L_2$ . Then the parity check matrix,  $H$  can be obtained by exponent coupling of  $E(H)$  and the  $L_1 L_2 \times L_1 L_2$  circulant permutation matrix,  $P$  where  $P_{mn} = \begin{cases} 1 & \text{if } n+1 \equiv m \text{ mod } L \\ 0 & \text{otherwise} \end{cases}$ .

Points to be noted here; [4], [6], and [7] have designed the codes only with prime-prime number combination. Moreover, the design of  $H_1, H_2, \dots, H_t$  is quite complicate when designing nonprime-nonprime or nonprime-prime combinations. In next section we introduce the method to construct  $H_1, H_2, \dots, H_t$  that compatibles with the rules of CRT even if nonprime-nonprime or non prime-prime combination are the cases.

### IV. FLEXIBLE LENGTH CODES DESIGN VIA CRT

The construction method with nonprime number parameters for both  $GCD(L_1, L_2) = 1$  and  $GCD(L_1, L_2) \neq 1$  will be elaborated in detail in this section. For better understanding, case examples are also given. To extend an  $jL_q \times kL_q$  to  $jL \times kL$ , parity matrix,  $H$  can be

constructed by combining  $E(\mathbf{H})$  via CRT. This method can be separated into 2 cases. First case,  $GCD(L_1, \dots, L_q) = 1$ , is the combination of either prime-prime such as  $L_7$  and  $L_3$ , or prime-nonprime such as  $L_7$  and  $L_6$ . In the second case,  $GCD(L_1, \dots, L_q) \neq 1$ , that can be either nonprime-prime such as  $L_6$  and  $L_3$  or nonprime-nonprime such as  $L_6$  and  $L_4$ . The prime-prime choice is in fact the same as [4]. The design of each case is elaborated as the follows:

Case 1: Design to support  $x = GCD(L_1, \dots, L_q) = 1$

- Construct the  $\mathbf{H}_1$  parity matrix as (2) given in [11]
- Construct  $\mathbf{H}_2$  by cyclic shift down for one time and replace the 1<sup>st</sup> row with  $\mathbf{I}$  for all  $a_{1n}^2$
- Using CRT to combine  $\mathbf{H}_1$  and  $\mathbf{H}_2$  to form  $\mathbf{H}$
- Rearrange the obtained  $\mathbf{H}$  matrix into Modified array codes structure, since Modified array codes yields attractive properties in encoding.
- Process the interleave (permutation) with the method given in (5)

Case 2: Design to support  $x = GCD(L_1, \dots, L_q) \neq 1$

- Construct the  $\mathbf{H}_1$  parity matrix as (2) given in [11]
- Construct  $\mathbf{H}_2$  by
  - the 1<sup>st</sup> row construct with  $\mathbf{I}$  for all  $a_{1n}^2$
  - Construct  $a_{2n}^2$  for  $2 \leq n \leq k$  by  $a_{2n}^2 = (I + y)$ , while  $a_{2n}^2 - a_{2n}^1 | x$  and  $y = 0, 1, \dots, x-1$
  - Construct  $a_{ij}^2$  in  $\mathbf{H}_2$  for  $3 \leq m \leq j$  and  $2 \leq n \leq k$  by  $a_{mn}^2 = a_{mn}^1 + x$
  - $a_{mn}^2 = I$ , and  $L = \left( \prod_{i=1}^t L_i \right) / x$
- Using CRT to combine  $\mathbf{H}_1$  and  $\mathbf{H}_2$  to form  $\mathbf{H}$
- Check whether matrices,  $\mathbf{H}$  satisfy the conditions that all remainders of  $a_{mn} / L_q = a_{mn}^q$  for all  $m, n$
- Rearrange the obtained  $\mathbf{H}$  matrix into Modified array codes structure
- Process the interleave (permutation) with the method given in (5)

In the case where  $GCD(L_1, \dots, L_q) \neq 1$ ,  $a_{mn}^1, a_{mn}^2, \dots, a_{mn}^q$  in each matrix,  $\mathbf{H}_k$  must be compatible with the rules of CRT that  $a_{mn}^2 - a_{mn}^1 | GCD(L_1, L_2)$ . Therefore we can construct the  $\mathbf{H}_2$  with the modified version of  $\mathbf{H}_1$ . And to be complied with CRT rules, all the remainders  $a_{mn}$  of  $\mathbf{H}$  must satisfy the condition that  $a_{mn} / L_q = a_{mn}^q$  for all  $m, n$ . Then we will show the combination matrix via CRT when  $GCD(L_1, \dots, L_q) \neq 1$  that illustrated by the follow example

**Example 1:** (Prime-Prime,  $GCD(L_1, L_2) = 1$ ); To design the parity check matrix,  $\mathbf{H}$  for 2050 codeword LDPC codes. With  $j = 3, k = 10, L = 205$ , we can have  $L_1 = 205, L_2 = 5$ .

