

Received October 2, 2020, accepted October 15, 2020, date of publication October 21, 2020, date of current version November 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3032837

Cyclic Low Density Parity Check Codes With the Optimum Burst Error Correcting Capability

SINA VAFI¹, (Senior Member, IEEE)

College of Engineering, IT and Environment, Charles Darwin University, Darwin, NT 0810, Australia

e-mail: sina.vafi@cdu.edu.au

This work was financially supported by the Charles Darwin University.

ABSTRACT The paper presents a new scheme of cyclic codes suitable for the correction of burst errors. This is accomplished by the proper definition of their parity check polynomials in which the difference between orders of every two consecutive elements of the utilized polynomial is unique and in order of power of 2. In the proposed polynomials, the number of applied elements is much lower than their orders (or codes' lengths). This leads to represent codes as a class of low-density parity check (LDPC) codes, while they do not have any 4 cycle in their Tanner graphs. Considering the properties of the circulant matrix and structure of the defined polynomials, it is proven that codes have the optimum burst error-correcting capability. This is evident for short and long length codes. Moreover, it is shown that constructed codes can be combined with Fire codes and demonstrate cyclic codes that are applicable for the simultaneous correction of random and burst errors.

INDEX TERMS Burst error correcting cyclic codes, circulant parity check matrix, low density parity check (LDPC) codes, compound channels.

I. INTRODUCTION

Cyclic codes and their shortened shapes named as shortened cyclic codes are the reputable codes for the protection of data against the burst error. Due to the high performance in the correction of errors as well as rich algebraic structure, these codes were widely used in global standards. Depending on the code's characteristics, burst errors are correctable if the allocated length of code is set greater than the length of error patterns. As a class of linear block codes, the burst error-correcting capability of a (n, k) cyclic code is upper bounded by the value of $\lfloor \frac{n-k}{2} \rfloor$ [1], where n and k are lengths of the codeword and message, respectively.

There are several methods for constructing single or multiple dimensional cyclic codes suitable for the correction of burst errors [2], [3]. As expected, multi-dimensional codes provide better error protection than the one-dimensional codes as they can correct a number of single burst errors but at the expense of more complexity in design due to utilizing two or more codes in their structures. One dimensional cyclic codes can be found either by the computer search or through an algorithm [4]–[7]. BCH codes, Fire codes and Hsu-Kasami-Chien (HKC) codes are amongst the

famous structure-based codes although the majority of them do not provide optimum error correcting capability [8], [9].

Cyclic codes can be represented as a class of low density parity-check (LDPC) codes, when the cyclic property of the code is satisfied and the number of elements applied in their parity check polynomials are much smaller than the code lengths. Cyclic LDPC codes are mainly recognized as suitable codes for random error correction, which are conventionally constructed based on either Euclidean geometry (EG) or projective geometric (PG) algorithm. The analysis reveals that their burst error-correcting capability is not the same as their burst error correcting limit as the algorithm used for correction of burst errors is not implemented based on the canonical structure of the circulant parity check matrix [10].

This paper presents a method for constructing cyclic LDPC codes with the optimum burst error-correcting capability. In parity check polynomials of these codes, the difference between two consecutive orders is in order of power of 2. To analyze the performance of these codes, the algorithm represented in [5] is modified based on the number of submatrices defined at their parity check matrices. Considering the effect of each submatrix, in particular, those having one or two 1s in their rows, new bounds for the burst error-correcting capability of the code will be presented. The results obtained from this analysis are extended to verify the effect

¹The associate editor coordinating the review of this manuscript and approving it for publication was Zilong Liu.

of other submatrices on the correction of bursts with the specified lengths. Based on features of the submatrices and the circulant matrix, it is proven that proposed codes have the optimum burst error-correcting capability. This is evident for short and long length codes, while their rates can be reached to 0.5. As an application, these codes are combined with Fire codes to construct codes suitable for the simultaneous correction of random and burst errors. The organization of the paper is as follows:

Section II introduces the structure of the circulant parity check matrix and its application for the correction of burst errors. Sections III and IV present the structure and analysis of cyclic LDPC codes with the optimum burst error-correcting capability. Section V represents the application of these codes in the construction of cyclic codes suitable for the simultaneous correction of burst and random errors. Finally, Section VI summarizes the paper.

II. BURST ERROR CORRECTING CYCLIC CODES

A linear code \mathbf{C} is called a cyclic code if every cyclic shift of a codeword in \mathbf{C} is also a codeword in \mathbf{C} [4]. A codeword \mathbf{v} can be represented as a n -tuple vector, which is $\mathbf{v} = (v_0, v_1, v_2, \dots, v_{n-2}, v_{n-1})$. It can also be expressed in the polynomial form. That is, $v(x) = v_0 + v_1 x + v_2 x^2 + \dots + v_{n-1}x^{n-1}$. Let $u(x)$ be the polynomial representing k bit message to be encoded by the code. The codeword $v(x)$ is given by

$$v(x) = u(x)g(x) = (u_0 + u_1x + u_2x^2 + \dots + u_{k-1}x^{k-1})g(x),$$

where $g(x) = 1 + g_1 x + g_2 x^2 + \dots + g_{n-k-1}x^{n-k-1} + x^{n-k}$ is the generator polynomial of the code and in the order of $n - k$. For a (n, k) cyclic code, there exists one and only one generator polynomial, which is applied for expression of all codewords. This can be achieved by the implementing a low-complex shift register based encoder. For a binary cyclic code defined in Galois Field 2 ($GF(2)$), g_i s, $1 \leq i \leq n - k - 1$, are either 0 or 1.

It is proven that $g(x)$ of the cyclic code is a factor of $x^n + 1$. Hence, for a (n, k) cyclic code with the generator polynomial $g(x)$, the corresponding *parity check polynomial* $h(x)$ is defined by [4]:

$$h(x) \equiv \frac{x^n + 1}{g(x)}. \tag{1}$$

A cyclic code can be represented by its $(n \times n)$ circulant parity check matrix (H) in the canonical form. The zeroth row of this matrix is constructed by elements of $h(x)$ followed by $n - k - 1$ zeros. Other rows are obtained by cyclic shifts of the zeroth row. In this paper, the representation of rows and columns of the matrix is indexed from zero.

For a non-zero n -tuple over $GF(2)$, a zero span is defined as the sequence of zeros between two 1s. The maximal zero span of the n -tuple, is the maximum length of the zero spans [10]. The *maximal zero span* of the circulant parity check matrix

(δ) is the maximal zero span of the first row, which is given by $\delta = n - k - 1$.

