VOL. 13, NO. 3, FEBRUARY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

CONSTRUCTION OF REGULAR QUASI CYCLIC-LOW DENSITY PARITY CHECK CODES FROM CYCLIC CODES

Bouchaib Aylaj[1], Mostafa Belkasmi[2], Said Nouh[3] and Hamid Zouaki[1]
[1]Department of Maths, LIMA Lab, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco
[2]SIME Labo, ENSIAS, TIM Lab, Mohammed V. University, Rabat, Morocco
[3]Faculty of Sciences Ben M'sik, Hassan II University, Casablanca, Morocco
E-Mail: bouchaib_aylaj@yahoo.fr

ABSTRACT

Low Density Parity Check Codes (LDPC) are a class of linear error-correcting codes which have shown ability to approach or even to reach the capacity of the transmission channel. This class of code approaches asymptotically the fundamental limit of information theory more than the Turbo Convolutional codes. It's ideal for long distance transmission satellite, mobile communications and it's also used in storage systems. In this paper, a new method for constructing quasi-cyclic low density parity-check (QC-LDPC) codes derived from cyclic codes is presented. The proposed method reduces the incidence vectors, by eliminating the conjugates lines in parity-check matrix of the derived cyclic code to construct circulant shifting sub-matrices. In the end, this method produces a large class of regular LDPC codes of quasi-cyclic structure having very low density, high coding rates and Tanner graphs which have no short cycles with girth of at least 6. Performance with computer simulations are also shown in this work for some constructed codes.

Keywords: LDPC codes, cyclic codes, quasi-cyclic codes, minimum distance.

1. INTRODUCTION

LDPC codes were invented by Robert Gallagher [1] [2] in the early 1960s; in his doctoral thesis he has proposed a pseudo-random method which generated good LDPC codes. However, the lack of a well defined mathematical structure has made the coding/decoding system very complex for this family of codes. Shortly, after their invention, these codes have been forgotten largely, until 1981 when Tanner [3] gave them a new interpretation: a graphical representation. His theory has also been ignored more than 14 years until the rediscovery of these codes by MacKay in 1995 [4]. These codes have made a big comeback. Recently, they have become the topic of many research activities in the coding theory. It has been proved that the LDPC codes have a minimum distance that increases linearly with code's length [5]. Mackay and Neal [6]have demonstrated that these codes can approach the Shannon limit more than the turbo codes, later, in 2001, Richardson *et al.* [7] have proved that irregular LDPC codes outperform the turbo codes for long codes.

LDPC codes have been used in many practical applications: they are applied in Code Division Multiple Access (CDMA), Orthogonal Frequency Division Multiplexing (OFDM) systems and space-time coding systems. Recently, they have been adopted in several digital video transmission standards DVB-S2, DVB-NGH, radio standards (IEEE 802.16m mobile), and local radio networks (IEEE 802.11n). Also, they are used for real-time applications such as magnetic storage, high-speed for Ethernet and local area networks (WLAN)

A Low Density Parity Check Code is a linear block code that's the parity check matrix H has a low density of 1's [1]. The sparseness of the H matrix has several advantages (coding, decoding, minimum distance ...)

In this work we are interested in the problems related to the improvement of the error-correcting performances of LDPC codes. This improvement can be made during the construction of the LDPC codes or during their decoding operation. We focus on improving the construction in terms of various parameters that cause problems in order to construct good LDPC codes: density, coding rate, minimum distance and girth of Tanner graphs. This construction improvement is made on the special sub-class of LDPC codes, named quasi-cyclic (QC) LDPC codes that are well studied in the literature for various mathematical properties assured by the cyclic structure of code. In addition, they can be encoded with less complexity using shift registers and no need to store full G or H matrix of QC-LDPC for encoding or decoding operations, that's why this class of code is the most efficient in hardware implementation. As already mentioned, the first construction of LDPC codes has been proposed by Gallager [2] in 1962. The construction of the parity check matrix H of an LDPC code Gallagher's consists firstly to build a matrix H_s having a column weight w_c and a row weight equal to w_r. Then we define random permutations Γ_j of columns of this sub-matrix H_s to form others sub-matrices, the regular H matrix Gallager's is then formed as follow.