- Check whether  $x = GCD(41, 5) = 1$
- Construct  $\mathbf{H}_1$  and  $\mathbf{H}_2$  as discussed above. The obtained matrices are shown in Fig.1.

		Column Index										
Row Index	$\mathbf{H}_1$	1	2	3	4	5	6	7	8	9	10	
	1	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$
	2	$\mathbf{I}$	$\mathbf{I}$	2	3	4	5	6	7	8	9	
	3	$\mathbf{I}$	2	4	6	8	10	12	14	16	18	

		Column Index										
Row Index	$\mathbf{H}_2$	1	2	3	4	5	6	7	8	9	10	
	1	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$
	2	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$
	3	$\mathbf{I}$	$\mathbf{I}$	2	3	4	$\mathbf{I}$	$\mathbf{I}$	2	3	4	

Fig. 1. The matrix structures of  $\mathbf{H}_1$  and  $\mathbf{H}_2$

- Determine
$$L = \frac{41 \times 5}{1} = 205, L'_1 = 205 / 41 = 5, L'_2 = 205 / 5 = 41$$

$$b_1(5) \equiv 1 \pmod{41}, b_1 = 33; b_2(41) \equiv 1 \pmod{5}, b_2 = 1$$
- We then have  $c_{22} \equiv \{(1 \times 33 \times 5) + 0\} \pmod{205} = 165$ . The obtained  $\mathbf{H}$  matrix is given in Fig. 2.

		Column Index										
Row Index	$\mathbf{H}$	1	2	3	4	5	6	7	8	9	10	
	1	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$
	2	$\mathbf{I}$	165	125	85	45	5	170	130	90	50	
	3	$\mathbf{I}$	166	127	88	49	10	176	137	98	59	

Fig. 2. The matrix structures of  $\mathbf{H}$  (Ex.1)

- Rearrange  $\mathbf{H}$  as shown in Fig. 3

		Column Index										
Row Index	$\mathbf{H}$	1	2	3	4	5	6	7	8	9	10	
	1	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$
	2	$\underline{0}$	$\mathbf{I}$	165	125	85	45	5	170	130	90	
	3	$\underline{0}$	$\underline{0}$	$\mathbf{I}$	166	127	88	49	10	176	137	

Fig. 3. The matrix structures of modified  $\mathbf{H}$  (Ex.1)

**Example 2:** (Nonprime – Nonprime,  $GCD(L_1, L_2) \neq 1$ ); Consider codeword,  $\mathbf{C}$  which has a  $3 \times 12$  parity check matrix,  $\mathbf{H}$  with  $L = 174$ . We use two circulant permutation matrices,  $\mathbf{H}_1$  and  $\mathbf{H}_2$  with  $L_1 = 87$  and  $L_2 = 6$ , respectively. As  $GCD(\mathbf{H}_1, \mathbf{H}_2) = 3$ , we are sticking to case 2.

- Construct the  $\mathbf{H}_1$  parity matrix

		Column Index												
Row Index	$\mathbf{H}_1$	1	2	3	4	5	6	7	8	9	10	11	12	
	1	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$	$\mathbf{I}$
	2	$\mathbf{I}$	$\mathbf{I}$	2	3	4	5	6	7	8	9	10	11	
	3	$\mathbf{I}$	2	4	6	8	10	12	14	16	18	20	22	

- $\mathbf{H}_2$  is obtained with the modification of  $\mathbf{H}_1$

		Column Index												
Row Index	$H_1$	1	2	3	4	5	6	7	8	9	10	11	12	
	1	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$
	2	$I$	$I$	2	$I$	$I$	2	$I$	$I$	2	$I$	$I$	2	$I$
	3	$I$	5	$I$	3	5	$I$	3	5	$I$	3	5	$I$	3

