IJICTR International Journal of Information & Communication Technology Research

Volume 8- Number 2- Spring 2016 (45-50)

QC-LDPC Codes Construction by Concatenating of Circulant Matrices as Block-Columns

Mohammad Hesam Tadayon
Iran Telecommunication Research Center (ITRC)
Tehran, Iran
tadayon@itrc.ac.ir

Mohammad Mohammadi
Malek-Ashtar University
Isfahan, Iran
Amohamadi70@gmail.com

Received: June 14, 2015- Accepted: March 17, 2016

Abstract—**In this paper a new low complexity method for constructing binary quasi-cyclic low-density parity-check (QC-LDPC) codes is introduced. In the proposed method, each block-column of the parity check matrix *H* is made by a circulant matrix in a way that the associated Tanner graph is free of cycle four. Each circulant matrix in *H* is made by a generator column. The generator columns should be selected in a way that each associated circulant matrix and every two distinct circulant matrices are free of cycle four. The generator columns are made by row distance sets. An algorithm for generating distance sets and obtaining circulant matrices with columns of weight three is presented separately. Simplicity of construction and having a good flexible family of quasi cyclic LDPC codes both in rate and length are the main properties of the proposed method. The performance of the proposed codes is compared with that of the random-like and Array LDPC codes over an AWGN channel. Simulation results show that from the performance perspective, the constructed codes are competitive with random-like and Array LDPC codes.**

Keywords- QC-LDPC codes, girth, circulant matrices, AWGN channel, concatenation.

I. INTRODUCTION

QC-LDPC codes are a family of capacity-approaching and high performance error correcting linear codes [1, 2]. Construction of these codes is divided into two categories: random-like codes, such as [1, 2] and structured codes, such as [3-12]. As mentioned in many papers, the encoding complexity of quasi-cyclic codes is extremely low [3-5]. In general, QC-LDPC codes are constructed by two main methods: superposition techniques [4, 9] and parity check matrices derived by circulant matrices [6, 8].

The proposed method in this paper can produce QC-LDPC codes with different lengths and rates. A parity check matrix H has been constructed by concatenation of circulant matrices as block-columns. Each circulant matrix is constructed by a generator column with an arbitrary considered weight. We must take an order on nonzero elements of each generator column such that each associated circulant matrix and every two disjoint circulant matrices be free of cycle four. Therefore the associated Tanner graph of parity check matrix *H* will have girth at least six. Constructed quasi-cyclic LDPC codes in this paper can have arbitrary column weights, lengths and rates. Therefore the main task in this paper is to construct appropriate generator columns. We have introduced a method of constructing particular sets, known as row distance sets, which are used for constructing generator columns. Furthermore, we represent generator columns by generator polynomials that demonstrate a simple exhibition of *H*. The performance of the proposed codes on an AWGN channel by sum-product algorithm (SPA) decoding is examined and compared with that of the random-like and Array LDPC codes as well-known QC-LDPC codes [13]. Simulation results show that the constructed

QC-LDPC codes outperform random-like and Array LDPC codes. There exist some papers for the construction of QC-LDPC codes based on difference sets [12, 14, 15]. They are indeed very similar to our work, but they are based on some algebraic and combinatory methods with inherent restriction on using and making various difference sets. Our method approach to constructing QC-LDPC codes that are not directly related to difference sets, but can be a generalization of them on constructing a large family of QC-LDPC codes.

This paper is organized as follows: The method of constructing a quasi-cyclic parity check matrix by generator columns and associated circulant matrices is introduced in Section II. The technique and algorithm of constructing the appropriate generator columns by row distance sets are given in Section III. A simple representation of generator columns and parity check matrix H by generator polynomials is introduced in Section IV. Simulation results are presented in Section V. Section VI concludes the paper.

