Non-Binary LDPC Codes vs. Reed-Solomon Codes

Bo Zhou, Li Zhang, Jingyu Kang, Qin Huang, Ying Y. Tai and Shu Lin
Department of Electrical and Computer Engineering
University of California, Davis
Davis, CA 95616
Email: bozhou, liszhang, jykang, qinhuang, shulin@ece.ucdavis.edu

Meina Xu
Northrop Grumman Space Technology
One Space Park
Redondo Beach, CA 90278
Email: meina.xu@ngc.com

***Abstract*—This paper investigates the potential of non-binary LDPC codes to replace widely used Reed-Solomon (RS) codes for applications in communication and storage systems for combating mixed types of noise and interferences. The investigation begins with presentation of four algebraic constructions of *RS-based* non-binary *quasi-cyclic* (QC)-LDPC codes. Then, the performances of some codes constructed based on the proposed methods with iterative decoding are compared with those of RS codes of the same lengths and rates decoded with the hard-decision Berlekamp-Massey (BM)-algorithm and the algebraic soft-decision Kötter-Vardy (KV)-algorithm over both the AWGN and a Rayleigh fading channels. Comparison shows that the constructed non-binary QC-LDPC codes significantly outperform their corresponding RS codes decoded with either the BM-algorithm or the KV-algorithm. Most impressively, *the orders of decoding computational complexity* of the constructed non-binary QC-LDPC codes decoded with 5 and 50 iterations of a *Fast Fourier Transform* based sum-product algorithm are much smaller than those of their corresponding RS codes decoded with the KV-algorithm, while achieve 1.5 to 3 dB coding gains. The comparison shows that well designed non-binary LDPC codes have a great potential to replace RS codes for some applications in communication or storage systems, at least before a very efficient algorithm for decoding RS codes is devised.**

I. Introduction

Although a great deal of research effort has been expended in study and construction of LDPC codes [1], most of this research has been focused only on binary LDPC codes, very little being done in the design and construction of non-binary LDPC codes. Non-binary LDPC codes were first investigated by Davey and MacKay in 1998 [2]. In their paper, they also generalized the sum-product algorithm (SPA) for decoding binary LDPC codes to decode q-ary LDPC codes. We refer to this generalized SPA for decoding q-ary LDPC codes as the q-ary SPA (QSPA). To reduce decoding computational complexity, Mackay and Davey also devised a *Fast Fourier Transform* (FFT) based QSPA, called FFT-QSPA in 2000 [3]. Their work on FFT-QSPA was recently further improved by Declercq and Fossorier [4].

A q-ary regular LDPC code $\mathcal{C}$ is given by the null space over GF(q) of a sparse parity-check matrix $\mathbf{H}$ over GF(q) that has the following structural properties: 1) each row has weight ρ; 2) each column has weight γ. We further impose the following additional structural property which is enforced in almost all constructions of LDPC codes: 3) no two rows (or two columns) have more than one place where they both have nonzero components. Such a parity-check matrix $\mathbf{H}$ is said to be (γ,ρ)-regular and the code $\mathcal{C}$ given by its null space is called a (γ,ρ)-regular LDPC code. Structural property 3 is a constraint on the rows and columns of the parity-check matrix $\mathbf{H}$ and is referred to as the *row-column (RC)-constraint*. This RC-constraint ensures that the minimum distance of the (γ,ρ)-regular LDPC code $\mathcal{C}$ is at least $\gamma + 1$ and its Tanner graph [5] has a girth of at least 6 [6], [7]. If the columns and/or rows of $\mathbf{H}$ have *varying* weights, then the null space of $\mathbf{H}$ gives an *irregular* LDPC code. If $\mathbf{H}$ is an *array* of *sparse circulants* over GF(q), then its null space gives a QC-LDPC code over GF(q) [6]–[8]. Encoding of a QC-LDPC code can be implemented using simple shift-registers with complexity linearly proportional to the number of parity-check symbols of the code [9].