Let C_0 be the zeroth column of the matrix. The module-2 sums of the ℓ th column (C_ℓ), $1 \leq \ell \leq \lfloor \frac{n-k}{2} \rfloor - 1$, with its previous columns are given by

$$A_{2^{\ell-1}+j} = A_j + C_\ell,$$

where $A_0 = C_0$ and $0 \leq j < 2^{\ell-1}$ [10]. In this paper, module-2 sum of columns is expressed by sum.

Example 1: In a circulant matrix, for $1 \leq \ell \leq 3$, sums of C_ℓ s are as follows:

$$\begin{aligned} A_1 &= C_0 + C_1, & A_2 &= C_0 + C_2, & A_3 &= C_0 + C_1 + C_2, \\ A_4 &= C_0 + C_3, & A_5 &= C_0 + C_1 + C_3, & A_6 &= C_0 + C_2 + C_3, \\ A_7 &= C_0 + C_1 + C_2 + C_3. \end{aligned}$$

Bursts with length $\ell + 1$ ($1 \leq \ell \leq \lfloor \frac{n-k}{2} \rfloor - 1$) are correctable if all $A_{2^{\ell-1}+j}$ s, $0 \leq j < 2^{\ell-1}$, generate a unique maximal zero span with length $\delta - \ell$ started from the $(\ell + 1)$ th position [10]. In this case, a simple decoding algorithm can be implemented based on the burst-error correcting capability of the code, which is represented as $B(H_n)$.

The circulant parity check matrix can be divided into two parts. The first part contains the first $n - k$ rows of the matrix, while the remaining rows (or the last k rows) represent the second part of the matrix. Considering this structure, a simpler algorithm for determining burst error correcting capability of codes can be formed, when the sum of columns at the last k rows of the matrix is initially calculated.

For the fixed column ℓ , if each of $A_{2^{\ell-1}+j}$ s, has a maximal zero span less than $\delta - \ell$, the effect of zeros positioned at the end (or second) part of the matrix is considered. Again, for the fixed column ℓ , if any of $A_{2^{\ell-1}+j}$ s has the number of zeros with length greater than or equal to $\delta - 2\ell$, the corresponding sum for the first ℓ rows, represented as the initial part of the matrix, will be calculated.

Figure 1 shows the circulant matrix of $(30,11)$ cyclic code with $h(x) = 1 + x^2 + x^3 + x^5 + x^8 + x^{11}$ and its two parts. For any $0 \leq i \leq 7$, corresponding A_{2^i-1+j} , $0 \leq j < 2^{i-1}$, produces unique maximal zero spans at the first part of the matrix. However, for sums of the 8th column (C_8), all unique maximal zero spans are not provided from the first part of the matrix. For example, define $\hat{C}_0 := [100100101101]$, $\hat{C}_3 := [000100100101]$, and $\hat{C}_8 := [00000001001]$, whose first 11 elements are the zeroth, third and eighth columns of the second part of the matrix, respectively. Their last elements are also the zeroth, third and eighth components of the zeroth row of the circulant matrix. The sum of \hat{C}_i , $i = 0, 3, 8$, will be $\hat{C}_0 + \hat{C}_3 + \hat{C}_8 = (100000000001)$, which yields a zero span with the length of 10. Similarly, the sum of $C_8 = [10010110100000000000000000100]$ with previous columns will generate the zero span with the length of $\delta - 8 = 10$ in the first part. This means that the unique maximal zero span is not gained from the first part of the matrix and consequently the burst error-correcting capability is $B(H_n) = 8$.

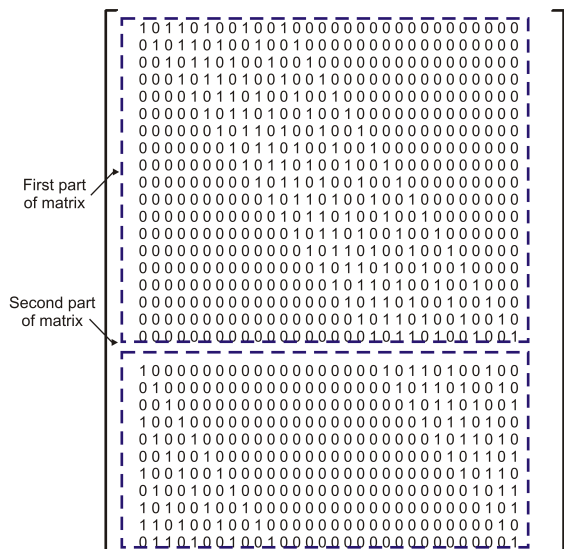


FIGURE 1. Circulant matrix of (30,11) cyclic code and its submatrices formed at the second part of matrix.

III. CYCLIC CODES WITH THE OPTIMUM BURST ERROR CORRECTING CAPABILITY

Let $p(x)$ be a polynomial in $GF(2)$, which is defined by

$$p(x) = 1 + \sum_{i=0}^{m-2} x^{\sum_{j=0}^i (2^\eta)^j}, \quad (2)$$

where η is a positive integer ($\eta \geq 1$). m is represented as number of elements of $p(x)$, which is an integer value greater than or equal to 3 ($m \geq 3$). Obviously, the order of i th element of $p(x)$, $1 \leq i \leq m - 1$, is $\sum_{j=0}^{i-1} (2^\eta)^j$ ¹.

Theorem 1: The polynomial $p(x)$ defined in equation (2) is the parity check polynomial of the (n, k) cyclic code, where $n = \sum_{j=0}^{m-1} (2^\eta)^j$ and $k = \sum_{j=0}^{m-2} (2^\eta)^j$.

