International Journal of Electronics and
Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 2, Issue 5, Nov 2013, 17-28
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

A CLASS OF STRUCTURED QUASI-CYCLIC LDPC CODES BASED ON PLANAR DIFFERENCE FAMILIES

SHADY M. IBRAHEEM[1], M. M. ABD ELRAZZAK[2], SALWA M. SERAG ELDIN[3], W. SAAD[4] & ATEF E. ABOELAZM[5]

[1,2]Department of Communication Engineering, Faculty of Engineering, Mansoura University, Mansoura, Egypt

[3]Department of Communication Engineering, Faculty of Engineering, Tanta University, Tanta, Egypt

[4,5]Department of Communication Engineering, Faculty of Electronic Engineering, Menoufiya University, Menouf, Egypt

ABSTRACT

This paper is devoted to introduce a special classes of (QC-LDPC) with very restricted code parameters based on planar difference families. Such difference families could be obtained by numerical analysis and computer programs. The resulting codes have parity check matrices with column-weight greater than three, at least no 4-cycle and approximately full rank. It can be noted that the construction based on planar difference families exhibits more flexibility than that based on difference sets in terms of length and code rate selections. Besides, the more increasing in the column-weights of parity check matrices of QC-LDPC codes, the more improvement in the minimum distances of them. Simulation results show that over the additive white Gaussian noise channel, these codes could outperform their randomly constructed counterparts.

KEYWORDS: LDPC Codes, Quasi-Cyclic Codes, Planar Difference Family, Girth, Minimum Distance

INTRODUCTION

Low-density parity-check (LDPC) codes were first presented by Gallager in1962 [1] and have created much interest recently when rediscovered and shown to perform remarkably close to the Shannon limit [2]. Quasi-cyclic low-density parity-check (QC-LDPC) codes are a special class of LDPC codes whose parity check matrices consist of circulant matrices. Quasi cyclic LDPC codes have attracted much interest in research because the quasi-cyclic structure facilitates the encoder and decoder implementations [3]. A greedy algorithm which maximizes the length of cycles in the parity-check matrix and offers an excellent performance is the progressive edge growth (PEG) algorithm [4]. Unfortunately, the generator matrix of PEG-LDPC construction is not sparse so encoding is more costly due to the required matrix multiplication. Quasi-cyclic PEG allows low-complexity encoding as well as decoding [5]. A (J,K)-regular LDPC code is defined by a parity-check matrix H in which each column has weight J and each row has weight K.

Some researchers considered a special class of regular QC-LDPC codes whose circulant matrices are circulant permutation matrices. It has been proved that any (J, K)-regular QC-LDPC code of this classes has minimum distance always upper bounded by (J + 1)!, and girth upper bounded by 12 [6].

In this paper, we extend the construction of moderate to high rate QC-LDPC codes to the ones that are based on planar cyclic difference families or planar perfect difference families (PCDF or PPDF) [7] to obtain restricted parameters LDPC code families with a less redundancy and a large scale of rate selections.

A regular QC LDPC codes with parity-check matrices consisting of a single row block of circulants with the column-weight $>$ 3 are proposed based on PCDF or PPDF. They are at least no 4-cycle classes of codes. It can be shown that there is an improvement in their minimum distances along with the increasing in the column-weight of their parity-check matrices.

Numerical analysis shows that the proposed QC LDPC codes of moderate to high lengths exhibit somewhat performance improvements than that of the existing similar classes of QC LDPC codes.

The remainder of the paper is organized as follows. Section II introduces the definition and the existence theorems of PCDF and PPDFs, and provides a construction method of those classes. In Section III, regular QC LDPC codes are proposed and analyzed.

In Section IV, the error correcting performance of the proposed QC LDPC codes is compared to some of the existing LDPC codes via numerical analysis. Finally, we draw some conclusions and future works and in Section V.

DIFFERENCE FAMILIES

We begin our concept theorems by defining the difference set.

Definition 1

Consider the Abelian additive group Zv ={0, 1, 2, · · · , v −1} of order v. A k-subset D = $\{d_1, \cdots, d_k\}$ of Zv is called a (v, k, λ)-difference set for Zv if every nonzero element of Zv has precisely λ distinct expressions $d_i - d_j$ mod v in terms of elements of D.

Definition 2

Consider the additive group Zv = {0, 1,….. , v - 1}. Then t k-element subsets of Zv, $B_i = \{b_{i1}, b_{i2}, \ldots, b_{ik}\}$, i = 1,2, …. , t, $b_{i1} < b_{i2} < \ldots < b_{ik}$, form a (v, k, λ) cyclic difference family (CDF) if every nonzero element of Zv occurs λ times among the differences $b_{im} - b_{in}$, i = 1, 2, …… , t , m ≠n , m,n = 1,2,….., k.

This (v, k, λ)-CDF is called a planar CDF in short PCDF if λ=1 and it is called a (v, k, λ)-planar perfect difference family in short (v, k, λ)-PPDF if and only if λ=1 and for v= k(k-1)t+1 a tk(k-1)/2 forward differences $b_{im} - b_{in}$ cover the subset {(v-1)/2+1, ………, v-1} and the remaining tk(k-1)/2 backward differences cover the subset {1,2, ….. ,(v -1)/2} over Zv [8].

The existences of PCDFs are summarized in the following theorem [8]-[10].