$$H = \begin{bmatrix} \Gamma_1(H_s) \\ \Gamma_2(H_s) \\ \mathbf{M} \\ \Gamma_{w_c}(H_s) \end{bmatrix} \quad (1)$$

Various algebraic or random methods for the construction of regular or irregular LDPC codes of quasi-cyclic structure have been proposed, the authors in [8-12] have already presented a survey of works which have been

carried by algebraic constructions based on finite geometries, elements of finite fields and RS codes. Yi *et al.* [13] for their part have given an algebraic method for constructing regular QC-LDPC codes based on narrow-sense-primitive BCH codes, this construction method resulted in a class free of cycles of length 4. On the other hand, Tomlinson et al. [14] have shown how to construct an algorithm to search for binary idempotents which may be used to construct binary LDPC codes. Fossorier [15] has investigated construction of (LDPC) codes from circulant permutation matrices, and he has shown that such codes cannot have a Tanner graph representation with girth larger than 12. In [16] S. Aly *et al*. have presented two algebraic methods for constructing regular LDPC codes which were derived, one from nonprimitive narrow sense BCH codes and the second directly from cyclotomic cosets. In [17] the authors have presented a construction of High-Rate Regular Quasi-Cyclic LDPC Codes based on cyclic difference families. Authors in [19] have proposed « a new code structure for QC LDPC codes with multi-weight circulant matrices by introducing overlapping matrices»

In this paper, we present an algebraic method for constructing binary regular LDPC codes based on cyclic codes, which we named MC-LDPC. The construction method produces a class of LDPC codes of quasi-cyclic structure having a good minimum distance, a high coding rate and it is distinguished from the previously construction given in the literature [13-17] by the following properties:

- Generalization of the construction: making derivation from any cyclic code by using non-primitive elements of extension Galois field $GF(q^m)$
- A very low complexity of coding and decoding by reducing the parity matrix by 50%, which is efficient because if the parity matrix check matrix is further reduced, then a better of error-correcting performance is obtained
- A very low density which implies that the graph will contain no cycle of length 4 and with girth of at least 6.
- The dimension and the minimum distance are bounded for constructed codes.

The remainder of this paper is organized as follows. On the next section, we give an introduction on cyclic, quasi-cyclic codes and BCH codes. In section 3 we present the proposed constructing method of regular QC-LDPC codes. The proprieties of generated QC-LDPC codes are presented in section IV. And we present the performance of constructed codes with computer simulations in section V. Finally, a conclusion and a possible future direction of this research are outlined in section VI.

2. CODES OF CYCLIC STRUCTURE

A. Cyclic codes

Cyclic codes are a class of error correcting codes that can be efficiently encoded and decoded using simple shift registers and combinatorial logic elements, on the basis of their representation using polynomials [18].

Let $C(n, k)$ denote a linear block code. The code C is cyclic if and only if every cyclic shift of a code word is another code word. An important property of cyclic codes is that all code polynomials are multiples of a unique polynomial, g(x) called the generator polynomial of the code. It can be shown that the generator polynomial g(x) divides $(x^n - 1)$ Therefore, to find a generator polynomial, the polynomial $(x^n - 1)$ must be factored into its irreducible factors

$\varphi j\,(x), j = 1, 2, \ldots, l,$

$$(x^n - 1) = \varphi_1(x)\varphi_2(x) \ldots \varphi_l(x) \quad (2)$$

Also, note that over the field of binary numbers. As a consequence of the above, the polynomial $g(x)$ is given by

$$g(x) = \prod_{j \in J \subset \{1,2,\ldots l\}} \varphi_j(x) \quad (3)$$

Definition 1:

The operation of multiplying by q divides the integer *mod N* into sets called the cyclotomic cosets *mod N*.

The cyclotomic coset C_i containing i consists of $Ci=\{i,qi,iq^2,\ldots,iq^j\}$

Where j is the smallest positive such that $iq^j = i\ (modN)$

Each cyclotomic class is a set of conjugate roots (the powers of the primitive root).