Proof: The difference between orders of the i' and $(i' - 1)$ elements of $p(x)$, $1 \leq i' \leq (m - 1)$, is expressed by

$$\sum_{j=0}^{i'-1} (2^\eta)^j - \sum_{j=0}^{i'-2} (2^\eta)^j = (2^\eta)^{i'-1}. \quad (3)$$

For $[p(x)]^{2^\eta}$, the order of $(i' - 1)$ th element is given by

$$\begin{aligned} 2^\eta \sum_{j=0}^{i'-2} (2^\eta)^j &= 2^\eta \left[\sum_{j=0}^{i'-3} (2^\eta)^j + (2^\eta)^{i'-2} \right] \\ &= \sum_{j=0}^{i'-3} (2^\eta)^{j+1} + (2^\eta)^{i'-1} \\ &= \sum_{j=1}^{i'-2} (2^\eta)^j + (2^\eta)^{i'-1}. \end{aligned} \quad (4)$$

Let $n = \sum_{j=0}^{m-1} (2^\eta)^j$ be the order of $(m - 1)$ th element of $x[p(x)]^{2^\eta}$. Indeed, the value of n represents the order of the

¹The order of the zeroth element is 0.

polynomial. The order of $(i' - 1)$ th element of $x[p(x)]^{2^\eta}$ is

$$1 + \sum_{j=1}^{i'-2} (2^\eta)^j + (2^\eta)^{i'-1} = \sum_{j=0}^{i'-2} (2^\eta)^j + (2^\eta)^{i'-1}. \quad (5)$$

Refer to equation (3), it is concluded that this order is equal to the order of i' th element of $p(x)$. Similarly, the order of zeroth element of $x[p(x)]^{2^\eta}$, i.e. 1, is the same as the order of the first element of $p(x)$. Therefore, except x^n , elements of $x[p(x)]^{2^\eta}$ are the same as elements of $p(x)$. $p(x)$ also has an element with the order of zero, which is $x^0 = 1$. As a result, $p(x) + x[p(x)]^{2^\eta} = x^n + 1$ or $p(x)[1 + x(p(x))^{2^\eta-1}] = x^n + 1$.

This means that $p(x)$ is a factor of $x^n + 1$ and can be represented as the parity check polynomial of (n, k) cyclic code, where $k = \sum_{j=0}^{m-2} (2^\eta)^j$ is the order of $p(x)$. Considering equation of (1), $h(x) = p(x)$ and the generator polynomial of the code is $g(x) = 1 + x[h(x)]^{2^\eta-1}$.

Let α_i , $0 \leq i \leq m - 1$, be the order of i th element of $h(x)$, where α_0 and α_{m-1} ($\alpha_0 = 0$, $\alpha_{m-1} = k$) are introduced as the lowest and greatest orders of $h(x)$, respectively.

In the defined $h(x)$, values of n and k are odd numbers. Hence, for all codes, $\lfloor \frac{n-k}{2} \rfloor = \frac{n-k}{2}$. From the $(n-k)$ th row of the parity check matrix, $m - 1$ submatrices are defined, whose columns size is $\frac{n-k}{2}$. For the λ th submatrix ($S\lambda$), $1 \leq \lambda \leq m - 1$, its row size is equal to $\alpha_{m-1-(\lambda-1)} - \alpha_{m-1-\lambda}$, which gives the difference between orders of two consecutive elements. In this paper, the content of the i th row and j th column of the λ th submatrix is denoted by $S\lambda_{i,j}$.

If $\alpha_{m-1} - \alpha_{m-2} = \frac{n-k}{2}$, a $\frac{n-k}{2} \times \frac{n-k}{2}$ submatrix is formed, whose i th row, $0 \leq i \leq \frac{n-k}{2} - 1$, has only one 1 at i th column. The submatrix with such a feature is named exclusive-1 submatrix and formed in codes with $\eta = 1$. The number of submatrices (except the exclusive-1 submatrix) is given by $N = m_{eff} - 1$.

For codes with exclusive-1 submatrix, $m_{eff} = m - 1$. Otherwise, $m_{eff} = m$.

Example 2: Let $p(x) = 1 + x + x^3 + x^7 + x^{15} + x^{31}$ be a polynomial with the order of 31 in $GF(2)$. Refer to equation (2), this polynomial is formed by $\eta = 1$ and $m = 6$. Based on $p(x)$, $x[p(x)]^2 = x + x^3 + x^7 + x^{15} + x^{31} + x^{63}$. Hence, $p(x) + x[p(x)]^2 = x^{63} + 1$. As $p(x)$ is in order of 31 and a factor of $x^{63} + 1$, it can be considered as the parity check polynomial of a $(63,31)$ cyclic code. The generator polynomial of this code is $g(x) = 1 + x[p(x)] = 1 + x^2 + x^4 + x^8 + x^{16} + x^{32}$. In the given $p(x)$, $\alpha_5 = 31$ and $\alpha_4 = 15$. As $\alpha_5 - \alpha_4 = \frac{n-k}{2}$, the circulant parity check matrix of the code includes an exclusive-1 submatrix. It also has four submatrices ($N = 4$) in its second part.

IV. BURST ERROR CORRECTING CAPABILITY OF PROPOSED CYCLIC CODES

In this section, the structure of submatrices is analysed to determine the longest possible zero patterns resulted from sums of columns in the second part of the parity check matrix. Considering columns selected from this part, the zero pattern

obtained from their sum at the initial part of the matrix is determined. This consequently concludes the maximal zero span from the sum of columns, which is positioned at the second and initial parts of the matrix. Then, the length of obtained zero span is compared with the lengths of zero spans formed in the first part of the matrix to determine the burst-error correcting capability of the code.

Lemma 1: Let $Z_1 = \alpha_{m-1} - \alpha_{m-2} - 1$ be the difference between two greatest orders of $h(x)$ minus one. The burst error correcting capability of (n, k) cyclic code with $h(x)$ defined in equation (2) is upper bounded by

$$(i) (B_{low})_{\eta=1} \geq \left\lfloor \frac{n-2k+Z_1+1}{2} \right\rfloor + 1, \text{ if } \eta = 1,$$

$$(ii) (B_{low})_{\eta>1} \geq Z_1, \text{ if } \eta > 1.$$

Proof: As mentioned above, for codes with $\eta = 1$, an exclusive-1 submatrix having $Z_1 + 1$ rows exists at the second part of the parity check matrix. In these codes, $Z_1 = \frac{n-k}{2} - 1$. The content of C_ℓ at ℓ th row of this submatrix, $0 \leq \ell \leq \frac{n-k}{2} - 1$, is 1. Based on this structure, at the zeroth row of the first submatrix, only content of C_0 is 1. Therefore, sums of C_ℓ s at the zeroth row of the first submatrix will be 1 and consequently zero spans formed from each sum in exclusive-1 submatrix will have the length of $Z_1 - \ell$. As $Z_1 < \delta$, lengths of these zero spans will be shorter than the shortest length of zero spans formed at the first part of the matrix, i.e. $\delta - \ell$. Hence, only the last $k - (Z_1 + 2)$ rows of the matrix become important in determining the maximal zero span of sum of columns.