- Use CRT to combine  $H_1$  and  $H_2$  to form  $H$ 
  - $L = \frac{87 \times 6}{3} = 174$
  - $L_1 = 87, L_2 = 6, L_{11} = 29, L_{12} = 3, L_{21} = 3, L_{22} = 2,$   
 $L_{12} = L_{21} = 3,$  So, we choose  $L_{12}$  only
  - $L'_{11} = 174 / 29 = 6, L'_{12} = 174 / 3 = 58, L'_{21} = 174 / 2 = 86,$   
 $b_{11}(6) \equiv 1 \pmod{29}, b_{11} = 5, b_{12}(58) \equiv 1 \pmod{3}, b_{12} = 1$   
 $b_{22}(87) \equiv 1 \pmod{2}, b_{22} = 1$
  - $c_{22} \equiv \{(1 \times 5 \times 6) + (1 \times 1 \times 58) + (1 \times 1 \times 87)\} \pmod{174} = 1$

		Column Index												
Row Index	$H_1$	1	2	3	4	5	6	7	8	9	10	11	12	
	1	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$
	2	$I$	$I$	2	90	91	92	6	7	8	96	97	98	
	3	$I$	89	91	93	95	97	99	101	103	105	107	109	

- Check whether matrices,  $H$  satisfy the conditions that all remainders of  $a_{mn} / L_q = a_{mn}^q$  for all  $m, n$
- Rearrange the obtained  $H$  matrix into Modified array codes

		Column Index												
Row Index	$H_1$	1	2	3	4	5	6	7	8	9	10	11	12	
	1	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$
	2	$\underline{0}$	$I$	$I$	2	90	91	92	6	7	8	96	97	98
	3	$\underline{0}$	$\underline{0}$	$I$	89	91	93	95	97	99	101	103	105	

**Example 3:** (Prime – Nonprime,  $GCD(L_1, L_2) = 1$ ); Let  $H_1$  and  $H_2$  be sub-matrices of a  $3 \times 8$  parity check matrix,  $H$  with  $L_1 = 43$ ,  $L_2 = 6$  such that  $L = 258$ . Since  $GCD(41, 6) = 1$ , we use case 1 to design parity check matrix,  $H$ . The resulted  $H$  of this example is shown in Fig. 4 and Fig. 5 below.

		Column Index							
Row Index	H	1	2	3	4	5	6	7	
	1	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$
	2	$\underline{0}$	$I$	42	84	126	168	210	
	3	$\underline{0}$	$\underline{0}$	$I$	43	86	129	172	

Fig. 4. The matrix structures of modified  $H$  (Ex.3)

		Column Index							
Row Index	H	1	2	3	4	5	6	7	
	1	$I$	$I$	$IT$	$IT^2$	$IT^3$	$IT^3$	$IT^3$	
	2	$\underline{0}$	$I$	$42T$	$84T^2$	$126T^3$	$168T^3$	$210T^3$	
	3	$\underline{0}$	$\underline{0}$	$I$	$43T^2$	$86T^3$	$129T^3$	$172T^3$	

Fig. 5. The matrix structures of interleaved  $H$  (Ex.3)

**Example 4:** (Nonprime–Prime,  $GCD(L_1, L_2) = 1$ ); Choose non-prime  $L_1 = 44$  for  $H_1$  and prime  $L_1 = 5$  for  $H_2$  to construct  $3 \times 8$  parity check matrix,  $H$  which  $L = 220$ . Case 1

is then used to construct  $H_1$  and  $H_2$  because  $GCD(44, 5) = 1$ . The parity check matrices,  $H$  obtained in this example are shown in Fig.6 and Fig.7 below.

		Column Index							
Row Index	H	1	2	3	4	5	6	7	
	1	$I$	$I$	$I$	$I$	$I$	$I$	$I$	$I$
	2	$\underline{0}$	$I$	45	90	135	180	5	
	3	$\underline{0}$	$\underline{0}$	$I$	46	92	138	184	

Fig. 6. The matrix structures of modified  $H$  (Ex.4)

		Column Index							
Row Index	H	1	2	3	4	5	6	7	
	1	$I$	$I$	$IT$	$IT^2$	$IT^3$	$IT^3$	$IT^3$	
	2	$\underline{0}$	$I$	$45T$	$90T^2$	$135T^3$	$180T^3$	$5T^3$	
	3	$\underline{0}$	$\underline{0}$	$I$	$46T^2$	$92T^3$	$138T^3$	$184T^3$	

Fig. 7. The matrix structures of interleaved  $H$  (Ex.4)

## V. PERFORMANCE EVALUATION

To illustrate the performance of codes designed with the technique proposed in the previous section, we design the codes of 4Kbits block length with slightly high code rate, i.e. 0.81 and 0.9. The high rate is generally required by the data storage system. Designed parameters are shown in table I and II below. The channel is assumed to be AWGN. The decoder iteration limit is set to 30.