In this paper, we present a general and four specific algebraic constructions of RS-based QC-LDPC codes (construction based on RS codes). Some codes are constructed based on these methods and their performances over the AWGN and a Rayleigh fading channel with iterative decoding using the FFT-QSPA are compared with those of RS codes of the same lengths and rates decoded with either hard-decision (HD) BM-algorithm [7], [10], [11] and/or algebraic soft-decision (ASD) KV-algorithm [12]. Also presented in the paper is a class of *asymptotically optimal* erasure-burst correction QC-LDPC codes.

II. Matrix Dispersion of Field Elements

Consider the Galois field GF(q) with q element where q is a power of a prime. Let α be a primitive element of GF(q). Then, the power, $\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha, \ldots, \alpha^{q-2}$ give all the elements of GF(q) and $\alpha^{q-1} = 1$. For each nonzero element α^i in GF(q) with $0 \leq i < q-1$, we form a $(q-1)$-tuple over GF(q), $\mathbf{z}(\alpha^i) = (z_0, z_1, \ldots, z_{q-2})$, whose components correspond to the $q-1$ nonzero components of GF(q), where the ith component $z_i = \alpha^i$ and all the other components are equal to zero. This $(q-1)$-tuple over GF(q) is called the q-ary *location-vector* of the field element α^i and has a single nonzero component. The single nonzero components of the q-ary location-vectors of two different nonzero elements of

This research was supported by NASA under the Grant NNX07AK50G, NSF under the Grant CCF-0727478, and the gift grant from Northrop Grumman Space Technology.

GF(q) are at two different locations. The q-ary location-vector of the 0-element of GF(q) is defined as the all-zero $(q-1)$-tuple, $\mathbf{z}(0) = (0, 0, \ldots, 0)$.

Let δ be a nonzero element of GF(q). Then, the q-ary location-vector $\mathbf{z}(\alpha\delta)$ of the field element $\alpha\delta$ is the right *cyclic-shift* (one place to the right) of the location-vector $\mathbf{z}(\delta)$ of δ multiplied by α. Form a $(q-1) \times (q-1)$ matrix $\mathbf{A}$ over GF(q) with the q-ary location-vector of $\delta, \alpha\delta, \ldots, \alpha^{q-2}\delta$ as rows. Matrix $\mathbf{A}$ is a special type of *circulant permutation matrix* (CPM) over GF(q) for which each row is the right cyclic-shift of the row above it multiplied by α and the first row is the right cyclic-shift of the last row multiplied by α. Such a matrix is called a q-ary *α-multiplied* CPM. Since $\mathbf{A}$ is obtained by dispersing δ *horizontally* and *vertically*, $\mathbf{A}$ is referred to as the *two-dimensional $(q-1)$-fold matrix dispersion* of δ (simply matrix dispersion of δ). It is clear that the dispersion of the 0-element is a $(q-1) \times (q-1)$ zero matrix. Dispersion of a field element into a binary CPM was recently introduced in [13], [14].

III. Construction of Non-binary QC-LDPC Codes by Matrix Dispersion

In this section, we present a general method for constructing QC-LDPC codes over GF(q). Construction begins with an $m \times n$ matrix over GF(q),

$$\mathbf{W} = \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{m-1} \end{bmatrix} = \begin{bmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,n-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{m-1,0} & w_{m-1,1} & \cdots & w_{m-1,n-1} \end{bmatrix}, \quad (1)$$

whose rows satisfies the following two constraints: 1) for $0 \leq i < m$, $0 \leq k, l < q-1$, and $k \neq l$, $\alpha^k \mathbf{w}_i$ and $\alpha^l \mathbf{w}_i$ differ in at least $n-1$ places; 2) for $0 \leq i, j < m$, $i \neq j$, and $0 \leq k, l < q-1$, $\alpha^k \mathbf{w}_i$ and $\alpha^l \mathbf{w}_j$ differ in at least $n-1$ places. These two constraints on the rows of $\mathbf{W}$ are called the *α-multiplied row-constraints* 1 and 2. The α-multiplied row-constraint 1 implies that each row of $\mathbf{W}$ contains *at most* one 0-component. The α-multiplied row-constraint 2 implies that any two rows of $\mathbf{W}$ differ in at least $n-1$ places.