For the ℓ th column, in order to ensure that the unique maximal zero span is from the first part of the matrix, the following condition should be satisfied:

$$k - (Z_1 + 2) + \ell < \delta - \ell$$

or

$$\ell < \frac{n - 2k + Z_1 + 1}{2}. \tag{6}$$

The above inequality means that all bursts with the length shorter than or equal to $\left\lfloor \frac{n-2k+Z_1+1}{2} \right\rfloor + 1$ are correctable. As a result, its burst-error correcting capability is bounded by

$$(B_{low})_{\eta=1} \geq \left\lfloor \frac{n - 2k + Z_1 + 1}{2} \right\rfloor + 1.$$

For codes with $\eta > 1$, the exclusive-1 submatrix is not defined and $Z_1 + 1$ is the number of rows of the first submatrix. In this case, $Z_1 < \frac{n-k}{2} - 1$. At the first submatrix of codes with $\eta > 1$, $S1_{i,i} = 1, 0 \leq i \leq Z_1$. This means, sums of C_ℓ s, $0 \leq \ell \leq Z_1$, will produce zero patterns, whose lengths are $Z_1 - \ell$ or shorter. These lengths are shorter than $\delta - \ell$. At the zeroth row of the second submatrix, $S2_{0,0} = 1$ and $S2_{0,Z_1+1} = 1$. Considering this, sum of columns at the zeroth row of $S2$ is also 1. Hence, the longest zero pattern obtained from sums will be $k - (Z_1 + 2)$, which can be started from the first row of $S2$. The longest possible zero pattern generated from sums at the initial part of the matrix is Z_1 . Therefore, the maximal zero span formed at the second and initial parts of the parity check matrix will be $(\zeta_{span})_2 = k - (Z_1 + 2) + Z_1 = k - 2$.

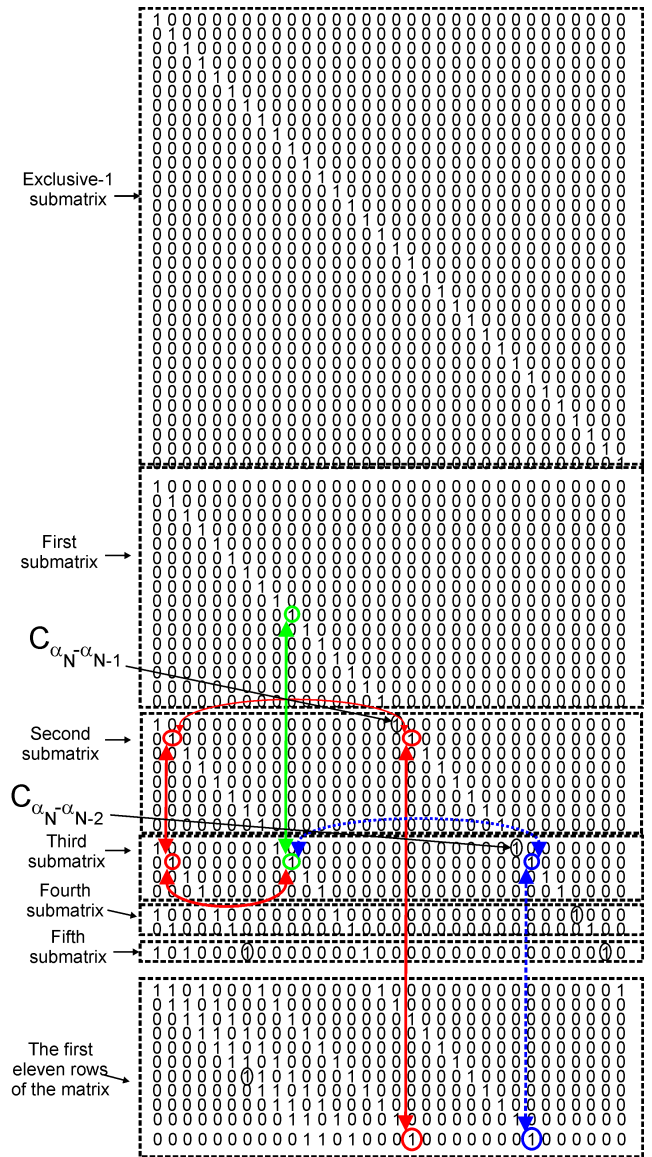


FIGURE 2. Structure of the second and initial parts of parity check matrix for (127,63) cyclic code.

On the other hand, in the first part of the matrix, the shortest zero span is $(\zeta'_{span})_2 = \delta - \ell = n - k - 1 - Z_1$, where $\ell = Z_1$. For codes with $\eta > 1$, $Z_1 < \frac{n-k}{2} - 1$ and $n > 4k$. Hence, $(\zeta'_{span})_2 > (\zeta_{span})_2$. This means, all bursts with length Z_1 or shorter can be correctable. As a result, $(B_{low})_{\eta>1} \geq Z_1$.

Example 3: Figure 2 shows the second part as well as the first eleven rows of the parity check matrix for (127,63) cyclic code. It only includes the first 32 columns. The parity check polynomial of this code is $h(x) = 1 + x + x^3 + x^7 + x^{15} + x^{31} + x^{63}$ with $m = 7$, $Z_1 = 31$ and $\eta = 1$. This matrix includes an exclusive-1 submatrix. Hence, $m_{eff} = m - 1 = 6$ and $N = m_{eff} - 1 = 5$ submatrices are defined. In exclusive-1 submatrix, maximal zero spans obtained from sums of C_ℓ s, $0 \leq \ell \leq 31$ is shorter than $\delta - (\frac{n-k}{2} - 1) = 32$. This means, only the last 29 rows of the matrix become important

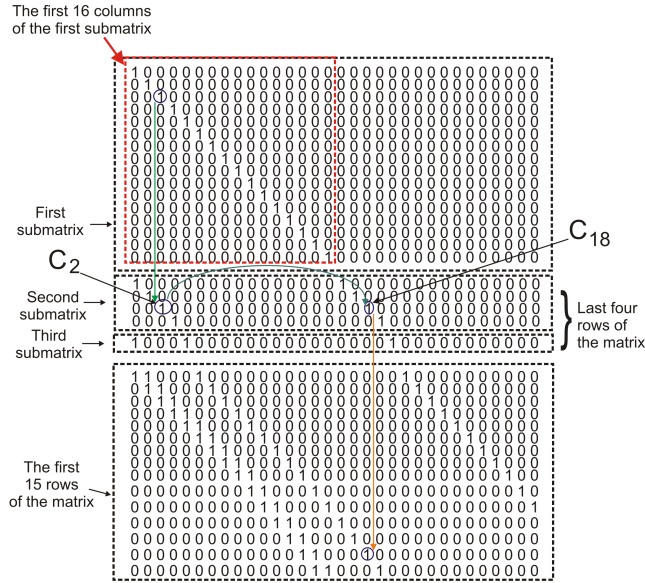


FIGURE 3. Structure of the second and initial parts of parity check matrix for (85,21) cyclic code.

in determining the maximal zero span at the second part of the matrix. Therefore, $(B_{low})_{\eta=1} \geq 17$.