Definition 2:

We define a minimal polynomial m_i associated with cyclotomic cosets C_i, by the following equation:

$$m_i = \prod_{j \in C_i} (x - \alpha^j) \quad (4)$$

Cyclotomic cosets can determine the number of irreducible factors of $x^N - 1$. They allow to find all minimal polynomials m_i of $x^N - 1$ (all factors of $x^N - 1$).

B. Quasi-Cyclic codes

Quasi-cyclic (QC) codes are a generalization of cyclic codes where a cyclic shift of a codeword by p positions results in another codeword. Therefore, cyclic codes are QC codes with $p = 1$.

The QC codes can be described by circulant matrices. A circulant matrix is defined to be a square matrix A of the form

$$A=\begin{pmatrix} a & a_1 & a_2 & .... & a_{n-1} \\ a_{n-1} & a_0 & a_1 & .... & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & .... & a_{-3} \\ & .... & & & \\ a_1 & a_2 & a_3 & & a_0 \end{pmatrix} \quad (5)$$

Where each successive row a cyclic shift of the previous one

C. BCH codes

BCH codes, as a class, are one of the most known powerful error-correcting cyclic codes. The most common BCH codes are characterized as follows: specifically, for any positive integer $w \geq 3$, and $t < 2^w - 1$, there exists a binary BCH code with the following parameters:

- Block length: $n=2^w-1$
- Number of message bits: $k \leq n-wt$
- Minimum distance: $d \geq 2t + 1$

These BCH codes are called primitive because they are built using a primitive element of $GF(2^w)$.

3. CONSTRUCTING METHOD OF REGULAR QC-LDPC CODES

A. Description of The proposed constructing method

Let $GF(q)$ denote a finite Galois field of q elements, and let $GF(q^m)$ its extension field, $N=q^m-1$, where m is the multiplicative order of q modulo N and α denote a primitive root of $GF(q^m)$.

For any primitive element α of $GF(q^m)$, we associate the function δ, defined by:

$$GF(q^m)-\{0\} \rightarrow (GF(2))^N$$
$$\delta: \quad \alpha^i \rightarrow \delta(\alpha^i)=(0,...,1,...,0) \quad (6)$$

$\delta(\alpha^i)$ has the value 1 in position i and the value 0 anywhere, with i going over set $\{0, 1, \ldots, q^N - 1\}$.

Example 1:

$\delta(\alpha^3) = (0, 0, 1, 0, \ldots, 0)$

We can define the vector $\delta(\alpha^4)$ as the right cyclic shift of the vector $\delta(\alpha^3)$.

We define the circulant matrix $A(\alpha^j)$ over $(GF(2))^{N*N}$ of vectors $\delta(\alpha^j)$, as follows:

$$A(\alpha^i)=\begin{pmatrix} \delta(\alpha^i) \\ \delta(\alpha^{i+1}) \\ \mathrm{M} \\ \delta(\alpha^{i+N-1}) \end{pmatrix} \quad (7)$$

The circulant matrix $A(\alpha^i)$ contains a 1 in each of its rows and its columns. $A(\alpha^0)$ is the identity matrix of order N. And $A(\alpha^2)$ is written as follows:

$$A(\alpha^2)=\begin{pmatrix} 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & . & . & . & 0 \\ . & . & . & & . & & . \\ . & . & . & & . & & . \\ . & . & . & & . & & . \\ 1 & 0 & 0 & . & . & . & 0 \end{pmatrix} \quad (8)$$

Let β be a non-primitive element of $GF(q^m)$, α a primitive element of $GF(q^m)$ therefore $N=q^m-1$ its multiplicative order. Let n be the length of a cyclic code defined over $GF(q^m)$ so n divides N.

In our Construction we choose n which verifies the following inequality $q^{m/2}<n\leq q^m-1$. β has n the multiplicative order over $GF(q^m)$.