Dispersing each nonzero entry of $\mathbf{W}$ into an α-multiplied $(q-1) \times (q-1)$ CPM over GF(q) and each 0-entry (if any) of $\mathbf{W}$ into a $(q-1) \times (q-1)$ zero matrix, we obtain the following $m \times n$ *array* of α-multiplied $(q-1) \times (q-1)$ CP and/or zero matrices over GF(q):

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}_{0,0} & \mathbf{A}_{0,1} & \cdots & \mathbf{A}_{0,n-1} \\ \mathbf{A}_{1,0} & \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{m-1,0} & \mathbf{A}_{m-1,1} & \cdots & \mathbf{A}_{m-1,n-1} \end{bmatrix}. \quad (2)$$

The array $\mathbf{H}$ is an $m(q-1) \times n(q-1)$ matrix over GF(q). It follows from the structure of the location-vectors of nonzero elements in GF(q) and the α-multiplied row-constraints 1 and 2 that $\mathbf{H}$, as a matrix over GF(q), satisfies the RC-constraint. The array $\mathbf{H}$ is called the *two dimensional $(q-1)$-fold array dispersion* of $\mathbf{W}$ (or simply array dispersion of $\mathbf{W}$). We also call $\mathbf{H}$ an RC-constrained array. The matrix $\mathbf{W}$ is called the *base matrix* for array dispersion.

For any pair (γ,ρ) of integers with $1 \leq \gamma \leq m$ and $1 \leq \rho \leq n$, let $\mathbf{H}(\gamma, \rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}$. The matrix $\mathbf{H}(\gamma, \rho)$ is a $\gamma(q-1) \times \rho(q-1)$ matrix over GF(q) and also satisfies the RC-constraint. Then, the null space of $\mathbf{H}(\gamma, \rho)$ over GF(q) gives a q-ary QC-LDPC code $\mathcal{C}_{qc}$ of length $\rho(q-1)$ with rate at least $(\rho - \gamma)/\rho$, whose Tanner graph has a girth of at least 6. The above construction gives a class of q-ary QC-LDPC codes.

In Sections IV and VI, two specific RS-based constructions of base matrices that satisfy the α-multiplied row-constrained 1 and 2 will be presented. These base matrices are then dispersed into RC-constrained arrays of α-multiplied CPMs over GF(q) for constructing q-ary QC-LDPC codes.

IV. Construction of Q-ary QC-LDPC Codes by Dispersing a Universal RS Parity-Check Matrix

Consider the Galois field GF(q). Let m be the largest *prime factor* of $q-1$ and $q-1 = cm$. Let α be a primitive element of GF(q) and $\beta = \alpha^c$. Then, β is an element of GF(q) of order m, i.e., m is the smallest integer such that $\beta^m = 1$. The set $\mathcal{G}_m = \{1, \beta, \beta^2, \ldots, \beta^{m-1}\}$ form a *cyclic subgroup* of the *multiplicative group* $\mathcal{G}_{q-1} = \{1, \alpha, \ldots, \alpha^{q-2}\}$ of GF(q). Form the following $m \times m$ matrix over GF(q):

$$\mathbf{W}^{(1)} = \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \\ \vdots \\ \mathbf{w}_{m-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \beta & \beta^2 & \cdots & \beta^{m-1} \\ 1 & \beta^2 & (\beta^2)^2 & \cdots & (\beta^2)^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{m-1} & (\beta^{m-1})^2 & \cdots & (\beta^{m-1})^{m-1} \end{bmatrix}, \quad (3)$$

where the power of β is taken modulo m. For any $1 \leq t \leq m$, any t consecutive rows of $\mathbf{W}^{(1)}$ form a parity-check matrix of a cyclic (m,$m-t$,$t+1$) RS code over GF(q) [7], [10], [15], including the end-around case. Its generator polynomial has t consecutive powers of β as roots. If $q-1$ is a prime, then $m = q-1$ and $\beta = \alpha$, a primitive element of GF(q). In this case, the RS code is a primitive RS code [7]. If $q-1$ is not a prime, the RS code is a non-primitive RS code. Since m is a prime, we can easily prove that $\mathbf{W}^{(1)}$ has the following structural properties: 1) except for the first row, all the entries in a row are different and the they form all the m elements of the cyclic subgroup $\mathcal{G}_m$; 2) except for the first column, all the entries in a column are different and they form all the m elements of $\mathcal{G}_m$; 3) any two rows have only the first entries that are identical (equal to 1) and they differ in all the other $m-1$ positions; 4) any two columns have only the first entries that are identical (equal to 1) and they differ in all the other positions.