Example 4: Figure 3 shows the second and initial parts of the circulant matrix for (85,21) cyclic code. The parity check matrix of this code is $h(x) = 1 + x + x^5 + x^{21}$. In the first submatrix, $S1_{i,i} = 1, 0 \leq i \leq Z_1$, where $Z_1 = 15$. This means that at the first 16 rows of the first submatrix as well as the zeroth row of the second submatrix, sums of $C_{\ell s}$, $0 \leq \ell \leq Z_1$ are 1. The longest possible zero pattern formed in the second part of the matrix is started from the first row of the second submatrix. This length is $k - (Z_1 + 2) = 4$. At the initial part of the matrix, the longest zero pattern is 15, where $\ell = Z_1$. Based on this structure, the maximal zero span obtained from sums of $C_{\ell s}$ is 18, which is shorter than $\delta - Z_1 = 48$. Therefore, the given code can correct all bursts with length $Z_1 = 15$ or shorter. Hence, $(B_{low})_{\eta>1} \geq 15$.

Lemma 2: Cyclic codes with the $h(x)$ given in equation (2) can correct bursts with the length of $\alpha_N - \alpha_{N-2} - 1$ or shorter.

Proof: In the second submatrix, $S2_{\gamma,\gamma} = 1$ and $S2_{\gamma,\gamma+\alpha_N-\alpha_{N-1}} = 1$, where $0 \leq \gamma \leq \alpha_{N-1} - \alpha_{N-2} - 1$.

Meanwhile, in the first submatrix, $S1_{i,i} = 1$, where $0 \leq i \leq \alpha_N - \alpha_{N-1} - 1$. Hence, in sums of $C_{\ell s}$, $\alpha_N - \alpha_{N-1} \leq \ell \leq \alpha_N - \alpha_{N-2} - 1$, the longest zero pattern is positioned at $\ell - (\alpha_N - \alpha_{N-1}) + 1$ th row of the first submatrix. This means that $C_{j s}$, $\alpha_{N-1} - \alpha_{N-2} \leq j \leq \alpha_N - \alpha_{N-1} - 1$, are not involved in the sum.

In the third submatrix, $S3_{0,0} = 1$, $S3_{0,\alpha_{N-1}-\alpha_{N-2}} = 1$, and $S3_{0,\alpha_N-\alpha_{N-2}} = 1$. In order to have zero from sums, C_0 and $C_{\alpha_{N-1}-\alpha_{N-2}}$ should be involved. However, as mentioned in above, $C_{\alpha_{N-1}-\alpha_{N-2}}$ is one of the columns, which is not involved in the sum. As a result, sum of those columns generating the longest zero pattern at the first and second submatrices will be 1 at the zeroth row of the third submatrix. In this case, lengths of zeros formed at the first and second

submatrices are $(\alpha_N - \alpha_{N-1}) - [\ell - (\alpha_N - \alpha_{N-1}) + 1]$ and $\alpha_{N-1} - \alpha_{N-2}$, respectively. Hence, the length of zero span will be $(\zeta_{span})_2 = 2(2^\eta)^{m_{eff}-2} + (2^\eta)^{m_{eff}-3} - \ell - 1$, where $\alpha_N - \alpha_{N-1} = (2^\eta)^{m_{eff}-2}$ and $\alpha_{N-1} - \alpha_{N-2} = (2^\eta)^{m_{eff}-3}$. The length of this zero span is shorter than the length of the zero span formed at the first part of the matrix, i.e. $(\zeta'_{span})_2 = (2^\eta)^{m-1} - \ell - 1$, where $n - k = (2^\eta)^{m-1}$.

As mentioned, when $C_{\alpha_{N-1}-\alpha_{N-2}}$ is ignored, sums of $C_{\ell s}$ at the zeroth row of the third submatrix will be 1. In this case, the greatest length of the zero pattern positioned at the third and following submatrices is $\alpha_{N-2} - 1$. Therefore, the maximal zero span placed at these submatrices and the initial part of the matrix will be $\alpha_{N-2} - 1 + \ell$. Obviously, for all codes defined by equation (2), $\delta - \ell > \alpha_{N-2} - 1 + \ell$. Hence, the length of the above zero span is shorter than the one formed at the first part of the matrix.

If $C_{\alpha_{N-1}-\alpha_{N-2}}$ is used in the sum, the longest length of the zero pattern obtained from sums of $C_{\ell s}$ will be $\alpha_N - (\alpha_{N-1} - \alpha_{N-2} + 1)$. This pattern is started from $(\alpha_{N-1} - \alpha_{N-2} + 1)$ th row of the first submatrix. In this case, columns positioned between $C_{\alpha_{N-1}-\alpha_{N-2}+1}$ and $C_{\alpha_N-\alpha_{N-1}-1}$ are not involved in the sum. Let $X = \alpha_{N-1} - \alpha_{N-2}$. At $Y = \alpha_N - 2\alpha_{N-1} + X$ th row of the matrix, content of $C_{\alpha_{N-2}}$ at the zeroth row of the matrix will be placed at $C_{\alpha_N-\alpha_{N-1}}$ of the Y th row of the matrix. Other columns with the content of 1 are either between $C_{\alpha_{N-1}-\alpha_{N-2}+1}$ and $C_{\alpha_N-\alpha_{N-1}-1}$ or after $C_{\alpha_N-\alpha_{N-2}-1}$. Of these columns with the content of 1, only $C_{\alpha_{N-1}-\alpha_{N-2}}$ is used in the sums of columns at the second part of the matrix. Hence, sum of selected columns at Y th row of the matrix is 1 and consequently the length of zero span formed at the second and initial parts of the matrix is $2(\alpha_N - \alpha_{N-1}) - 1$. This length is shorter than the shortest length of zero spans placed at the first part of matrix, which is the value of $\delta - (\frac{n-k}{2} - 1) = 2(\alpha_N - \alpha_{N-1})$. Hence, all bursts with the length of $\alpha_N - \alpha_{N-2} - 1$ or shorter are correctable. ■

The above two lemmas conclude that the maximal zero span of sums of $C_{\ell s}$, $1 \leq \ell \leq \alpha_N - \alpha_{N-2} - 1$, are positioned at the first part of the parity check matrix. To precisely determine the burst error correcting capability of codes, it is essential to consider effect of other columns positioned between $C_{\alpha_N-\alpha_{N-2}}$ and $C_{\frac{n-k}{2}-1}$.