We define s by the equality $s=N/n$ then $\beta=\alpha^s$ (in this case β is an nth root of unity)

When a cyclic code is specified by roots $\beta_1, \beta_2, \ldots \beta_r$ over $GF(q^m)$[18], The parity check matrix of this code can be defined as follows

$$H=\begin{pmatrix} \beta_1^{\,0} & \beta_1^{\,1} & \beta_1^{\,2} & . & . & . & \beta_1^{\,n-1} \\ \beta_2^{\,0} & \beta_2^{\,1} & \beta_2^{\,2} & . & . & . & \beta_2^{\,n-1} \\ . & . & . & & & & . \\ . & . & . & & & & . \\ . & . & . & & & & . \\ \beta_r^{\,0} & \beta_r^{\,1} & \beta_r^{\,2} & . & . & . & \beta_r^{\,n-1} \end{pmatrix} \quad (9)$$

The proposed construction method (MC-LDPC) consists in the first place, of reducing the parity matrix of the derived cyclic code C whose matrix is written as the form of H to a new parity matrix H_s which is simplified, by preceding an elimination of some rows as follows:

When we have the parity check matrix H of cyclic code C, we introduce one root from the set $\{\beta_i, \beta_i^q, \beta_i^{q2} \ldots\}$ in matrix H and we calculate cyclotomic cosets of C to determine conjugates roots of β over $GF(q^m)$ in order to simplify the matrix H by removing the conjugates rows.

With $\beta=\alpha^s$ and $r^* \leq r$, the matrix simplified H_s is as follow:

$$H_s=\begin{pmatrix} 1 & \alpha^{s\times 1} & \alpha^{s\times 2} & . & . & . & \alpha^{s\times(n-1)} \\ 1 & \alpha^{2s\times 1} & \alpha^{2s\times 2} & . & . & . & \alpha^{2s\times(n-1)} \\ . & . & . & & & & . \\ . & . & . & & & & . \\ . & . & . & & & & . \\ 1 & \alpha^{r^*\times s\times 1} & \alpha^{r^*\times s\times 2} & . & . & . & \alpha^{r^*\times s\times(n-1)} \end{pmatrix} \quad (10)$$

The construction of parity check matrix H_{LDPC} of LDPC code can be obtained from the simplified parity matrix H_s of the code C specified by the roots, then we apply the function δ in equation 6 to each element of the parity matrix H_s, and we apply the equation 7 in order to obtain circulant sub- matrices into H_s. We will have the following matrix:

$$H_{LDPC} = \begin{pmatrix} A(1) & A(\alpha^{s\times 1}) & A(\alpha^{s\times 2}) & \cdots & A(\alpha^{s\times(n-1)}) \\ A(1) & A(\alpha^{2s\times 1}) & A(\alpha^{2s\times 2}) & \cdots & A(\alpha^{2s\times(n-1)}) \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ A(1) & A(\alpha^{r^*\times s\times 1}) & A(\alpha^{r^* s\times 2}) & \cdots & A(\alpha^{r^*\times s\times(n-1)}) \end{pmatrix} \quad (11)$$

The obtained parity matrix H_{LDPC} has the following properties:

- The size of H_{LDPC} is $(r^*\times N)(n\times N)$
- MC-LDPC method reduces lines number of matrix H_{LDPC} by 50 %: r becomes r^* ,with $r<r^*$
- Each column has a Hamming weight equal to r^*
- Each row has a Hamming weight equal to n
- H_{LDPC} is regular
- the density is equal $\frac{n*r^*N}{r^*N*nN} = \frac{r^**nN}{r^*N*nN} = \frac{1}{N}$ (12)
- Perimeter (Girth) the graph of at least 6.
- If the minimum distance of the cyclic code C is d_c then the minimum distance d_{LDPC} of the derivative LDPC code is bounded by d_c: $d_{LDPC} \geq d_c$

B. Proposed MC-LDPC algorithm

The description of the algorithm of the proposed constructing method is as follows:

Algorithm 1: MC-LDPC algorithm

Inputs:
q, m
n: length of cyclic code C
g(x): generator polynomial of cyclic code C