Theorem 1: The existence of (v, k, 1)-PCDFs is given as:

- A (6t + 1, 3, 1)-CDF exists for all t ≥ 1 with v=k(k-1)t+1=6t+1.
- A (12t+1,4, 1)-CDF exists for all 1 ≤ t ≤1000 with v=k(k-1)t+1=12t+1.
- (20t + 1, 5, 1)-CDF exists for 1 ≤ t ≤50 and t ≠ 16,25,31,34,40,45 with v=k(k-1)t+1=20t+1 [9].
- (v, 6, 1)-CDF exists for any prime power v=1 (mod 30) ,v ≠ 61.
- (v, 7, 1)-CDF exists for any prime power v=1 (mod 42) ,v ≠ 43, possibly for v = 127, 211,31^6, and primes v ∈ [261239791, 1.236597. 10^{13}] such that $(-3)^{\frac{v-1}{14}}$ = 1 in GF(v) [8]-[9].

Proof: Is omitted.

The existences of PPDFs are summarized in the following theorem [11].

Theorem 2: The existence of (k(k-1)t + 1, k, 1)-PPDFs is given as:

- A (6t + 1, 3, 1)-PDF exists if and only if t = 0 or 1 mod 4.

- A (12t+1,4, 1)-PDF exists for t = 1, 4 ≤ t ≤1000.
- (20t + 1, 5, 1)-PDFs are known for t = 6, 8, 10 but for no other small value of t.
- There is no (k(k - 1)t + 1, k, 1)-PDF for k = 6.

Proof: Is omitted.

An obvious necessary condition for the existence of a (v, k, 1)-DF is v= 1, k (mod k(k-1)).

QC LDPC CODES CONSTRUCTED FROM PLANAR DIFFERENCE FAMILIES

Consider a regular QC-LDPC code whose parity check matrix H consists of two row blocks array of circulants. A circulant is entirely described by the positions of nonzero elements in the first column. With the aid of a special cases of (v, k, λ)- PCDF or PPDF we construct H matrix consists of two row blocks. Each row block is an array of circulant matrices. For 1 ≤ i ≤ t, the first row block is denoted by $H^{'}$=[$A_1^{'}$… $A_t^{'}$] matrices and the second block is denoted by $H^{''}$= [$A_1^{''}$ …… $A_t^{''}$] matrices.

$A_i^{'}$ is a k × k circulant matrix (circulant matrix such that each row is a cyclic shift of the row above it). Its first row has k-column elements those are the elements of one of the t k-sets of (v, k, 1)-DFs elements modulo v, respectively.

$A_i^{''}$ is a k × k circulant matrix and its first row has k-column elements fulfilled with the negative elements of that one of the t k-sets of (v, k, 1)-DFs elements modulo v, respectively.

For α be a primitive field element for a Galois field Fq. The (q−1) × (q−1) dispersed matrix associated with α^k, denoted D(α^k), is defined by matrix,

$$D(\alpha^k)=\begin{pmatrix} 0 & 0 & 0 & .. & \alpha^k & ... & ...0 & 0 \\ 0 & 0 & 0 & .. & 0 & \alpha^{k+1} & ...0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & ...0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & ...0 & \alpha^{q-2} \\ 1 & 0 & 0 & 0 & 0 & 0 & ...0 & 0 \\ 0 & \alpha^1 & 0 & 0 & 0 & 0 & ...0 & 0 \\ 0 & 0 & ... & 0 & 0 & 0 & ...0 & 0 \\ 0 & 0 & 0 & \alpha^{k-1} & 0 & 0 & ...0 & 0 \end{pmatrix}.$$

So, with v=q-1, each element of k x k circulant matrix $A_i^{'}$ (and $A_i^{''}$) is dispersed by a v × v circulants over Fq, denoted by D(α^k) previously defined, or dispersed by a v × v binary circulants emerged from replacing each nonzero entry of D(α^k) with ‘1’.

The resultant parity-check matrix H is a double row ($\frac{H^{'}}{H^{''}}$) of t−k × k array of v × v circulants over F2 or Fq (mod q-1).

Suppose that α is a primitive field element of a q-element field Fq and D_i = {$d_{i\,1}$, $d_{i\,2}$,….. , $d_{i\,k}$}, i = 1,2, …. , t, $b_{i\,1}$ < $b_{i\,2}$ < ….< $b_{i\,k}$, form a (v, k, 1)-CDFs or a (v, k, 1)-PDFs for Zv where v = q−1 = k(k-1)t + 1, we have the following theorems.

Theorem 3: Associated with α^k, the (q−1) × (q−1) dispersed matrix (denoted by D(α^k)) of the combined 2k × k A_i =($\frac{A_i^{'}}{A_i^{''}}$),1≤ i ≤ t, circulant matrix mod(q-1) and its binary version, with k is odd, has no 4-cycles tanner graph.

Proof: See appendix A.

Example1: Consider the (13, 3, 1)-CDF $D_i = \{d_{i\,1}, d_{i\,2},\ldots.., d_{i\,k}\}$, i = 1,2, for Z13 and the field F14.

In this case k = 3 is odd.

A (6 × 2 + 1, 3, 1)-CDF:

D_1={0, 3, 12} with differences 3, 12, 9.

D_2={0, 5, 11} with differences 5, 11, 6.

Negative sets are,

D_{-1}={0, 10, 1} with differences 10, 1, 4.

D_{-2}={0, 8, 2} with differences 8, 2, 7.