II. PARITY CHECK MATRIX CONSTRUCTION BASED ON THE CIRCULANT MATRICES

Let the parity check matrix H of an LDPC code be denoted by

$$H= [A_1\ A_2\ \ldots\ A_n], \qquad (1)$$

where each A_i, $1\leq i \leq \theta$ is a circulant matrix with arbitrary column weight. To avoid girth four, parity check matrix H must have the following condition:

Condition 1

1. any sub-matrix A_i be free of cycle four,

2. matrix $[A_i, A_j]$ for $1\leq i\neq j \leq \theta$ is free of cycle four.

Definition 1 *The row distance σ between two nonzero components a and b in a fixed column of a circulant matrix A_k is determined one greater than the number of rows containing a and b and it is shown by $m_{ab}^k= \sigma$.*

Definition 2 *A set of row distances of nonzero elements in a fixed column of a circulant matrix is called a row distance set.*

Definition 3 *The first column of a circulant matrix is called a generator column.*

Every circulant matrix A_i, $1\leq i \leq \theta$ in (1) made by a fixed cyclically shifting the associated generator column and every generator column is made from associated row distance set. Hence, first of all, we focus on constructing appropriate row distance sets.

Example 1 In Fig. 1 there are four row distances in a column of weight three (including three nonzero components a, b and c). So the row distances are:

1. The row distance between a and b is: $m_{ab}= 1$,

2. The row distance between b and c is: $m_{bc}= 2$,

3. The row distance between a and c is: $m_{ac}= 3$,

4. The row distance between c down to the first nonzero component a is $m_{ca}= 4$.

So the row distance set is $R=\{ m_{ab}= 1, m_{bc}= 2, m_{ac}= 3, m_{ca}= 4\}$. The circulant matrix obtained by cyclically shifting the associated generator column is shown in Fig. 2, note that $a=b=c=1$.

Remark 1 *In a column between every two nonzero components there is a row distance, so in a column of weight w, there is a row distance set with the cardinality of at most $\binom{w}{2}+1$.*

The circulant matrices A_i, $1\leq i \leq \theta$ in (1) will be produced by different row distance sets such that the Condition 1 is satisfied. Therefore we have the following outcomes.

Proposition 1 *An associated Tanner graph of a circulant matrix produced by a column generator of weight w and row distance set of cardinality $\binom{w}{2}+1$ is free of cycle four.*

Proof: Obviously, when the cardinality of a row distance set of a column generator of weight w is $\binom{w}{2}+1$, then the row distances between nonzero components of the generator column are different and under a fixed cyclically shifting on the column generator, the Tanner graph of the produced circulant matrix will have no cycle of length four.□

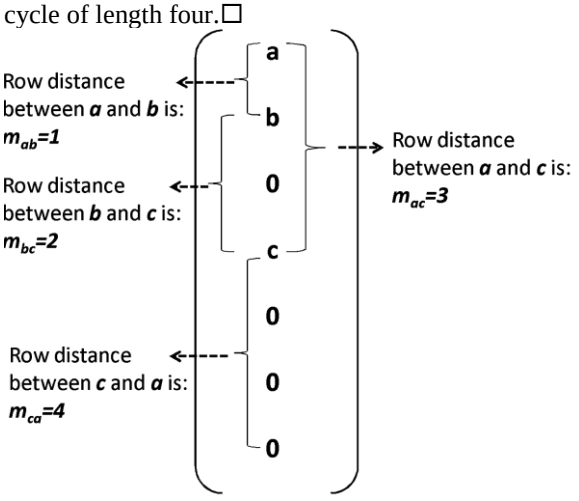

Fig 1: Four row distances between the three nonzero components a, b and c in a column.

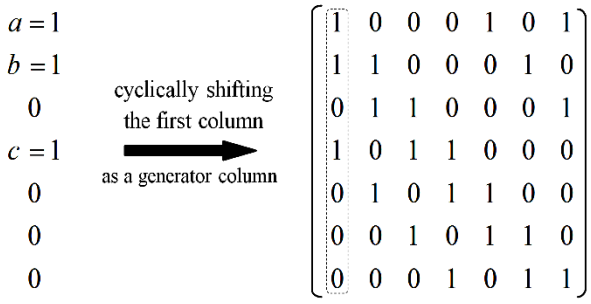

Fig 2: Cyclically shifting the generator column in Fig.1 to produce a circulant matrix.