Outputs:
N, r, H_{LDPC}*

Step 1: Calculate C_i cyclotomic cosets modulo n
Step 2: Calculate m_i minimal polynomials m_i associated to cyclotomic cosets C_i
Step 3: If (*g(x)== least common multiple (LCM) $(m_1,\ldots,m_j)$* **)**
Then $r \longleftarrow j$ // r: number of the roots associated to m_i //
EndIf

Step 4: Calculate ***p*** // p: number conjugates roots of β_i//
Step 5: Calculate $r^* \longleftarrow r\text{-}p$ //r^***:** number of H_s rows //
Step 6: Calculate H_s
Step 7: Calculate H_{LDPC}

We can give the following example to illustrate the sequences of the MC-LDPC algorithm

Example 2:

We take the extension field *GF(256)*, with *q=2* and the primitive polynomial $p(x)=1+x^2+x^3+x^4+x^8$
The starting cyclic code is C(51,19,11), it's a non primitive code of generator polynomial $g(x)=1+x^2+x^3+x^5+$
$x^6+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{14}+x^{16}+x^{19}+x^{21}+x^{24}+x^{30}+x^{32}$
Then we have: *m=8, N=255, n=51, s=5* and $\beta=\alpha^5$ root in *GF(256)* of multiplicity order *51*

Step 1: The cyclotomic cosets C_i mod 51 are as follows:
C_0 ={0}
C_1 ={ 1,2,4,8,16,32,13,26}
C3 ={ 3,6,12,24,48,45,39,27}
C_5 ={ 5,10,20,40,29,7,14,28}
C_9 ={ 9,18,36,21,42,33,15,30}
C_{11} ={ 11,22,44,37,23,46,41,31}
C_{17} ={ 17,34}
C_{19} ={ 19,38,25,50,49,47,43,35}

Step 2: Minimal polynomials m_i associated to C_i are respectively:
m_0 (x)=x+1
m_1 (x)= $1+x+x^4+x^5+x^6+x^7+x^8$
m_3 (x)= $1+x+x^2+x^4+x^6+x^7+x^8$
m_5 (x)= $1+x+x^3+x^4+x^8$
m_9 (x)= $1+x^3+x^4+x^5+x^8$
m_{11} (x)= $1+x^3+x^4+x^5+x^8$
m_{17} (x)= $1+x+x^2$
m_{19} (x)= $1+x+x^2+x^3+x^4+x^7+x^8$

Step 3: $g(x) = LCM(m_1,\ldots,m_{10})$ then $r=10$

Step 4-5: We have β^2, β^4, β^8 conjugates roots of β, β^6 is conjugate root of β^3 and β^7, β^{10} conjugates roots of β^5
Then *p=6* whence *r*=4* and $(\beta, \beta^3, \beta^5, \beta^9)$ are roots of H_s

Step 6-7:

$$H_{LDPC} = \begin{pmatrix} A(1) & A(\alpha^5) & A(\alpha^{10}) & \cdots & A(\alpha^{46}) \\ A(1) & A(\alpha^{15}) & A(\alpha^{30}) & \cdots & A(\alpha^{36}) \\ A(1) & A(\alpha^{25}) & A(\alpha^{50}) & \cdots & A(\alpha^{26}) \\ A(1) & A(\alpha^{45}) & A(\alpha^{90}) & \cdots & A(\alpha^{6}) \end{pmatrix} \quad (13)$$

So, we construct the regular QC-LDPC code of the matrix H_{LDPC} of size (1020*13005), each circulant sub-matrix $A(\alpha^i)$ is the size *(255*255).*

H_{LDPC} has Hamming weight columns equal to 4, Hamming weight rows equal to 51 and a density 0, 004.

The Table-1 presents some QC-LDPC codes constructed by the MC-LDPC method (Algorithm1).

Table-1. Parameters of some regular QC-LDPC codes derived from some cyclic codes using algorithm 1.