Theorem 2: A cyclic code with the parity check polynomial of $h(x)$ given in equation (2) has the optimum burst error correcting capability.

Proof: To verify the effect of the third and following submatrices, columns positioned after $C_{\alpha_N-\alpha_{N-2}-1}$ are considered in sums of $C_{\ell s}$, $1 \leq \ell \leq \frac{n-k}{2} - 1$. This leads to represent cases for the sum of $C_{X s}$, $\alpha_N - \alpha_{N-2} \leq X' \leq \frac{n-k}{2} - 1$, which generate zero patterns from a row of the first submatrix to the end of the matrix. A common point of the cases is utilizing even number columns with the content of 1 at every row of $S_{\lambda s}$, $3 \leq \lambda \leq N$ to determine the maximal zero span positioned at the second and initial parts of the matrix.

1) SUM OF $C_{X'}$ WITH NUMBER OF COLUMNS POSITIONED BETWEEN C_0 AND $C_{\alpha_{N-1}-\alpha_{N-2}}$

At a row of S_λ with $C_{X'} = 1$, odd number of C_j s $0 \leq j \leq X' - (\alpha_N - \alpha_{N-2})$ should be applied to produce zero for the sum of the selected columns. In rows with $C_{X'} = 0$, even number of C_j s, $0 \leq j' \leq \alpha_{N-1} - \alpha_{N-2}$ should be applied. Alternatively, it is possible to have sum of odd number of C_j s with the content of 1 and a column with the content of 1 positioned between $C_{\alpha_N-\alpha_{N-2}}$ and $C_{X'}$. In addition to $C_{\alpha_N-\alpha_{N-1}}$, for each of C_j s and $C_{j'}$ s applied in the sum, $C_{j+(\alpha_N-\alpha_{N-1})}$ and $C_{j'+(\alpha_N-\alpha_{N-1})}$ will also be used to ensure that sum of columns remains zero in the second submatrix. Let j_{select} be the greatest index of C_j s and $C_{j'}$ s used in the sum. Let $Y = \alpha_N - 2\alpha_{N-1} + j_{select}$. At Y th row of the parity check matrix, columns with the content of 1 are placed at $C_{Y+\alpha_i}$, where $0 \leq i \leq N$. Of these columns, only $C_{j_{select}+\alpha_N-\alpha_{N-1}}$ is used in the sum of columns positioned in the second part of the matrix. As a result, sum of columns selected from the second part of the matrix produces a zero pattern with the length of $\alpha_N - 2\alpha_{N-1} + j_{select}$ at the initial part of the matrix. Hence, the maximal zero span positioned at the second and initial parts of the matrix will be $2(\alpha_N - \alpha_{N-1}) - 1$, which is shorter than the shortest length of zero spans formed at the first part of the matrix, i.e. the value of $\delta - (\frac{n-k}{2} - 1) = 2(\alpha_N - \alpha_{N-1})$.

2) SUM OF $C_{X'}$ WITH NUMBER OF COLUMNS POSITIONED BETWEEN C_0 AND $C_{\alpha_{N-1}-1}$

This case is considered as the extension of the previous case as all columns with the content of 1 positioned at S_λ s, $3 \leq \lambda \leq N$ can be applied in sums.

In a row of S_λ with $C_{X'} = 1$ s, the sum of columns will be zero, when an odd number of columns with the content of 1 positioned before $C_{X'}$ is applied.

Assume $C_{X'}$ and C_j are applied in the sum, where $j = X' - (\alpha_N - \alpha_{N-1})$. In the considered row, in addition to these two columns, there exist a number of columns with the content of 1, which are positioned at $C_{j'}$ s, where $j' = j - (\alpha_{N-1} - \alpha_{N-U})$ and $2 \leq U \leq \lambda - 1$.

In rows of S_λ with $C_{X'=0}$, a C_{j_1} , $\alpha_{N-1} - \alpha_{N-2} + 1 \leq j_1 \leq \alpha_{N-1} - 1$, with the content of 1 exists, whose sum with the $C_{j'_1}$, $j'_1 = j_1 - (\alpha_{N-1} - \alpha_{N-U})$, will be zero.

Based on C_{j_1} s and $C_{j'_1}$ s applied in the sum, $C_{j'_1}$ s and $C_{j''}$ s will be used to ensure that sum of columns at the second submatrix is zero, where $j''_1 = j'_1 + (\alpha_N - \alpha_{N-1})$ and $j'' = j' + (\alpha_N - \alpha_{N-1})$.

Let j_{select} be the greatest index of C_j s and C_{j_1} s involved in the sum. Let $Y = \alpha_N - 2\alpha_{N-1} + j_{select}$. At Y th row of the parity check matrix, columns with the content of 1 are placed at $C_{Y+\alpha_i}$, where $0 \leq i \leq N$. Of these columns, only $C_{j_{select}+\alpha_N-\alpha_{N-1}}$ is used in the sum of columns positioned at the second part of the matrix. As a result, sum of columns selected from the second part of the matrix produces a zero pattern with the length of $\alpha_N - 2\alpha_{N-1} + j_{select}$ at the initial part of the matrix. Hence, the maximal zero span positioned at the second and initial parts of the matrix will be $2(\alpha_N - \alpha_{N-1}) - 1$, which is shorter than the shortest length of zero

spans formed in the first part of the matrix, i.e. the value of $\delta - (\frac{n-k}{2} - 1) = 2(\alpha_N - \alpha_{N-1})$.