Theorem 1 *If every two disjoint row distance sets, corresponding to two distinct generator columns, have no intersection and every associated circulant matrix of them satisfies Proposition 1, then there is no cycle of length four in Tanner graph made by the concatenation of their circulant matrices.*

Proof: Let A_1 and A_2 be two distinct circulant matrices pertaining to the generator columns G_1 and G_2, which satisfy Proposition 1. Without loss of generality, we assume that the generator columns G_1 and G_2 have weight three. Let nonzero components of generator column G_1 and G_2 be $\{a, b, c\}$ and $\{ \acute{a}, \acute{b}, \acute{c} \}$, respectively. So the row distance set of the generator column G_1 and G_2 are $R_1=\{ m^1_{ab}, m^1_{bc}, m^1_{ac}, m^1_{ca}\}$ and $R_2=\{ m^2_{a'b'}, m^2_{b'c'}, m^2_{a'c'}, m^2_{c'a'} \}$, respectively. We know that matrices A_1 and A_2 are made by a fixed cyclically shifting of the generator columns G_1 and G_2. So by Proposition 1, circulant matrices A_1 and A_2 will be free of cycle four (Condition 1 (i)). Since $R_1 \cap R_2 = \emptyset$ and circulant matrices A_1 and A_2 are constructed by a fix cyclical shift to their generator columns G_1 and G_2, respectively, then by concatenating matrices A_1 and A_2 the associated Tanner graph will be free of cycle four (Condition 1 (ii)).□

Corollary 1 *concatenating any two disjoint circulant matrices that satisfy Theorem 1, results in parity check matrix with a Tanner graph free of cycle four.*

III. CONSTRUCTION OF CIRCULANT MATRICES

In the following, to construct the parity check matrix of the form given by (1), we have focused on the appropriate row distance sets that satisfy Corollary 1.

Remark 2 *Proposition 2 is intended to construct parity check matrix with column weight three. However it can be easily generalized for column weights greater than three by enforcing more restrictions on the involved distance sets.*

Proposition 2 *Let parity check matrix H in (1) satisfy Proposition 1 and Theorem 1, and also circulant matrices A_k, $1 \le k \le \theta$, in (1), be $h \times h$ matrices with a column weight three. Then there exist disjoint distance sets $R_i = \{n_{i1}, n_{i2}, n_{i3}, n_{i4}\}$ and $R_{i'} = \{n_{i'1}, n_{i'2}, n_{i'3}, n_{i'4}\}$ associated to circulant matrix A_i and $A_{i'}$, so that the following restrictions hold:*

$$1 \le n_{ij}, n_{i'j} < h, 1 \le j \le 4, i \ne i',$$

$$n_{ij} \ne n_{ij'}, 1 \le j, j' \le 4, j \ne j', \quad (2)$$

$$n_{i1} + n_{i2} = n_{i3}, \quad (3)$$

$$n_{i1} + n_{i2} + n_{i4} = h, \quad (4)$$

$$n_{ij} \ne n_{i'j}, i \ne i', 1 \le j \le 4, \quad (5)$$

$$n_{i'j} \ne n_{i'j'}, 1 \le j, j' \le 4, j \ne j', \quad (6)$$

$$n_{i'1} + n_{i'2} = n_{i'3}, \quad (7)$$

$$n_{i'1} + n_{i'2} + n_{i'4} = h. \quad (8)$$

Proof: The weight of the generator columns is three and the associated circulant matrices in (1) are $h \times h$. At first, let $R_i = \{ n_{i1}, n_{i2}, n_{i3}, n_{i4} \}$ be a distance set pertaining to sub-matrix A_i in (1), where $1 \le n_{ij} \le h$, $1 \le j \le 4$. For Proposition 1 to be established, elements of R_i must be satisfied in (2)-(4). It is evident that another distance set $R_{i'} = \{n_{i'1}, n_{i'2}, n_{i'3}, n_{i'4}\}$, $i \ne i'$, which is associated to the sub-matrix $A_{i'}$ in (1) (where $1 \le n_{i'j} < h, 1 \le j \le 4$) must be disjoint from R_i and so according to Proposition 1 and Corollary 1 must be satisfied in (5)-(8). Intuitively, the above-mentioned constraints must be satisfied for every pair of disjoint distance sets.□