$N=2^m-1$	Code cyclic	Roots of H_s	Size of H_{LDPC}	Density of H_{LDPC}
31	C(31,16,7)	β, β^3, β^5	(93,961)	0.035
63	C(21,12,5)	β, β^3	(126,1323)	0.015
63	C(9,3,3)	β	(63,567)	0.015
127	C(127,92,11)	$\beta,\beta^3,\beta^5,\beta^7,\beta^9$	(635,16129)	0.007
255	C(17,9,5)	β	(255,4335)	0.003
255	C(51,19,11)	$\beta, \beta^3, \beta^5, \beta^9$	(1020,13005)	0.003
511	C(73,19,21)	$\beta,\beta^3,\beta^5,\beta^9,\beta^{11},\beta^{13}$	(3066,37303)	0.002
1023	C(33,13,10)	β, β^3	(2046,33759)	0.0009
2047	C(23,13,10)	β	(2047,47081)	0.0004
4095	C(105,81,5)	β, β^3	(8190,429975)	0.0002

4. PROPRIETIES OF GENERATED QC-LDPC CODES

A. Girth of Tanner graph

Girth is one parameter usually targeted for optimization of errors performance, in particular error floor. A LDPC code with large girth is desirable, as iterative decoding converges faster for graphs with large girth.

In MC-LDPC method, QC-LDPC codes are constructed by blocks of sparse circulant matrices of weight not more than 1 in each row or column, then, there is no two rows (or two columns) in the same matrix or different blocks of circulant matrices having more than one value in common. Consequently, the obtained HLDPC matrix is also a sparse matrix of lower density, which gives a quasi-cyclic LDPC code whose the Tanner graph has no cycles of length 4.

We calculated the girth of Tanner graph for some codes constructed by MC-LDPC derived from BCH codes.

The Table-2 shows that MC-LDPC method reduces lines number of matrix H_{LDPC} by 50 % and increases the girth value of at least 6 form BCH codes tested.

The girth is obtained by the algebraic calculator MAGMA.

B. Density of H_{LDPC}

It can be demonstrated that the density D of the matrix H_{LDPC} *of size* $(r^* \times N)(n \times N)$ *is*

$$D = \frac{1}{N} = \frac{1}{n \times s} \quad (14)$$

Form a non-primitive cyclic code the density of the obtained LDPC code is very low because the integer $S \neq 1$

We note that it has a lower density if $S > 1$

Table-2. Girth for some constructed QC-LDPC from BCH codes.

$N=2^m-1$	Code	Roots H_s	MC-LDPC	
			H_{LDPC}	Girth
15	BCH(15,11,3)	β	(15,225)	No cycle
15	BCH(15,7,5)	β, β^3	(30,225)	8
15	BCH(15,5,7)	β, β^3, β^5	(45,225)	6
31	BCH(31,21,5)	β, β^3	(62,961)	8
31	BCH(63,51,5)	β, β^3	(126,3969)	6

C. Rank and rate of H_{LDPC}

We note that the lines of the matrix H_{LDPC} are not necessarily linearly independent on the binary Galois field *GF (2)*. In this case, to determine the dimension of the constructed code, we must calculate the rank of the matrix H_{LDPC}.

The Rank of regular matrix H_{LDPC} of size $(r^* \times N)(n \times N)$ constructed by *MC-LDPC is:*

$$Rank \leq \mathrm{r}^* N \quad (15)$$

We proved that the Rank depends on the nonzero integer r^*, so we can write that:

$$Rank = \mathrm{r}^* N - cst \quad (16)$$

Where *cst* denote a constant that depends on r^*

We found the equivalent matrix of H_{LDPC} in systematic form, in order to calculate the Rank of equivalent codes. The Table-3 gives the rank of several tests codes.

From the obtained results, we can limit the value of the *cst* between *0* and $r^* - 1$.

The Rank can be rewritten as follow:

$$Rank = r^* N - (r^* - 1) \quad (17)$$

Table-3. Rank and coding rate for some constructed QC-LDPC codes.