The above analyses conclude that at the initial part of the matrix, the longest zero pattern obtained from the sum of columns will be $\alpha_N - 2\alpha_{N-1} + (col)_{sel}$. $(col)_{sel}$, $1 \leq (col)_{sel} \leq \alpha_N - \alpha_{N-1} - 2$, is the column with the content of 1 such that the zero pattern is started from $(col)_{sel} + 1$ th row of the first submatrix. At the second part of the matrix, the longest zero pattern formed from the sum of columns will be $\alpha_N - (col)_{sel} - 1$. As a result, the maximal zero span positioned in the second and initial parts of the matrix will be $2(\alpha_N - \alpha_{N-1}) - 1$. This maximal zero span is shorter than the shortest length of zero spans formed at the first part of the matrix, i.e. $\delta - (\frac{n-k}{2} - 1) = \frac{n-k}{2}$. Therefore, all bursts with length $\frac{n-k}{2}$ or shorter are correctable. ■

Example 5: In the parity check matrix of (127,63) cyclic code shown in Figure 2, let $X' = 30$. At the last row of the matrix, $C_{X'} = 1$. To have zero from sum of columns in this row of the matrix, odd number of columns with content of 1 positioned between C_0 and C_8 can be applied. In this case, $C_0 + C_2 + C_6 + C_{30} = 0$. C_{26} is added to this sum to provide zero at the second row of the third submatrix. C_8 and C_{16} are also added to the sum, which conclude zero at the zeroth rows of the second and third submatrices. As a result, $C_0 + C_2 + C_4 + C_6 + C_{30} + C_8 + C_{16} + C_{26}$ will conclude zero patterns placed at the third, fourth and fifth submatrices. As C_2 , C_4 , and C_6 are used, C_{18} , C_{20} , and C_{22} will also be applied in the sum to produce zero pattern at the second submatrix. Among C_0, C_2, C_4, C_6 and C_8 , C_8 has the greatest index. Hence, the zero pattern obtained from the sum of columns is started from the 9th row of the first submatrix. At 9th row of the matrix, among the mentioned columns, only C_{16} with the content of 1 was used in the sum. Indeed, other columns with the content of 1 are either C_{24} or placed between C_9 and C_{15} . Note that as C_0 and C_8 are used, C_{24} is exempted to make sure that the sum of columns remains zero at the zeroth row of the third submatrix. The sum of the mentioned columns will result in zero patterns with lengths of 22 and 9 at the second and initial parts of the matrix, respectively. Hence, the length of the zero span obtained from the sum of the above columns will be 31, which is shorter than the shortest length of zero spans formed in the first part of the matrix, i.e. the value of $\delta - 31 = 32$.

Example 6: In the parity check matrix of (127,63) cyclic code shown in Figure 2, let $X' = 25$. In the first row of the third submatrix, $C_{25} = 1$. In this row, other columns with the content of 1 are C_9 and C_1 . $C_0 + C_1 + C_8 + C_{12} + C_{14} + C_{13} + C_{25}$ will conclude zero patterns at the third, fourth and fifth submatrices. Of these columns positioned between C_0 and C_{14} , C_{14} has the greatest index. Therefore, $j_{select} = 14$ and $C_{j_{select}} = C_{14}$. Sum of the above columns with C_{16} and C_{17} will form a zero pattern with the length of 16, which is started from the 15th row of the first submatrix. At 15th row of the matrix, among the mentioned columns, only content of C_{16} is 1. This will result in a zero pattern with the length of 15 at the

initial part of the matrix. The length of the zero span obtained from the sum of above columns will be 31, which is shorter than the shortest length of zero spans formed at the first part of the matrix $\delta - 31 = 32$. Hence, all bursts with the length of 32 or shorter are correctable.

A. SPECIAL CASE

It is possible to have a zero pattern, which is started from the zeroth row of the first submatrix with the length of α_N . This is achievable from $C_0 + C_{\alpha_N - \alpha_i}$, where $1 \leq i \leq N - 1$ and $C_0 = 1$. Moreover, in the zeroth row of the matrix content of C_0 is 1. Sum of selected columns at the zeroth row of the matrix will be 1 because every two rows of the matrix do not have more than one common 1. Hence, the length of zero span will be α_N , which is shorter than the shortest length of zero spans formed at the first part of the matrix.

Example 7: In parity check matrix of (127,63) cyclic code shown in Figure 2, there exists a sum of columns, which generates zero pattern from 10th row of the first submatrix. In addition to C_0 and C_{16} , C_1 and C_{17} should be involved to ensure that the sum remains zero at the second and third submatrices. Based on C_1 , C_5 and C_{21} are also summed to conclude zero from the fourth and second submatrices. Similarly, C_6 and C_{22} are used to have zero from the sum of columns at the fifth and second submatrices. Zero is resulted from the sum at the zeroth rows of the third and fourth submatrices by utilizing C_{24} and C_{28} . Such this zero pattern will be formed, when $C_{X'}$ s, $10 \leq X' \leq 15$, are not applied in the sum. Moreover, C_{25} can not be used since its sum with already selected C_1 and C_9 will become 1 at the first row of the third submatrix. Based on the above conditions, the length of this zero pattern will be 21. At the tenth row of the matrix, amongst columns with the content of 1 only C_{17} was involved in the sum. Hence, the sum of selected columns will be 1 and consequently a zero pattern with the maximum length of 10 is obtained. As a result, the length of obtained zero span will be 31, which is shorter than the shortest length of the zero spans formed at the first part of the matrix (the value of 32).

Example 8: In the parity check matrix of (85,21) cyclic code shown in Figure 3, the sum of C_0 , C_{16} , and C_{20} generates zero pattern with the length of 20 in the second part of the matrix. At 11th row of the matrix, among these columns, only content of C_{16} is 1. Hence, the longest possible length of that sum formed at the initial part of the matrix is 12. As a result, the length of zero span is $20+11=31$. This length is shorter than the shortest length of zero spans formed at the first part of the matrix, i.e. $\delta - \ell = 32$, where $\ell = \frac{n-k}{2} - 1$.

V. APPLICATION OF PROPOSED LDPC CODES FOR COMPOUND CHANNELS

Proposed cyclic LDPC codes can be combined with Fire codes to construct cyclic codes suitable for the compound channel, where burst and random errors are mixed.

For $GF(2^m)$, let $g_F(x) = (x^b + 1)\phi(x)$ be generator polynomial of (n, k) Fire code, where n is an order of $2^m - 1$

TABLE 1. Cyclic codes suitable for the compound channel.