Example 2 For positive integer $h = 15$, there are two disjoint distinct sets that satisfy Proposition 2. $R_1 = \{1, 2, 3, 12\}$ and $R_2 = \{4, 5, 9, 6\}$ since for R_1

$$1 \ne 2 \ne 3 \ne 12,$$

$$1 + 2 = 3,$$

$$1 + 2 + 12 = 15,$$

and for R_2

$$1 \ne 2 \ne 3 \ne 4 \ne 5 \ne 6 \ne 9 \ne 12,$$

$$4 + 5 = 9,$$

$$4 + 5 + 9 = 15.$$

Therefore,

$$R_1 \cap R_2 = \emptyset.$$

Based on Proposition 2, we can have the following algorithm that generates all row distance sets for an arbitrary positive integer h (size of circulant matrices in (1)).

Algorithm 1 Generating row distance sets

Input: h (size of circulant matrices A_k in (1)) and $w = 3$ (weight of a generator column).

Output: row distance sets R_i, $1 \le i \le \tau$ (τ is the maximum number of row distance sets).

Assume a, b and c are three nonzero components in a generator column from top to bottom.

Start

- $i = 1$, $R_1 = \emptyset$;
- While ($R_i \cap R_{i-1} = R_i \cap R_{i-2} = \ldots = R_i \cap R_1 = \emptyset$)
  do {
  - $i = i+1$;
  - assign a positive integer smaller than h to m^i_{ab} : *(row distance between two nonzero elements a and b.)*

-assign a positive integer smaller than h to m_{bc}^i, such that $m_{ab}^i \neq m_{bc}^i$; (row distance between two nonzero elements b and c.)
-set $m_{ac}^i = m_{bc}^i + m_{ab}^i$, $1 \leq m_{ac}^i < h$; (row distance between the two nonzero elements a and c.)
- $m_{ca}^i = h - m_{ac}^i$ such that $m_{ac}^i \neq m_{ca}^i \neq m_{ab}^i \neq m_{bc}^i$ and $1 \leq m_{ca}^i < h$; (row distance between the two nonzero element c down to the first element a.)
-set R_i={m_{ab}^i, m_{bc}^i , m_{ac}^i, m_{ca}^i};
}
-τ=i;
End

The row distance sets, given by the above algorithm, and their associated generator columns can produce circulant matrices in a way that the Tanner graph of the parity check matrix *H* in (1) be free of cycle 4.

Example 3 Let *h = 21*. According to Algorithm 1, there are three row distance sets (τ = 3) as follows:

$$R_1 = \{m_{ab}^1 , m_{bc}^1 , m_{ac}^1 , m_{ca}^1\} = \{1, 2, 3, 18\},$$
$$R_2 = \{m_{ab}^2 , m_{bc}^2 , m_{ac}^2 , m_{ca}^2\} = \{4, 5, 9, 12\},$$
$$R_3 = \{m_{ab}^3 , m_{bc}^3 , m_{ac}^3 , m_{ca}^3\} = \{6, 7, 13, 8\}.$$

We can see the maximum number of row distance sets obtained by applying Algorithm 1 and varying the value of *h* in the first two columns of Table 1.
In Table 2, some binary QC-LDPC codes with different lengths and rates for a fixed values of *h* and different value of *θ*, where $1 \leq \theta \leq \tau(= 40)$, are presented.