$N=2^m-1$	Code	Size of H_{LDPC}	Rank	Coding rate
63	C(9,3,3)	(63,1323)	63	1260/1323
15	BCH(15,11,3)	(15,225)	15	210/225
15	BCH(15,7,5)	(30,225)	29	196/225
15	BCH(15,5,7)	(45,225)	43	182/225
255	C(17,9,2)	(255,4335)	255	4080/4335
63	C(21,9,3)	(63,1363)	63	1360/1363
31	BCH(31,21,5)	(62,961)	61	900/961
31	BCH(31,6,15)	(217,961)	211	750/961
63	BCH(63,24,15)	(441,3969)	435	3534/3969

5. SIMULATION RESULTS

The performance of constructed codes is simulated for some different lengths and rates coding, using the parameters of Table-4.

Table-4. Parameters of simulation.

Parameter	Value
Channel	*AWGN*
Modulation	*BPSK*
Minimum number of residual bit in errors	*200*
Minimum number of transmitted blocs	*1000*
Number of iterations	*[50,150]*

For the decoding method we use the decoding algorithm SPA (sum-product algorithm) in its logarithmic version [20]. The decoding algorithm is stopped when the predefined number of iterations is reached or when the syndrome of the received word is equal to zero.

We computed the bit error probability (BER) for each tested code and we plotted the BER curves as a function of signal-to-noise ratio (E_b / N_0) to analyze the error coding performance.

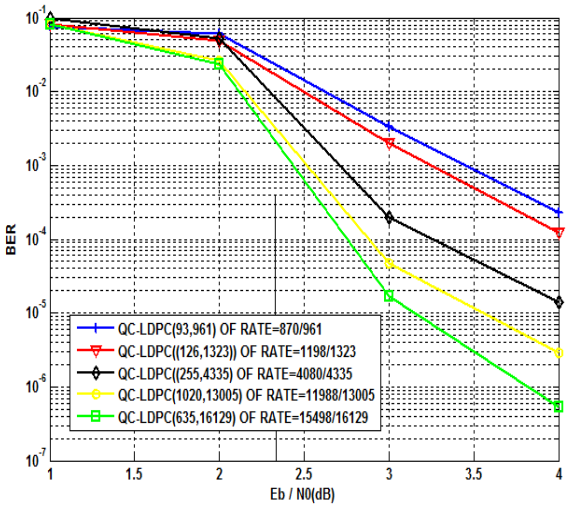

Figure-1. Performance of QC-LDPC codes constructed by MC-LDPC method.

The Figure-1 shows the error performance curves of same constructed QC-LDPC codes which are derived as follow: QC-LDPC(93,961) is derived from the cyclic code C(31,16,7) which is also a BCH code, the result QC-LDPC having a girth of 6 and density 0,035 . QC-LDPC (126, 1323) of girth 6 and density 0,015 is derived from the cyclic code C(21,12,5) which is a non primitive BCH code. QC-LDPC (255, 4335) is derived from the cyclic code C(17, 9, 5) which is a non primitive BCH code, the constructed QC-LDPC having a girth of 8 and density 0,003. QC-LDPC (1020, 13005) has a girth of 8 and density 0, 003 is derived from the non primitive BCH code C(51, 19, 11). And QC-LDPC (635, 16129) is derived from the cyclic code C(127, 92, 11) having a girth of 8 and density 0, 007.

The number of decoding iterations used in the SPA algorithm varies between 50 and 150 iterations in terms of the code size. We can observe that after about

150 iterations the oscillations of the decoding converge to a fixed threshold which remains the same until the end of iterations. From Figure-1, we show that simulated QC-LDPC codes perform better than other QC-LDPC previously constructed in [13-17] and QC-LDPC (1020, 13005) and QC-LDPC (635, 16129) codes perform much better below the BER of 10^{-4}. At the BER of 10^{-5}, these two codes respectively perform at 3.6 dB and 3.25 dB and LDPC (635, 16129) performs 0.8dB from the Shannon limit.

6. CONCLUSIONS AND PERSPECTIVES

In this paper, we have presented a construction method of regular QC-LDPC based on cyclic codes. The fact that we have eliminated the conjugates lines in parity-check matrix of the derived cyclic code; we have reduced in half the incidence vectors of matrix H_{LDPC} and have improved the error-correcting performance of QC-LDPC codes. In addition, we have increased the Girth value of at least 6. We have demonstrated that these constructed QC-LDPC codes have high density, high rates and the cyclic structure helps to compute their dimension and Rank. Our constructing method allows increasing the minimum distance of the constructing QC-LDPC code.