TABLE I  
PARAMETERS FOR 4KBITS (R=0.81)

Type of parameter	Block Length (bits)	$j$	$k$	$L$
MAC: prime [9]	4179,3383	4	21	199
CRT: pri $\times$ pri [4]	4263,3451,(29,7)	4	21	203
MAC: prime [9]	4431,3587	4	21	211
CRT: nonpri $\times$ pri	4410,3570,(30,7)	4	21	210
CRT: nonpri $\times$ nonpri	4410,3570,(42,10)	4	21	210

TABLE II  
PARAMETERS FOR 4KBITS (R=0.9)

Type of parameter	Block Length (bits)	$j$	$k$	$L$
MAC: prime [9]	4120,3708	4	40	103
CRT: nonpri $\times$ pri	4080,3672(51,2)	4	40	102
CRT: nonpri $\times$ nonpri	4080,3672(51,6)	4	40	102
CRT: nonpri $\times$ nonpri	4080,3672(51,34)	4	40	102

The available results of [9] were used to compare with our results at similar block length and code rate. Figure 8 shows the results of bit error rate (BER) performance, where  $(n, k), (L_1, L_2)$  represent code length, information length, and sub-matrix size of  $H_1$  and  $H_2$ , respectively. It can be seen that our work has superior performance compared to the original Modified array codes. The codes performance, however, seems to vary upon the selection of the pair-wise parameters. The pair of nonprime-prime yields slightly better performance compared to others.

Figure 9 shows the comparable to that offers by Modified array codes. Only one advantage we can have is that, over code can support any arbitrary length. With the consideration of interleaving and noninterleaving, as shown in Fig. 10,

interleaving can only slightly improve the performance of the code, for instance 0.1 dB at the BER of  $10^{-6}$ .

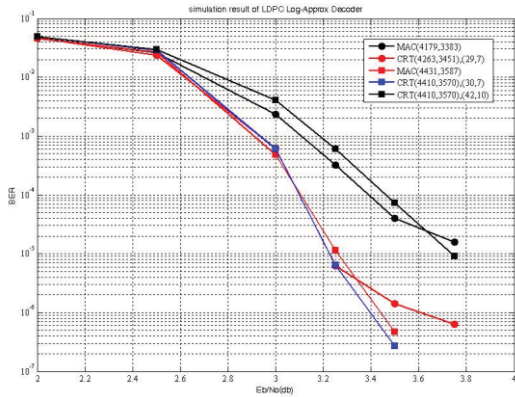


Fig. 8. Codes performance of ours and MAC's at  $R=0.81$

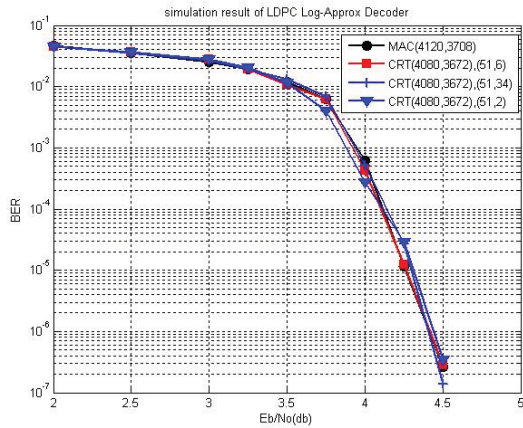


Fig. 9. Codes performance of ours and MAC's at  $R=0.9$ .