TABLE 1. PARAMETERS OF CONSTRUCTED BINARY QC-LDPC CODES WITH COLUMN WEIGHT 3 AND MAXIMUM NUMBER OF CIRCULANT MATRICES (θ = τ).

h (size of circulant matrices)	*τ* (maximum number of circulant matrices)	*n*	*k*	*r* (rate)
52	7	364	312	0.85
67	9	603	536	0.88
76	10	760	684	0.9
82	11	902	820	0.909
90	12	1080	990	0.916
97	13	1261	1146	0.923
120	16	1920	1800	0.937
127	17	2159	2032	0.941
150	20	3000	2850	0.95
172	23	3956	3784	0.956
202	27	5454	5252	0.962
292	40	11680	11388	0.975

IV. CONSTRUCTING CIRCULANT MATRICES VIA POLYNOMIALS ON F_2

Let *a*, *b* and *c* be three nonzero components in a generator column from top to bottom ($a, b, c \in F_2$) and R_i={ m_{ab}^i , m_{bc}^i , m_{ac}^i , m_{ca}^i } be the associated row distance set. A generator polynomial over F_2 associated with this row distance set can be defined as:

$$g_i(x) = 1 + x^{m_{ab}^i} + x^{m_{ac}^i}, \qquad (9)$$

where degree $(g_i(x)) = m_{ac}^i$. Circulant matrix A_i of size $h \times h$ can be determined as follows:

$$A_i = \begin{pmatrix} g_i(x) & xg_i(x) & \cdots & x^{h-1}g_i(x) \end{pmatrix},$$

where polynomials $g_i(x)$ are considered to be columns of A_i.

Example 4: Let *h = 15*, according to Example 2, we can construct the parity check matrix $H = (A_1 \ A_2)$ of size 15 × 30 based on two row distance sets
R_1={$m_{ab}^1 = 1$, $m_{bc}^1 = 2$, $m_{ac}^1 = 3$, $m_{ca}^1 = 12$},
R_2={$m_{ab}^2 = 4$, $m_{bc}^2 = 5$, $m_{ac}^2 = 9$, $m_{ca}^2 = 6$}.
According to (9), the associated generator polynomials $g_1(x)$ and $g_2(x)$ are:

$$g_1(x) = 1 + x^{m_{ab}^1} + x^{m_{ac}^1} = 1 + x^1 + x^3,$$

where $g_1(x)$ generates circulant matrix A_1 and

$$g_2(x) = 1 + x^{m_{ab}^2} + x^{m_{ac}^2} = 1 + x^4 + x^9,$$

where $g_2(x)$ generates circulant matrix A_2. The resultant parity check matrix *H* is shown in Fig. 3.
We compare performance of some of our codes with that random-like codes and Array LDPC codes in the next section.

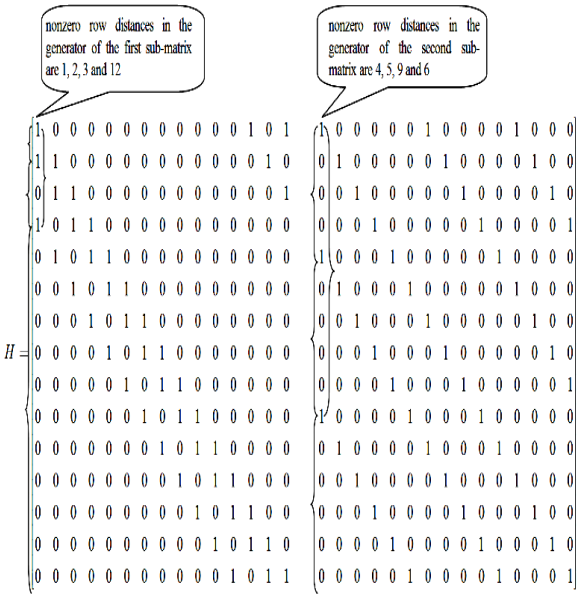

Fig. 3 Parity checks matrix *H* and circulant matrices made by generator columns in Example 4.

TABLE 2. PARAMETERS OF CONSTRUCTED BINARY QC-LDPC CODES FOR *H = 292*, $1 \leq \theta \leq \tau(= 40)$, COLUMN WEIGHT THREE, ROW WEIGHT 3θ AND DIERENT RATES IN MATRIX (1).