We plan to verify more properties of this QC-LDPC family and evaluate their performances over different communication channels, and we will find new linear codes based from binary cyclic codes.

REFERENCES

[1] D. R. Gallager. 1962. Low density parity-check codes. IRE Trans. Inform. Theory. pp. 21-28.

[2] R. Gallager. 1963. Low density parity-check codes. MIT Press, 16-17 May.

[3] R.M. Tanner. 1981. A recursive approach to low complexity codes. IEEE Transactions on Information Theory. 27: 533-547.

[4] D. J. C. MacKay and R. M. Neal. 1996. Near Shannon limit performance of low density parity check codes. Electron. Lett. 32(18): 1645-1646.

[5] V. V. Zyablov and M. S. Pinske. 1975. Estimation of the error correction complexity for gallager low density codes. Probl. Peredachi Inf. 11: 1: 23-36.

[6] D. J. C. MacKay and R. M. Neal. 1996. Near shannon limit performance of low density parity check codes. Electron. Lett. 32(18): 1645-1646.

[7] T. J. Richardson, M. A. Shokrollahi and R. L. Urbanke. 2001. Design of capacity approaching irregular low-density parity check codes. IEEE Trans. On Inform. Theory. 47: 619-637.

[8] I. Djurdjevic, J. Xu, K. Abdel-Ghaffar and S. Lin. 2003. A class of low density parity check codes constructed based on reed-solomon codes with two information symbols. IEEE Communications Letters. 7: 317-319.

[9] S. Song, L. Lan, S. Lin and K. Abdel-Ghaffar. 2006. Construction of quasicyclic ldpc codes based on the primitive elements of finite fields. Information Sciences and Systems, 2006 40th Annual Conference. pp. 835-838.

[10] S. Song, L. Zeng, S. Lin and K. Abdel-Ghaffar. 2006. Algebraic constructions of nonbinary quasi-cyclic ldpc codes. Proc. 2006 IEEE Intl. Symp. Inform. Theory. pp. 83-87.

[11] G. Liva, S. Song, Y. Ryan W. Lan, L. Zhang and S. Lin. Design of ldpc codes: A survey and new results. J. Comm. Software and Systems, 2006.

[12] J. Wang, J. Lei, S. Ni. 2011. QC-IRA-d Codes Based on Circulant Permutation Matrices. IEEE Commun. Lett. 15(11): 1224-1227.

[13] Y. Yi, L. Shaobo and H. Dawei. 2005. Construction of ldpc codes based on narrow-sense primitive bch codes. Vehicular Technology Conference. 3: 1571-1574.

[14] M. Tomlinson, C. J. Tjhai, M. A. Ambroze and M. Z. Ahmed. 2004. Binary cyclic difference set codes derived from idempotents based on cyclotomic cosets. IEEE Transactions on Information Theory.

[15] Marc P. C. Fossorier. 2004. Quasi-Cyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices. IEEE Transactions on Information Theory. 50(8).

[16] S. A. Aly. 2008. Families of ldpc codes derived from nonprimitive bch codes and cyclotomic cosets. CORR, February 2008.

[17] Hosung Park, Seokbeom Hong, Jong-Seon No and Dong-Joon Shin. 2013. Construction of High-Rate Regular Quasi-Cyclic LDPC Codes Based on Cyclic Difference Families. IEEE Transactions on Communications. 61(8).

[18] Morelos-Zaragoza. 2006. The Art of Error Correcting Coding. Second Edition Robert, John Wiley & Sons, Ltd. ISBN: 0-470-01558-6.

[19] B. Shin, H. Park, S. Hong, J.-S. No and S.-H. Kim. 2014. Quasi-cyclic LDPC codes using overlapping matrices and their layered decoders. AEU - International Journal of Electronics and Communications. 68(5): 379-383.

[20] T. K. Moon. 2005. Error Correction Coding - Mathematical Methods and Algorithms. Wiley.