Based on the structure of $\mathbf{W}^{(1)}$, we can prove that the matrix $\mathbf{W}^{(1)}$ given by (3) satisfies the α-multiplied row constraints 1 and 2. Hence, $\mathbf{W}^{(1)}$ can be used as a base matrix for array dispersion. The dispersion of $\mathbf{W}^{(1)}$ results in the following RC-constrained $m \times m$ array of α-multiplied $(q-1) \times (q-1)$

CPMs over GF(q):

$$\mathbf{H}^{(1)} = [\mathbf{A}_{i,j}]_{0 \le i < m, 0 \le j < m}. \quad (4)$$

Since all the entries of $\mathbf{W}^{(1)}$ are nonzero, $\mathbf{H}^{(1)}$ contains no zero matrix. The matrix $\mathbf{H}^{(1)}$ is an $m(q-1) \times m(q-1)$ matrix with both column and row weights m.

For any pair (γ,ρ) of integers with $1 \le \gamma, \rho \le m$, let $\mathbf{H}^{(1)}(\gamma, \rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}^{(1)}$. The matrix $\mathbf{H}^{(1)}(\gamma, \rho)$ is a $\gamma(q-1) \times \rho(q-1)$ matrix over GF(q) with column and row weights γ and ρ, respectively. The null space over GF(q) of $\mathbf{H}^{(1)}(\gamma, \rho)$ gives a q-ary QC-LDPC codes $\mathcal{C}_{qc}^{(1)}$. The above construction gives a class of q-ary RS-based QC-LDPC codes.

In the following, an example is given to illustrate the above construction of q-ary QC-LDPC codes based on an RS-based and RC-constrained array of α-multiplied CPMs over GF(q). In this example and other examples given in the rest of this paper, we set q as a power of 2, say $q = 2^s$. In decoding, we use the FFT-QSPA [4] with 50 (or 5) iterations. The number of computations required per iteration of the FFT-QSPA in decoding a q-ary regular LDPC code is in the order of $J\rho q \log q$ [4], denoted $\mathcal{O}(J\rho q \log q)$, where J and ρ are the number and weight of the rows of the parity-check matrix of the code, respectively. For a constructed code, we compute its error performance over the AWGN channel using BPSK signaling, and compare its word error performance with that of a (shortened) RS code of the same length and rate decoded with the HD BM-algorithm and the ASD KV-algorithm. The ASD KV-algorithm for decoding an RS code consists of three steps: *multiplicity assignment*, *interpolation*, and *factorization* [12]. The major computational complexity (70%) to carry out the ASD KV-algorithm comes from the interpolation step and is $\mathcal{O}(\lfloor\lambda\rfloor^4 N^2)$ [16], [17] where N is the length of the code and λ is a complexity parameter [16] that is determined by the interpolation cost of the multiplicity matrix constructed at the multiplicity assignment step. As λ increases, the performance of the KV-algorithm improves and the computational complexity also increases. As λ approaches ∞, the performance of the KV-algorithm reaches its limit. A typical value λ used for performance computation is 4.99 [16], [17].