The combined 2k × k $A_i = (\frac{A_i'}{A_i''})$ circulant matrices mod (q-1) for i = 1,2.

$$A_1 = \begin{pmatrix} 0 & 3 & 12 \\ 3 & 12 & 0 \\ 12 & 0 & 3 \\ 0 & 10 & 1 \\ 10 & 1 & 0 \\ 1 & 0 & 10 \end{pmatrix} A_2 = \begin{pmatrix} 0 & 5 & 11 \\ 5 & 11 & 0 \\ 11 & 0 & 5 \\ 0 & 8 & 2 \\ 8 & 2 & 0 \\ 2 & 0 & 8 \end{pmatrix}.$$

The null space of each matrix represents a code that has a Tanner graph with no 4-cycles.

Example 2: Consider the (25, 3, 1)-PDF $D_i = \{d_{i\,1}, d_{i\,2},\ldots.., d_{i\,k}\}$, i = 1,2,3, for Z25 and the field F26.

In this case k = 3 is odd.

A (6 × 4 + 1, 3, 1)-PDF:

D_1={0, 2, 12} with differences 2, 12, 10.

D_2={0, 3, 11} with differences 3, 11, 8.

D_3={0, 1, 7} with differences 1, 7, 6.

D_4={0, 4, 9} with differences 4, 9, 5.

Negative sets are

D_{-1}={0, 23, 13} with differences 23, 13, 15.

D_{-2}={0, 22, 14} with differences 22, 14, 17.

D_{-3}={0, 24,18} with differences 24, 18, 19.

D_{-4}={0, 21, 16} with differences 21, 16, 20.

The combined 2k × k $A_i = (\frac{A_i'}{A_i''})$ circulant matrices mod (q-1) for i = 1,2,3.

$$A_1 = \begin{pmatrix} 0 & 2 & 12 \\ 2 & 12 & 0 \\ 12 & 0 & 2 \\ 0 & 23 & 13 \\ 23 & 13 & 0 \\ 13 & 0 & 23 \end{pmatrix} A_2 = \begin{pmatrix} 0 & 3 & 11 \\ 3 & 11 & 0 \\ 11 & 0 & 3 \\ 0 & 22 & 14 \\ 22 & 14 & 0 \\ 14 & 0 & 22 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 0 & 1 & 7 \\ 1 & 7 & 0 \\ 7 & 0 & 1 \\ 0 & 24 & 18 \\ 24 & 18 & 0 \\ 18 & 0 & 24 \end{pmatrix} A_4 = \begin{pmatrix} 0 & 4 & 9 \\ 4 & 9 & 0 \\ 9 & 0 & 4 \\ 0 & 21 & 16 \\ 21 & 16 & 0 \\ 16 & 0 & 21 \end{pmatrix}.$$

The null space of each matrix represents a code that has a Tanner graph with no 4-cycles.

Example 3: Consider the (49, 4, 1)-PDF $D_i = \{d_{i\,1}, d_{i\,2}, \ldots\ldots, d_{i\,k}\}$, i = 1,2, ….4, for Z49 and the field F50. In this case k = 4 is even.

A (12 × 4 + 1, 4, 1)-PDF:

D_1={0, 5, 22, 24} with differences 5, 22, 17, 24, 19, 2.

D_2={0, 7, 13, 23} with differences 7, 13, 6, 23, 16, 10.

D_3={0, 3, 14, 18} with differences 3, 14, 11, 18, 15, 4.

D_4={0, 1, 9, 21} with differences 1, 9, 8, 21, 20, 12.

Negative sets are

D_{-1}={0, 44, 27, 25} with differences 44, 27, 32, 25, 30, 47.

D_{-2}={0, 42, 36, 26} with differences 42, 36, 43, 26, 33, 39.

D_{-3}={0, 46, 35, 31} with differences 46, 35, 38, 31, 34, 45.

D_{-4}={0, 48, 40, 28} with differences 48, 40, 41, 28, 29, 37.

The combined 2k × k $A_i = (\frac{A_i'}{A_i''})$ circulant matrices mod (q-1) for i = 1,2,…4.

$$A_1 = \begin{pmatrix} 0 & \mathbf{5} & 22 & \mathbf{24} \\ 5 & 22 & 24 & 0 \\ 22 & 24 & 0 & 5 \\ 24 & 0 & 5 & 22 \\ 0 & 44 & 27 & 25 \\ 44 & 27 & 25 & 0 \\ 27 & \mathbf{25} & 0 & \mathbf{44} \\ 25 & 0 & 44 & 27 \end{pmatrix} A_2 = \begin{pmatrix} 0 & \mathbf{7} & 13 & \mathbf{23} \\ 7 & 13 & 23 & 0 \\ 13 & 23 & 0 & 7 \\ 23 & 0 & 7 & 13 \\ 0 & 42 & 36 & 26 \\ 42 & 36 & 26 & 0 \\ 36 & \mathbf{26} & 0 & \mathbf{42} \\ 26 & 0 & 42 & 36 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 0 & \mathbf{3} & 14 & \mathbf{18} \\ 3 & 14 & 18 & 0 \\ 14 & 18 & 0 & 3 \\ 18 & 0 & 3 & 14 \\ 0 & 46 & 35 & 31 \\ 46 & 35 & 31 & 0 \\ 35 & \mathbf{31} & 0 & \mathbf{46} \\ 31 & 0 & 46 & 35 \end{pmatrix} A_4 = \begin{pmatrix} 0 & \mathbf{1} & 9 & \mathbf{21} \\ 1 & 9 & 21 & 0 \\ 9 & 21 & 0 & 1 \\ 21 & 0 & 1 & 9 \\ 0 & 48 & 40 & 28 \\ 48 & 40 & 28 & 0 \\ 40 & \mathbf{28} & 0 & \mathbf{48} \\ 28 & 0 & 48 & 40 \end{pmatrix}$$

We observe that the bold numbers lead to cycles of length four. So, we can use the left or right hand side halves as matrices whose null spaces represent codes that having a Tanner graph free of cycles of length four.