θ	*n*	*k*	*r*
2	584	292	0.5
3	876	584	0.66
4	1168	876	0.75
5	1460	1168	0.8
6	1752	1460	0.83
7	2044	1752	0.85
⋮	⋮	⋮	⋮
40	11680	11388	0.975

TABLE 3. PARAMETERS OF SOME CONSTRUCTED BINARY QC-LDPC CODES WITH COLUMN WEIGHT THREE.

h	τ	row weight	n	k	r
150	20	60	3000	2850	0.95
210	28	84	5880	5670	0.964
226	30	90	6780	6554	0.966
256	34	102	8704	8448	0.97

V. SIMULATION RESULTS

According to Table 3 and the discussions in Section II and III, we have constructed some *(n, k, r)* QC-LDPC codes with a minimum distance at least four so that the associated Tanner graph has no cycle of length four. These codes, in the following examples, have been compared with random-like LDPC codes, using the software in [16], and Array LDPC codes under SPA decoding on AWGN channels with maximum 50 iterations. Furthermore, by removing some circulant matrices in (1), one can obtain dierent codes with desired lengths and rates.

Example 5 Let $h = 256$. The associated parity check matrix given by Table 3 is:

$$H = (A_1 \ A_2 \ A_3 \ \cdots \ A_{34},),$$

where each circulant matrix A_i, $1 \le i \le 34$, is of size 256×256 and constructed by the proposed method in Section III. The null space of matrix H gives a *(8704, 8448, 0.97)* binary QC-LDPC code. The BER performance of this code over an AWGN channel is shown in Fig. 4 and this code is compared with random-like code and Array LDPC code of near length and rate. At a BER of 10^{-6}, the constructed *(8704, 8448, 0.97)* QC-LDPC code achieves approximately *0.2 dB* gain over the random-like code and *0.2 dB* gain over the Array LDPC code. In addition, the constructed code has better waterfall curve compared to Array LDPC code.

Example 6: Let $h = 226$. The associated parity check matrix given by Table 3 is:

$$H = (A_1 \ A_2 \ A_3 \ \cdots \ A_{30}),$$

where each circulant matrix A_i, $1 \le i \le 30$, is of size 226×226. The null space of matrix H gives a *(6780, 6554, 0.966)* binary QC-LDPC code. The BER performance of this code over an AWGN channel is shown in Fig. 4 and this code is compared with random-like code and Array LDPC code of the near length and rate. At a BER of 10^{-6}, the constructed *(6780, 6554, 0.966)* QC-LDPC code achieves approximately *0.08 dB* gain over the random-like code and *0.4 dB* gain over Array LDPC codes.

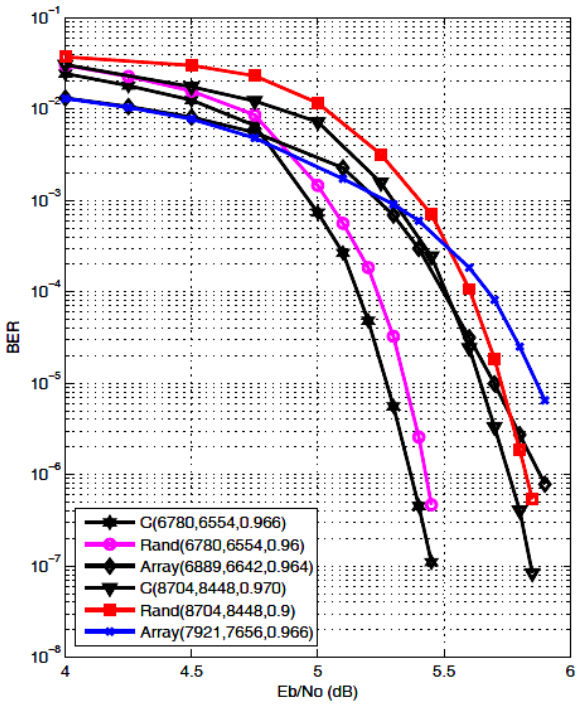

Fig. 4 Error performance of (8704, 8448, 0.970) QC-LDPC code and (6780, 6554, 0.966) QC-LDPC code in Examples 5 and 6.