Example 1. Let (31,2,30) RS code over GF(2^5) be the base code for code construction. The largest prime factor m of $2^5 - 1 = 31$ is 31. Let α be a primitive element of GF(2^5). Then, $c = 1$ and $\beta = \alpha$. Based on (3) and (4), we can construct a 31×31 RC-constrained array $\mathbf{H}^{(1)}$ of 31×31 α-multiplied CPMs over GF(2^5). Set $\gamma = 4$ and $\rho = 28$. Choose a 4×28 subarray $\mathbf{H}^{(1)}(4, 8)$ of $\mathbf{H}^{(1)}$. The matrix $\mathbf{H}^{(1)}(4, 28)$ is a 124×868 matrix over GF(2^5) with column and row weights 4 and 28, respectively. The null space of $\mathbf{H}^{(1)}(4, 28)$ gives a 32-ary RS-based (868,747) QC-LDPC code with rate 0.8606. The symbol and block error performances of this code decoded with iterative decoding using the FFT-QSPA using 50 iterations are shown in Figure 1 which also includes the block error performances of the (868,747,122) shortened RS code over GF(2^{10}) decoded with the HD BM- and ASD KV-algorithms, respectively. At the WER (word-error-rate) of 10^{-5}, the 32-ary (868,747) QC-LDPC code achieves a 1.83 dB coding gain over the (868,747,122) shortened RS code over GF(2^{10}) decoded with the BM-algorithm, while achieves a 1.56 dB and a 1.31 dB coding gains over the shortened RS code decoded using the KV-algorithm with interpolation complexity coefficients 4.99 and infinity, respectively. Also included in Figure 1 is the performance of the 32-ary (868,747) QC-LDPC code with 5 iterations of the FFT-QSPA. We see that even with 5 iterations of FFT-QSPA, the 32-ary (868,747) QC-LDPC code achieves a 1.3 dB and a 1 dB coding gains over the (868,747,122) shortened RS code decoded using the ASD KV-algorithm with interpolation complexity coefficients 4.99 and infinity, respectively.

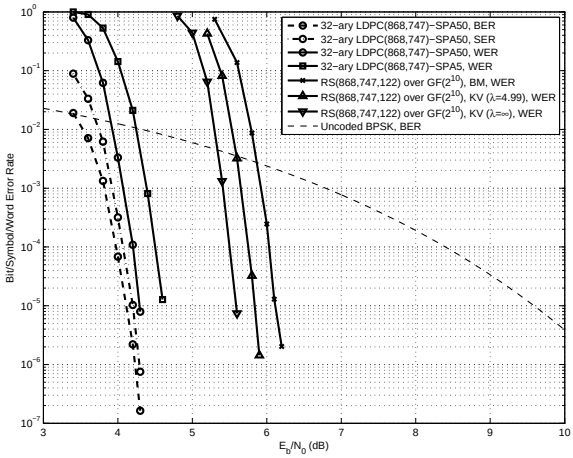

Fig. 1. Error performances of the 32-ary RS-based (868,747) QC-LDPC code and the (868,747,122) shortened RS code over GF(2^{10}) given in Example 1.

The number of computations required to decode the 32-ary RS-based (868,747) QC-LDPC code per iteration of FFT-QSPA is in the order of $124 \times 28 \times 32 \times 5 = 555,520$. Therefore, with 5 and 50 iterations of the FFT-QSPA, the numbers of computations required to decode the 32-ary RS-based (868,747) QC-LDPC code are in the orders of $2,777,600$ and $27,776,000$, respectively. However, the number of computations required to carry out the interpolation step of the KV-algorithm with interpolation complexity coefficient 4.99 in decoding the (868,747,122) shortened RS code over GF(2^{10}) is $192,876,544$ which is much larger than $2,777,600$ and $27,776,000$ required to decode the 32-ary RS-based (868,747) QC-LDPC code with 5 and 50 iterations of the FFT-QSPA, respectively. △△

V. Array Masking

In Section IV, we have presented a class of RS-based RC-constrained arrays of α-multiplied CPMs over finite fields for constructing nonbinary QC-LDPC codes. Although, arrays in this class are highly structured, their constituent CPMs are densely packed. In this section, we present a technique to reduce the density of α-multiplied CPMs of an RC-constrained

array. The reduction of the density of α-multiplied CPMs of an array results in a sparser array whose associated Tanner graph has fewer edges and hence fewer short cycles and probably a larger girth. As a result, the performance of the code given by the *sparser* array can be improved and decoding computational complexity can be reduced.