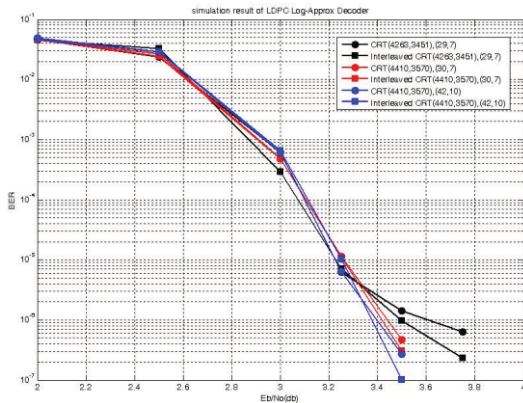


Fig. 10. Codes performance; before and after interleaving

## VI. CONCLUSIONS

We propose a new design of irregular LDPC codes that can support any block length. Using the idea of Chinese Remainder Theorem, we introduced a method to extend the shorten array code length to longer code length without reducing the code performance. Codes constructed with our method differ from [4], [6], [7] in such a way that our codes

can combine the matrix  $H_1$  and  $H_2$  when  $GCD(L_1, L_2) \neq 1$ . With this property, the code can support the arbitrary lengths because we can design matrix  $H_1$  and  $H_2$  with any submatrices size [11]. Our design has quite complicated compared to [6] and [7] but it doesn't generate large girth like [7]. In additions the codes still have the attractive properties of LDPC codes (such as simple encoding, low error floor and capability of detecting and correcting burst error) since the purposed matrices hold the structure as modified array codes. Our results show that even though there are some cycle-4 in  $H_2$ , they do not affect on the codes performance. Our codes have superior performance compared to modified array codes. Furthermore, we used the interleave method to improve the codes performance. The results show that the performance of interleaved codes is slightly higher than non-interleaved codes and it will be much higher, when the SNR is more increased. Of its high rate, the codes are ideal for magnetic recording system where 4Kbytes block length are of interest.

## REFERENCES

- [1] R. G. Gallager, "Low-Density parity-check Codes," *IRE Trans. Inform. Theory*, pp. 21-28, Jan. 1962.
- [2] D. J. C. Mackay and R. M. Neal, "Near Shannon limit performance of low-density parity-check codes," *Electronics Lett.*, vol. 33, pp. 457-458, Mar. 1997.
- [3] Chung, S.-Y., Forney, G. D., Jr. Richardson, T. J., and Urbanke, R. L., "On the design of low-density parity-check codes within 0.0045 dB of the shannon limit," *Electronics Lett.*, vol. 5, pp. 58-60, Feb. 2001.
- [4] S. Myung and K. Yang, "A combing method of quasi-cyclic LDPC codes by the Chinese Remainder Theorem," *IEEE Comm. Lett.*, vol. 9, pp. 823-825, Sept. 2005.
- [5] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE trans. Inform. Theory*, vol. 50, No. 8, pp. 1788-1793, Aug. 2004.
- [6] Y. Liu, X. Wangm, R. Chen, and Y. He, "Generalized Combining Method for Design of Quasi-Cyclic LDPC Codes," *IEEE comm. Lett.*, Vol. 12, No.5, pp. 392-394, May, 2008.
- [7] X. Jiang and M. H. Lee, "Large Girth Quasi-Cyclic LDPC Codes Based on the Chinese Remainder Theorem," *IEEE comm. Lett.*, Vol. 13, No. 5, pp. 342-344, May, 2009.
- [8] J. L. Fan, "Array Codes as Low-Density Parity-Check Codes," in *Proc. 2nd Int. Symp. on Turbo Codes*, Brest, France, Sept. 4-7, 2000, pp. 543-546.
- [9] 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.
- [10] C. Prasartkaew and S. Choomchuay, "A Parity Check Matrix Design for Irregular LDPC Codes with 2K Block Length," *ISPAICS Int. Symp. on Intelligent Signal Processing and Comm. Systems*, Dec. 7-9, 2009.
- [11] D. Abematsu, T. Ohtsuki, S. PW Jarot, and T. Kashima, "Size Compatible (SC)-Array LDPC Codes," *IEEE Vehicular Technology Conference 2007*, pp. 1147-1151, 2007.
- [12] K. H. Rosen, *Elementary Number Theory and Its Applications*. Reading, MA: Addition-Wesley, pp. 322-324, 2000.
- [13] C. Chusin, C. Prasartkaew and S. Choomchuay, "A Design of Non-prime LDPC Based on Interleave Modified Array Codes", *Inte. Data Storage Technology Conf. DST-CON 2010*, July 2010.
- [14] W. Singhaudom, S. Noppankeepong, P. Suphithi, "Design of High-Rate Modified Array Codes for Magnetic Recording System," *ECTI International Conference*, May 2007.