Theorem 4: Associated with α^k, if k is even, then, the (q−1) × (q−1) dispersed matrix (denoted by $D(\alpha^k)$) of the combined 2(k-1) × k-1 $A_i = (\frac{A_i'}{A_i''})$, 1≤ i ≤ t, circulant matrices mod(q-1) resulting from the construction using (v, k, 1)-CDFs or PDFs with $D_i = \{d_{i\,1}, d_{i\,2}, \ldots\ldots, d_{i\,k-l-1}, d_{i\,k-l+1}, \ldots\ldots, d_{i\,k}\}$, where 0 ≤ l ≤ k-1 has no 4-cycles tanner graph, individually.

Proof: See appendix B.

Example 4: From example 3, we observe that the following matrices are free of cycle four,

$$A_{11}=\begin{pmatrix}0 & \mathbf{5} & 22\\ 5 & 22 & 0\\ 22 & 0 & 5\\ 0 & 44 & 27\\ 44 & 27 & 0\\ 27 & \mathbf{0} & 44\end{pmatrix} A_{21}=\begin{pmatrix}0 & \mathbf{7} & 13\\ 7 & 13 & 0\\ 13 & 0 & 7\\ 0 & 42 & 36\\ 42 & 36 & 0\\ 36 & \mathbf{0} & 42\end{pmatrix}$$

$$A_{31}=\begin{pmatrix}0 & \mathbf{3} & 14\\ 3 & 14 & 0\\ 14 & 0 & 3\\ 0 & 46 & 35\\ 46 & 35 & 0\\ 35 & \mathbf{0} & 46\end{pmatrix} A_{41}=\begin{pmatrix}0 & \mathbf{1} & 9\\ 1 & 9 & 0\\ 9 & 0 & 1\\ 0 & 48 & 40\\ 48 & 40 & 0\\ 40 & \mathbf{0} & 48\end{pmatrix},$$

where $A_{i1}$are the modified versions of A_i for i=1,2 …4. The results obtained in the previous discussions in this section provide the ground for the construction of a restricted class no girth-four QC-LDPC codes.

Theorem 5: Associated with α^k , the (q−1) × (q−1) dispersed matrix (denoted by D(α^k)) of the combined $H=(\frac{H'}{H''})=(A_1\ A_2 \ldots .A_i)=(\frac{A_1'}{A_1''}\ \frac{A_2'}{A_2''} \ldots .\frac{A_i'}{A_i''})$, $1\leq i\leq t$, matrix mod(q-1) under the above mentioned conditions, i.e. for odd and modified even cases of k, has no 4-cycles tanner graph if $D_i \cap D_j = \emptyset$, $\forall\ 1\leq i,j \leq t$, $i\neq j$ and $\forall\ a,b \in D_i ,c,d \in D_j \rightarrow a-c\neq d-b$. For $D_i \cap D_j = e \neq \emptyset$, $1\leq i,j\leq t$, $i\neq j$. If, we replace all e shifts of the resultant matrix by zero matrices, then, H has also no 4-cycles tanner graph.

Proof: See appendix C.

The proof is built upon the ideas that for the case of PPDF, the pairs of differences of the upper half of the matrix are distinct due to the property of PDF and cover backward differences of the subset {1,2, ….. ,(v -1)/2} over Zv**.** In addition to the fact that the lower half parts of the matrix are subsets of Dev(D) (the development of D) and their pairs of differences are distinct and cover forward differences of the subset {(v-1)/2+1, ………, v-1} over Zv**.** Unlikely, for the case of PCDF, the pairs of differences of the upper half of the matrix cover mixed forward and backward differences over Zv group that differ in value from their lower half differences counterparts.

Example 5: For the following two matrices B1, B2 from example 2, 3-4, respectively.

$$B1=\begin{pmatrix}\mathbf{0} & 2 & 12 & \mathbf{0} & 3 & 11 & \mathbf{0} & 1 & 7 & \mathbf{0} & 4 & 9\\ 2 & 12 & \mathbf{0} & 3 & 11 & \mathbf{0} & 1 & 7 & \mathbf{0} & 4 & 9 & \mathbf{0}\\ 12 & \mathbf{0} & 2 & 11 & \mathbf{0} & 3 & 7 & \mathbf{0} & 1 & 9 & \mathbf{0} & 4\\ \mathbf{0} & 23 & 13 & \mathbf{0} & 22 & 14 & \mathbf{0} & 24 & 18 & \mathbf{0} & 21 & 16\\ 23 & 13 & \mathbf{0} & 22 & 14 & \mathbf{0} & 24 & 18 & \mathbf{0} & 21 & 16 & \mathbf{0}\\ 13 & \mathbf{0} & 23 & 14 & \mathbf{0} & 22 & 18 & \mathbf{0} & 24 & 16 & \mathbf{0} & 21\end{pmatrix}$$

$$B2=\begin{pmatrix}\mathbf{0} & 5 & 22 & \mathbf{0} & 7 & 13 & \mathbf{0} & 3 & 14 & \mathbf{0} & 1 & 9\\ 5 & 22 & \mathbf{0} & 7 & 13 & \mathbf{0} & 3 & 14 & \mathbf{0} & 1 & 9 & \mathbf{0}\\ 22 & \mathbf{0} & 5 & 13 & \mathbf{0} & 7 & 14 & \mathbf{0} & 3 & 9 & \mathbf{0} & 1\\ \mathbf{0} & 44 & 27 & \mathbf{0} & 42 & 36 & \mathbf{0} & 46 & 35 & \mathbf{0} & 48 & 40\\ 44 & 27 & \mathbf{0} & 42 & 36 & \mathbf{0} & 46 & 35 & \mathbf{0} & 48 & 40 & \mathbf{0}\\ 27 & \mathbf{0} & 44 & 36 & \mathbf{0} & 42 & 35 & \mathbf{0} & 46 & 40 & \mathbf{0} & 48\end{pmatrix}$$