Code	$g(x)$	Fire code(b)	LDPC code
(15,4)	(0,1,2,3,5,7,8,11)	(15,11)(3)	(15,7)
(63,24)	(0,1,2,4,7,9,11,15,16,23,32,39)	(63,50)(7)	(63,31)
(63,18)	(0,1,2,3,5,6,7,8,9,11,12,13,14,16,17,18,19,21,23,23,26,29,32,35,38,39,42,45)	(63,48)(7)	(63,31)
(63,12)	(0,1,2,6,8,14,15,16,17,20,21,23,24,25,29,30,35,36,37,38,41,43,45,46,48,51)	(63,44)(7)	(63,31)
(255,112)	(0,1,2,4,8,15,17,19,23,31,32,47,64,79,128,143)	(255,232)(15)	(255,127)
(255,104)	(0,1,2,6,13,14,15,16,17,20,22,24,28,29,32,35,38,39,40,47,51,52,53,55,64,68,69,70,72,79,83,84,85,87,128,132,133,134,136,143,147,148,149,151)	(255,224)(15)	(255,127)
(4095,2026)	(0,1,2,4,8,16,21,22,23,25,29,32,37,53,64,85,128,149,256,277,512,533,1024,1045,2048,2069)	(4095,4070)(21)	(4095,2047)
(4095,2022)	(0,3,8,9,12,16,17,20,21,24,27,30,32,36,37,38,41,53,54,57,64,65,68,85,86,89,128,129,132),149,150,153,256,257,260,277,278,281,512,513,516,533,534,537,1024,1025,1028,1045,1046,1049,2048,2049,2052,2069,2070,2073)	(4095,4070)(21)	(4095,2047)
(4095,2020)	(0,3,4,5,6,7,9,10,14,16,17,21,22,24,25,26,27,28,30,31,32,33,35,37,43,53,54,59,64,65,70,85,86,91,128,129,134,149,150,155,256,257,262,277,278,283,512,513,518,533,534,539,1024,1025,1030,1045,1046,1051,2048,2049,2054,2069,2070,2075)	(4095,4068)(21)	(4095,2047)
(4095,2038)	(0,2,5,6,7,8,10,12,13,15,18,23,24,25,32,33,34,39,40,41,64,65,61,71,72,73,128,129,130,135,136,137,256,257,258,263,264,265,512,513,514,519,520,521,1024,1025,1026,1031,1032,1033,2048,2049,2050,2055,2056,2057)	(4095,4086)(7)	(4095,2047)

and represented as $n = a \cdot b$. In this case, a and b are two integers and $\frac{b+1}{2} \leq m$. Moreover, $\phi(x)$ is a polynomial, which divides $1 + x^b + x^{2b} + \dots + x^{(a-1)b}$. The generator polynomial of the cyclic code applied for the compound channel is represented by the least common multiple (LCM) of two generator polynomials as follows [4]:

$$g(x) = LCM(g_F(x), g_{LDPC}(x)), \quad (7)$$

where $g_{LDPC}(x)$ is the generator polynomial of the cyclic LDPC codes constructed by $\eta = 1$. As $g_{LDPC}(x)$ is not order of $(x + 1)$, the above polynomial is given by

$$g(x) = (x^b + 1)LCM(g_{LDPC}(x), \phi(x)). \quad (8)$$

Constructed cyclic codes are capable for correction of burst errors with length b as well as t or less random errors, where t is the error correcting capability of the cyclic code. Table 1 shows a number of cyclic codes constructed on the basis of the above method. In the second column, values written in the parenthesis denote orders of elements of $g(x)$. Some short codes are comparable with other well-known codes. For example (15,4) code can correct bursts with lengths 2 or 3, which is equal to capability of (15,5) BCH code. However, (15,4) with the minimum weight of 8 can also correct 3 random errors. The parity check polynomial of this code is $h(x) = 1 + x + x^4$. As the difference between any two orders of $h(x)$ is unique, Tanner graph of the code does not include any 4 cycle. Hence, decoding of this LDPC code can be accomplished by a hard-decision based technique (such as bit flipping), which requires lower complexity than decoding techniques applicable for (15,5) BCH code. Similarly, (63,24) cyclic codes proposed for the compound channel has the minimum weight of 12. This means that the code can correct all burst errors with length 7 as well as five random errors. This code is comparable with (63,24) BCH code, which corrects either seven random errors or burst errors with length 17 or less [10].

VI. CONCLUSION AND FUTURE WORK

This paper represented cyclic LDPC codes with the optimum burst-error correcting capability. Considering the parity check matrix of these codes, bounds for determining their burst error correction were presented. Codes have flexibility in their lengths and rates. This allowed them to be combined with Fire codes to demonstrate a new scheme of cyclic codes suitable for simultaneous correction of random and burst errors. In future work, application of these codes for correction of multiple burst errors will be followed.

REFERENCES

- [1] S. Reiger, "Codes for the correction of 'clustered' errors," *IEEE Trans. Inf. Theory*, vol. IT-6, no. 1, pp. 16–21, Mar. 1960.
- [2] E. Olcayto and T. Lesz, "Class of linear cyclic block codes for burst errors occurring in one-, two- and three-dimensional channels," *IEE Proc.*, vol. 130, no. 5, pp. 468–475, Aug. 1983.
- [3] S. Roy and S. S. Garani, "Two-dimensional algebraic codes for multiple burst error correction," *IEEE Commun. Lett.*, vol. 23, no. 10, pp. 1684–1687, Oct. 2019.
- [4] S. Lin and D. Costello, *Error Control Coding: Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.
- [5] S. Vafi and N. R. Majid, "A lower bound for burst error correcting capability of low rate binary cyclic codes," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 33–36, Jan. 2016.
- [6] S. Vafi and P. H. Dung, "Binary burst error correcting cyclic codes designed with the circulant parity check matrix," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1277–1279, Aug. 2012.
- [7] A. S. Orozco, "Efficient algorithms for searching multiple burst-error correcting cyclic and shortened cyclic codes," Ph.D. dissertation, Dept. Informática, Despacho 431, Univ. Complutense de Madrid, Madrid, Spain, Jun. 2014.
- [8] P. Fire, "A class of multiple-error correcting binary codes for non independent errors," *Reconn. Syst. Lab Sylvania, Sylvania, OH, USA*, Tech. Rep. RSL-E-2, Mar. 1959.
- [9] W. Zhou, "On the maximum burst correcting capability of Hsu-Kasami-Chien codes," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2352–2355, Nov. 2017.
- [10] S. Song, S. Lin, K. Abdel-Ghaffar, Z. Ding, W. H. Fong, and M. P. C. Fossorier, "Burst decoding of cyclic codes based on circulant parity-check matrices," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1038–1047, Mar. 2010.



SINA VAFI (Senior Member, IEEE) received the Ph.D. degree from the University of Wollongong (UoW), Wollongong, NSW, Australia. He is currently a Senior Lecturer of electrical and electronics engineering with Charles Darwin University (CDU), where he get-chartered of Engineers Australia (EA). He also leads number of research projects in the abovementioned fields. His research interests include algebraic coding theory and broadband wireless video transmission systems.

...