Example 7 Let $h = 210$. The associated parity check matrix given by Table 3 is:

$$H = (A_1 \ A_2 \ A_3 \ \cdots \ A_{28}),$$

where each circulant matrix Ai, $1 \le i \le 28$, is of size 210×210. The null space of matrix H gives a *(5880, 5670, 0.964)* binary QC-LDPC code. The BER performance of this code over an AWGN channel is shown in Fig. 5 and this code is compared with random-like code and Array LDPC code of the same length and rate. At a BER of 10^{-5}, the constructed (5880, 5670, 0,964) QC-LDPC code achieves approximately 0.1 dB gain over the random-like code and Array LDPC code and it has better waterfall curve than them at BER of 10^{-6}.

Example 8 Let $h = 150$. The associated parity check matrix by Table 3 is:

$$H = (A_1 \ A_2 \ A_3 \ \cdots \ A_{20}),$$

where each circulant matrix A_i, $1 \le i \le 20$, is of size 150×150. The null space of matrix H gives a *(3000, 2850, 0.950)* binary QC-LDPC code. The BER performance of this code over an AWGN channel is shown in Fig. 5 and this code is compared with random-like code and Array LDPC code of the near length and rate. At a BER of 10^{-6}, the constructed *(3000, 2850, 0.950)* QC-LDPC code achieves approximately *0.15 dB* gain over the random- like code and *0.2 dB* Gain over the Array LDPC code.

The figures confirm that from the performance perspective, the constructed codes compete with and even outperform the random-like codes and Array LDPC codes.

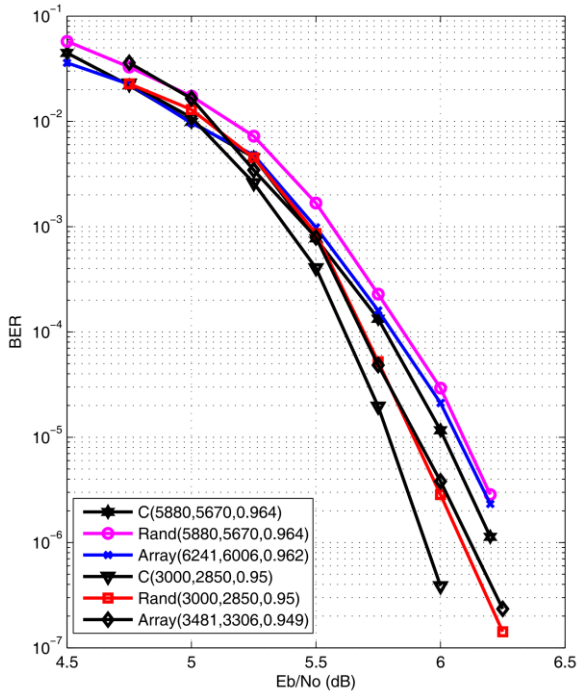

Fig. 5 Error performance of (5880, 5670, 0.964) QC-LDPC code and (3000, 2850, 0.95) QC-LDPC code in Examples 7 and 8.

VI. CONCLUSION

This paper considers a new and different QC-LDPC codes construction method by row distance sets with girth of at least six. Unlike the previous QC-LDPC code construction methods which were based on combinatorial designs and nite geometries, our method can produce a family of QC-LDPC codes with variable lengths and rates easily. Multi-rate QC-LDPC codes can be used in practical applications, particulary suitable particularly in wireless communications. Moreover by the introduced technique, we can simply construct a family of high rate QC-LDPC codes. The parity check matrices of these codes can be constructed by generator polynomials over F_2. We saw that the proposed codes perform comparably to the well-known Array LDPC codes, and have better waterfall curve than them. The results also confirm that from the performance perspective, the random-like LDPC codes at short to moderate code lengths are not better than the constructed codes by our method over AWGN channels. Moreover the proposed codes are quasi-cyclic and hence, their encoding can be implemented with linear shift-registers in linear time. Constructing LDPC codes with girth larger than eight can be achieved by putting more restrictions on the proposed technique and is the subject of a new research.
Therefore, constructing QC-LDPC codes with girths larger than six can be considered as a novel work by the proposed technique in this paper.