We have over F50 with v=49 of B2. If each element k of the matrix is dispersed by a v × v circulants over Fq, denoted by D(α^k) previously defined or dispersed by a v × v binary circulants emerged from replacing each nonzero entry of D(α^k) with ‘1’, then, this matrix is free of cycles of length four.

Hint: The bold zeros are dispersed to the zero matrix mod v

Over F26 with v=25 of B1 under the same conditions this matrix has cycles of length four. As, for 2, 12 ∈ D_1 and 3,11 ∈ D_2 there exist 12-11=3-2. So, by eliminating a sub-matrices that belong to D_1 and D_{-1} **,** if each element k of the resultant matrix

$$\mathbf{B1_{resultant}} = \begin{pmatrix} \mathbf{0} & 3 & 11 & \mathbf{0} & 1 & 7 & \mathbf{0} & 4 & 9 \\ 3 & 11 & \mathbf{0} & 1 & 7 & \mathbf{0} & 4 & 9 & \mathbf{0} \\ 11 & \mathbf{0} & 3 & 7 & \mathbf{0} & 1 & 9 & \mathbf{0} & 4 \\ \mathbf{0} & 22 & 14 & \mathbf{0} & 24 & 18 & \mathbf{0} & 21 & 16 \\ 22 & 14 & \mathbf{0} & 24 & 18 & \mathbf{0} & 21 & 16 & \mathbf{0} \\ 14 & \mathbf{0} & 22 & 18 & \mathbf{0} & 24 & 16 & \mathbf{0} & 21 \end{pmatrix}$$

is dispersed by a v × v circulants over Fq ,denoted by $D(\alpha^k)$ previously defined or dispersed by a v × v binary circulants emerged from replacing each nonzero entry of $D(\alpha^k)$ with '1', then, this matrix is free of cycles of length four. For the case of PPDF, in order to increase the minimum distance of the proposed codes, preserve the weight distribution and girth characteristics, one can disperse the zero matrices by a v × v circulants (previously interpreted) for the upper and lower parts interchangeably as follows,

$$\mathbf{B1'_{resultant}} = \begin{pmatrix} \mathbf{0} & 3 & 11 & 0 & 1 & 7 & \mathbf{0} & 4 & 9 \\ 3 & 11 & \mathbf{0} & 1 & 7 & 0 & 4 & 9 & \mathbf{0} \\ 11 & 0 & 3 & 7 & \mathbf{0} & 1 & 9 & 0 & 4 \\ 0 & 22 & 14 & \mathbf{0} & 24 & 18 & 0 & 21 & 16 \\ 22 & 14 & 0 & 24 & 18 & \mathbf{0} & 21 & 16 & \mathbf{0} \\ 14 & \mathbf{0} & 22 & 18 & 0 & 24 & 16 & \mathbf{0} & 21 \end{pmatrix},$$

$$\mathbf{B2'} = \begin{pmatrix} \mathbf{0} & 5 & 22 & 0 & 7 & 13 & \mathbf{0} & 3 & 14 & 0 & 1 & 9 \\ 5 & 22 & \mathbf{0} & 7 & 13 & 0 & 3 & 14 & \mathbf{0} & 1 & 9 & 0 \\ 22 & 0 & 5 & 13 & \mathbf{0} & 7 & 14 & 0 & 3 & 9 & \mathbf{0} & 1 \\ 0 & 44 & 27 & \mathbf{0} & 42 & 36 & 0 & 46 & 35 & \mathbf{0} & 48 & 40 \\ 44 & 27 & 0 & 42 & 36 & \mathbf{0} & 46 & 35 & 0 & 48 & 40 & \mathbf{0} \\ 27 & \mathbf{0} & 44 & 36 & 0 & 42 & 35 & \mathbf{0} & 46 & 40 & 0 & 48 \end{pmatrix}$$

where t is an even number, the normal zeroes are dispersed by identity v × v matrices and the bold zeroes are dispersed by zero matrices mod v. It can be shown that $\mathbf{B1'_{resultant}}$ and $B2'$ matrices are full rank matrices, but $\mathbf{B1'_{resultant}}$ matrix leads to irregular LDPC code.

Example 6: Consider the (101,5,1)-CDF. Let v= 101, k = 5, then, a set of base blocks of (101, 5, 1)-CDF={ D_1 ... D_5 }={{0,100,98,76,71},{0,17,51,21,74},{0,36,7,92,26},{0,14,42,47,55},{0,95,83,52,63}} over Z101 group and the field F102. {{0,100,98,76,71},{0,17,51,21,74},{0,36,7,92,26},{0,14,42,47,55} , {0,95,83,52,63}} are the set of negative blocks, so, the null space of the H matrix =

$$\begin{pmatrix} 0 & 14 & 42 & 47 & 55 & 0 & 95 & 83 & 52 & 63 & 0 & 17 & 51 & 21 & 74 & 0 & 36 & 7 & 92 & 26 & 0 & 100 & 98 & 76 & 71 \\ 14 & 42 & 47 & 55 & 0 & 95 & 83 & 52 & 63 & 0 & 17 & 51 & 21 & 74 & 0 & 36 & 7 & 92 & 26 & 0 & 100 & 98 & 76 & 71 & 0 \\ 42 & 47 & 55 & 0 & 14 & 83 & 52 & 63 & 0 & 95 & 51 & 21 & 74 & 0 & 17 & 7 & 92 & 26 & 0 & 36 & 98 & 76 & 71 & 0 & 100 \\ 47 & 55 & 0 & 14 & 42 & 52 & 63 & 0 & 95 & 83 & 21 & 74 & 0 & 17 & 51 & 92 & 26 & 0 & 36 & 7 & 76 & 71 & 0 & 100 & 98 \\ 55 & 0 & 14 & 42 & 47 & 63 & 0 & 95 & 83 & 52 & 74 & 0 & 17 & 51 & 21 & 26 & 0 & 36 & 7 & 92 & 71 & 0 & 100 & 98 & 76 \\ 0 & 87 & 59 & 54 & 46 & 0 & 6 & 18 & 49 & 38 & 0 & 84 & 50 & 80 & 27 & 0 & 65 & 94 & 9 & 75 & 0 & 1 & 3 & 25 & 30 \\ 87 & 59 & 54 & 46 & 0 & 6 & 18 & 49 & 38 & 0 & 84 & 50 & 80 & 27 & 0 & 65 & 94 & 9 & 75 & 0 & 1 & 3 & 25 & 30 & 0 \\ 59 & 54 & 46 & 0 & 87 & 18 & 49 & 38 & 0 & 6 & 50 & 80 & 27 & 0 & 84 & 94 & 9 & 75 & 0 & 65 & 3 & 25 & 30 & 0 & 1 \\ 54 & 46 & 0 & 87 & 59 & 49 & 38 & 0 & 6 & 18 & 80 & 27 & 0 & 84 & 50 & 9 & 75 & 0 & 65 & 94 & 25 & 30 & 0 & 1 & 3 \\ 46 & 0 & 87 & 59 & 54 & 38 & 0 & 6 & 18 & 49 & 27 & 0 & 84 & 50 & 80 & 75 & 0 & 65 & 94 & 9 & 30 & 0 & 1 & 3 & 25 \end{pmatrix}$$

Represents a code that has a rate of 0.6, five redundant rows and a Tanner graph free of cycles of length four.

SIMULATION RESULTS

The error correcting performance of the proposed QC LDPC codes is compared with random-like progressive edge-growth (PEG) and QC-PEG LDPC codes, the best ones were recognized by [4-5], [12]. As possible, the parameters are nearly the same. Results are obtained using sum-product decoding algorithm under the additive white Gaussian noise (AWGN) channel and BPSK modulation is considered. The maximum number of iterations is set to 100. We collect at least 100 block errors per simulation point. All the comparable proposed codes are constructed based on Theorems 5. This theorem enables one to suppress or impress one or more sub-classes of quasi-cyclic circulants that belong to one or more subsets of difference family of the mother code, without any changes in the desired mother code characteristics and consequently, leads to more flexibility in the selection of rates of the proposed codes. For a target girth greater than six, further results could be obtained by suppress or impress one or more elements as well as sub-classes at this time.

In the next, we simulate the binary dispersion of some mother matrices of previous examples taking in consideration that the constructed difference-family based codes have a good BER performance over AWGN channel decoded with iterative decoding using the Fast Fourier Transform based q-ary sum-product decoding algorithm.

BER Performance of a Proposed Regular (4, 6) QC-LDPC Code

A proposed regular (4,6)-quasi cyclic LDPC code of rate 1/3, whose mother parity check matrix $\mathbf{B1}_{\mathbf{resultant}}$ is dispersed in a binary manner, is compared with random-like progressive edge-growth (PEG) LDPC and QC-PEG LDPC codes. This code is based on (25, 3, 1)-PDF over F26. It has a length of 225 and only three redundant rows. The bit error rate (BER) performance of those LDPC codes is shown in Figure 1, with considerably the same code parameters. According to this figure, the PEG, QC-PEG and proposed-QC girth-six codes perform almost closely in the low SNR region. This is unlikely occur in the high SNR, as the proposed code begins to introduce a good error floor performance.

BER Performance of Proposed Regular (4, 8) and (5,10) QC-LDPC Codes

Figure 2 provides a BER performance of a redundant proposed regular (4,8)-quasi cyclic LDPC code of rate 1/2 based on parity check matrix B2 and a full rank proposed regular (5,10)-quasi cyclic LDPC code based on parity check matrix $\mathrm{B2}'$. The density of the parity check matrix $\mathrm{B2}'$ is shown in Figure 3.

For further comparison a PEG construction, QC-PEG and Modified PEG of [4-5], [12] and [13] were used, respectively. The proposed codes have a length of 300 and a dimension of 150 and is based on (49, 4, 1)-PDF over F50. The parity check matrix B2 is modified to form the $\mathrm{B2}'$ full rank matrix. As expected from Figure 2, the two proposed codes outperform both PEG and QC-PEG constructions especially in the high SNR region by a considerable margin. This is due to ideal diversity of none-zero elements in their parity check matrices.