REFERENCES

[1] 1. R.G.Gallager, "Low-density parity-check codes,'' IRE Trans. Inf. Theory, vol. 18, pp.21-28, November 1962.

[2] D.J.C.Mackay and R.M.Neal, "Good codes based on very sparse matrices," in Proc. 5th IMA Conf. Cryptography and Coding., vol. 1025, 1995, pp. 100-111.

[3] M.Esmaeili, M.H.Tadayon, and T.A.Gulliver, "Low-complexity girth-8 high-rate moderate length qc ldpc codes," AEU-International Journal of Electronics and Communications, vol. 64, pp. 360-365, 2010.

[4] M.Esmaeili and M.H.Tadayon, "A novel approach to generating long ldpc codes using two congurations," IET Commun., vol. 2, no. 4, pp. 587-597, 2008.

[5] "A lattice-based systematic recursive construction of quasi-cyclic ldpc codes,"IEEE Transactions on Commun., vol. 57, no. 10, Oct. 2009.

[6] M.P.C.Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," IEEE Trans. Inf. Theory, vol. 50, no. 8, pp. 1788-1793, 2004.

[7] B.Vasic and O.Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," IEEE Trans. Inf. Theory, vol. 50, no. 6, pp. 1156-1176, 2004.

[8] R.M.Tanner, D.Sridhara, A.Sridhara, T.E.Fuja, and D.J.Costello, "Ldpc block and convolutional codes based on circulant matrices," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 2966-2984, 2004.

[9] J.Xu, L.Chan, L.Lin, and S.Lin, "Construction of low density parity-check codes by superposition," IEEE Transaction on Commun., vol. 50, no. 2, pp. 243-251, 2005.

[10] O.Milenkovic, I.B.Djordjevic, and B.Vasic, "Block-circulant low-density parity-check codes for optical communication systems," IEEE Journal of Selected Topics in Quantum Electronics, vol. 10, no. 2, pp. 294-299, 2004.

[11] Y.Kou, S.Lin, and M.P.C.Fossorier, "Low-density parity-check codes based on nite geometries: a rediscovery and new results," IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 2711-2736, 2001.

[12] S. J. Johnson and S. R. Weller, "A family of irregular ldpc codes with low encoding complexity," IEEE Communications Letters, vol. 7, no. 2, pp. 79-89, 2003.

[13] J.L.Fan, "Array codes as low-density parity-check codes," in Proc. Int. Symp. Turbo Codes, Sep. 2000, pp. 543-546.

[14] T. Xia and B. Xia, "Quasi-cyclic codes from extended di erence families," in IEEE conference Wireless Communications and Networking, vol. 2, 2005, pp. 1036-1040.

[15] M. Fujisawa and S. Sakata, "A class of quasi-cyclic regular ldpc codes from cyclic difference families with girth 8," in International Symposium on Information Theory,2005, pp. 2290-2294.

[16] http://www.cs.utoronto.ca/radford/ldpc.software.html,2012.

Mohammad Hesam Tadayon received his B.Sc. degree in mathematics from the University of Mazandaran, Babolsar, Iran, in 1995, his M.Sc. degree in mathematics from the University of Tarbiat Modarres, Tehran, Iran, in 1997, and his Ph.D. degree in applied mathematics (coding and cryptography) from the University of Tarbiat Moallem of Tehran (Kharazmi), Tehran, Iran, in 2008. He is now an Assistant Professor at the Iran Telecommunications Research Center. His research interests include error control coding & information theory and security.

Mohammad Mohammadi received his B.Sc. degree in applied mathematics from Payame Noor University in 2007 and his M.Sc. degree in Communication engineering from Malek Ashtar University of Technology in 2010. His research interests include error control coding and cryptography.