This gain is seen obviously in the error floor region a result of the large degree of their tanner graph connectivity. It can be seen that the two proposed codes perform almost exactly as well in the low SNR region. The benefits of the full rank one appear in the error floor region. We observe that the Modified PEG construction is slightly better than the proposed codes. However, error floor starts to appear when the BER is closed to 10^{-6}. Hence, both proposed codes introduce lower error floors. The values of t and k, i.e. the number of subsets of a difference family and the number of elements inside every subset, determine the principle of the code length and rate selection.

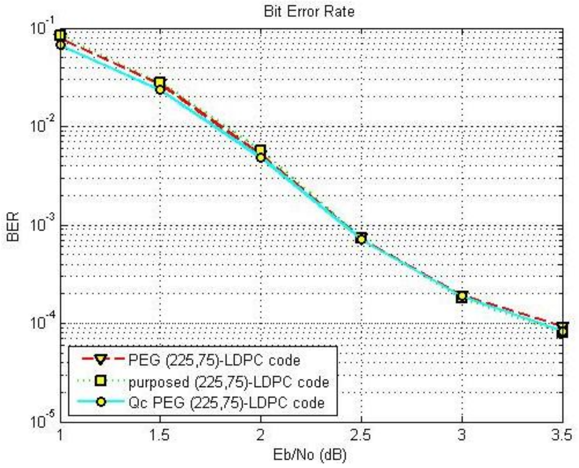

Figure 1: Performance Comparison between the Proposed QC Girth-Six (225,75)-LDPC Code and its PEG and QC-PEG Counterparts over AWGN Channel

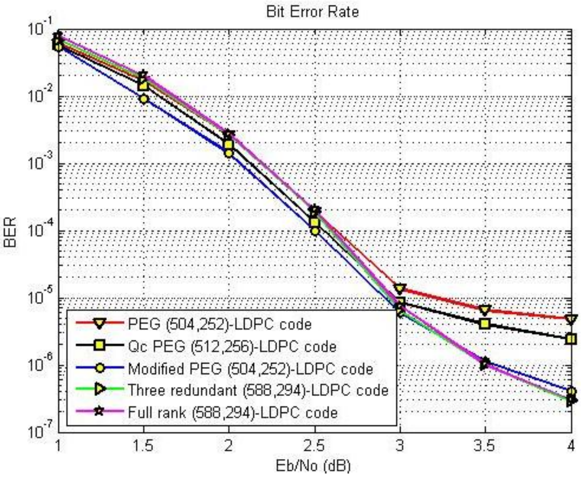

Figure 2: BER Performance Comparison between the Proposed QC Girth-Six (588,294)-LDPC Codes with PEG, QC-PEG and Improved PEG

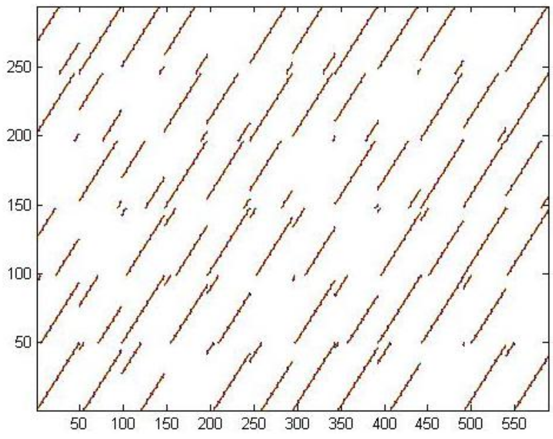

Figure 3: The Density of Non-Zero Elements of the Parity Check Matrix $B2'$

CONCLUSIONS

In this paper (v,k, λ)-PCDFs or PPDFs were used to construct several classes of moderate to high rate q-ary 4-cycle free (or more) quasi-cyclic LDPC codes and their dispersed binary versions but with restricted parameters. The parity-check matrices of these codes consist of a single row block of circulants and their negative extensions. These codes outperform over AWGN channel PEG and QC-PEG code constructions especially in the error floor region.

REFERENCES

1. R. G. Gallager, “*Low-density-parity-check code,*” IRE Trans. Inform. Theory, vol.8, no.1, pp.21–28, Jan. 1962.

2. D. MacKay and R.M. Neal, “*Near-Shannon limit performance of low density parity check codes,*” Electron. Lett., vol.32, no.18, pp.1645–1646, Mar. 1996.

3. R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, Jr., “*LDPC block and convolutional codes based on circulant matrices,*” IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

4. X. Y. Hu, E. Eleftheriou and D. M. Arnold, "*Regular and irregular progressive edge-growth tanner graphs,* "*IEEE Trans. Commun.*, vol.51, no.1, pp.386-388, 2005.

5. Zongwang Li and B.V.K.V. Kumar, “*A class of good quasi cyclic low-density parity check codes based on progressive edge growth graph,*” *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, vol. 2, pp. 1990– 1994, Nov. 2004.

6. J. L. Fan, “*Array codes as low-density parity-check codes,*” in Proc. 2nd Int. Symp. on Turbo Codes, Sept. 2000, pp. 543–546.

7. R. Mathon, “*Construction for cyclic Steiner 2-designs,*” Ann. Discrete Math., vol. 34, pp. 353-362, 1987.

8. G. Ge, Y. Miao, and X. Sun, “*Perfect difference families, perfect difference matrices, and related combinatorial structures,*” J. Combin. Des., vol. 18, no. 6, pp. 415-449, Nov. 2010.

9. R. Julian, R. Abel, S. Costa, and N. J. Finizio, “*Directed-ordered whist tournaments and (v; 5; 1) difference families: Existence results and some new classes of Z-cyclic solutions,*” Discrete Appl. Math., vol. 143, pp. 43-53, 2004.

10. T. Baicheva and S. Topalova, "*Optimal optical orthogonal codes of weight 5 and small lengths,* "International Conference on Applications of Computer Algebra, Sofia, Bulgaria, 2012.

11. Hosung Park, Seokbeom Hong, Jong-Seon No, Dong-Joon Shin, “*Construction of High-Rate Regular Quasi-Cyclic LDPC Codes Based on Cyclic Difference Families,” arXiv:1211.3828v1 [cs.IT] 16 Nov 2012.*

12. A. G. D. Uchoa, C. Healy, R. C. de Lamare and R. D. Souza, "*Design of LDPC codes based on progressive edge growth techniques for block fading channels*, "*IEEE Communications Letters*, vol.15, no.11, pp.1221-1223, 2011.

13. H. Xiao and A. Banihashemi, “*Improved progressive-edge-growth (PEG) construction of irregular LDPC codes,*” IEEE Commun. Lett., vol. 8, no. 12, pp. 715–717, Dec. 2004.

APPENDICES

APPENDIX A

Proof of Theorem 3

The proof is built up on the fact that any 2 x 2 sub-matrix does not contain a loop of 4- cycle for three cases: positive – positive, negative – negative and positive – negative elements each others.

For the first case:

Consider a two-by-two sub-matrix $X \subset A_i$ as

$$X = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

In fact, $a \neq b$ as a appears once and only once at each row and column of A_i and so are $a \neq c$, $b \neq d$ and $c \neq d$.

Hence, X has a loop of 4- cycle if and only if,

$a – b = c – d \bmod v$. (1)

For $a – b > 0$ and $c – d > 0$. (A)

This is impossible as $a – b < v$ and $a – b \neq c – d$ for a,b,c and $d \in D_i$, i=1,2…t.

For $a – b < 0$ and $c – d > 0$. (B)

From (1) this implies that b = c & a = d, so (1) becomes, 2a = 2c mod v, this is impossible since, v is an odd number.

For $a – b > 0$ and $c – d < 0$ is equivalent to $a – b < 0$ and $c – d > 0$. (C)

For $a – b < 0$ and $c – d < 0$ is equivalent to $a – b > 0$ and $c – d > 0$. (D)

For the second case:

Consider a two-by-two sub-matrix $X \subset A_i$ as,

$$X = \begin{pmatrix} -a & -c \\ -b & -d \end{pmatrix}.$$

This is equivalent to the first case as $\forall\, x \subset X \rightarrow x \in Dev(D)$.

For the third case:

Consider a two-by-two sub-matrix $X \subset A_i$ as

$$X = \begin{pmatrix} a & -c \\ b & -d \end{pmatrix}.$$

Hence, X has a loop of 4- cycle if and only if

$a – b = d – c \bmod v$. (2)

For $a – b < 0$ and $d – c > 0$ as (B).

From (2) this implies that a = c & b = d, so (2) becomes, 2a = 2c mod v.

This is impossible since, v is an odd number (E)

For $a – b > 0$ and $d – c > 0$ as (A).

From (2) this implies that a = d & b = c, this condition does occur if and only if, k is even i.e. the number of elements in D_i divides 2 (the number '2' here represents the number of division part matrices in A_i i.e. here, there exist positive and negative parts) (F)

For $a – b > 0$ and $d – c < 0$ is equivalent to (B).

For $a – b < 0$ and $d – c < 0$ is equivalent to (A). □

APPENDIX B

Proof of Theorem 4

For this situation, the number of elements in D_i becomes $k - 1$. So, as (F) if k is even, then, $k - 1$ is odd. Hence, X does not exist.

Hint: The eliminated d_{ik} element is arbitrary and A_i here, is $2(k-1)\times(k-1)$ circulant matrices. □

APPENDIX C

Proof of Theorem 5

To prove this theorem, We have to prove that for $0 < i < t$ the upper part (among the elements $A_i^{'}$s), the lower part (among the elements $A_i^{''}$s) and the mixed part (among $(\frac{A_1^{'}}{A_1^{''}}\ \frac{A_2^{'}}{A_2^{''}} \ldots . \frac{A_i^{'}}{A_i^{''}})$) are free of 4-cycles, separately.

Consider a two-by-two sub-matrix X as

$$X = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Where $a,b \in A_i^{'}$, $c,d \in A_j^{'}$ with $0 < i,j \leq t$, then, the pair of differences $a - b$ & $c - d$ satisfies the relation $a - b \neq c - d \bmod v$, due to the property of CDF or PDF. So, the matrices $A_i^{'}$ $0 < i < t$ may not contain 4-cycles, adjacently.

By the same way, it can also be proved that for $a,b \in A_i^{''}$, $c,d \in A_j^{''}$ with $0 < i,j \leq t$, the matrices $A_i^{''}$ $0 < i < t$ may not contain 4-cycles, adjacently.

Now, consider the case where $a \in A_i^{'}$, $b \in A_i^{''}$, $c \in A_j^{'}$, $d \in A_j^{''}$ with $0 < i,j \leq t$, hence, X has a property that $a - (-b) \neq c - (-d) \bmod v$ (follows from $- b \in A_i^{'}$, $-d \in A_j^{'}$). So, X has a loop of 4- cycle if and only if,

$$a–b=c–d \text{ modv} \tag{3}$$

Consequently, $a + b - 2b = c + d - 2d \bmod v$ and we have that $a + b \neq c + d \bmod v$. So, relation (3) is satisfied if and only if $a = b = c = d = 0$ (0 shifts should be prevented). □