Let $\mathbf{H}(\gamma,\rho) = [\mathbf{A}_{i,j}]$ be a $\gamma \times \rho$ subarray of an RC-constrained $(q-1)\times(q-1)$ array $\mathbf{H}$ of α-multiplied CPMs over GF(q). Masking $\mathbf{H}(\gamma,\rho)$ is simply to replace a set of α-multiplied CPMs by a set of zero matrices. The masking operation can be mathematically formulated as a special matrix product. Let $\mathbf{Z}(\gamma,\rho) = [z_{i,j}]$ be a $\gamma \times \rho$ matrix over GF(2). Define the following product: $\mathbf{M}(\gamma,\rho) = \mathbf{Z}(\gamma,\rho) \otimes \mathbf{H}(\gamma,\rho) = [z_{i,j}\mathbf{A}_{i,j}]$, where $z_{i,j}\mathbf{A}_{i,j} = \mathbf{A}_{i,j}$ for $z_{i,j} = 1$ and $z_{i,j}\mathbf{A}_{i,j} = \mathbf{O}$ (a $(q-1)\times(q-1)$ zero matrix) for $z_{i,j} = 0$. In this matrix product operation, a set of α-multiplied CPMs is masked by the 0-entries of $\mathbf{Z}(\gamma,\rho)$. We call $\mathbf{Z}(\gamma,\rho)$ the *masking matrix*, $\mathbf{H}(\gamma,\rho)$ the *base array*, and $\mathbf{M}(\gamma,\rho)$ the *masked array*. The distribution of the α-multiplied CPMs in the masked array $\mathbf{M}(\gamma,\rho)$ is identical to the distribution of 1-entries in the masking matrix $\mathbf{Z}(\gamma,\rho)$. Since the base array $\mathbf{H}(\gamma,\rho)$ satisfies the RC-constraint, it is clear that the masked array $\mathbf{M}(\gamma,\rho)$ also satisfies the RC-constraint, regardless of the masking matrix. Hence, the associated Tanner graph of $\mathbf{M}(\gamma,\rho)$ has a girth of at least 6. If the girth of the associated Tanner graph of the masking matrix $\mathbf{Z}(\gamma,\rho)$ has a girth $\sigma > 6$, the girth of the associated Tanner graph of the masked array $\mathbf{M}(\gamma,\rho)$ is at least σ. The concept of masking was recently introduced in [14], [18] for constructing binary LDPC codes.

The null space of $\mathbf{M}(\gamma,\rho)$ over GF(q) gives a q-ary QC-LDPC code $\mathcal{C}_{mas,qc}$ which is different from the code given by the null space of the base array $\mathbf{H}(\gamma,\rho)$. The error performance of $\mathcal{C}_{mas,qc}$ depends on the distribution of 1-entries of the masking matrix $\mathbf{Z}(\gamma,\rho)$. How to design masking matrices that result in good QC-LDPC codes is an interesting and challenging problem. Masking matrices can be constructed by computer search or algebraically [14], [18]. A special type of masking matrices is the circular type. A circular masking matrix consists of a row of k ($k \geq 1$) sparse circulants over GF(2) in the following form: $\mathbf{Z}(\gamma, k\gamma) = [\mathbf{G}_0\ \mathbf{G}_1 \cdots \mathbf{G}_{k-1}]$, where for $0 \leq j < k$, $\mathbf{G}_j$ is a $\gamma\times\gamma$ circulant with both column and row weights w_j. If $w_1 = w_2 = \cdots = w_k = w$, $\mathbf{Z}(\gamma, k\gamma)$ is a regular masking matrix with column and row weights w and kw, respectively. Otherwise, $\mathbf{Z}(\gamma, k\gamma)$ is irregular and has multiple column weights and constant row weight $w_1 + w_2 + \cdots + w_k$. A γ-tuple $\mathbf{g}$ over GF(2) is said to be *primitive* if $\mathbf{g}$ and its $\gamma - 1$ cyclic-shifts are all different. For $0 \leq j < k$, each circulant $\mathbf{G}_j$ is formed by a primitive γ-tuple $\mathbf{g}_j$ over GF(2) with weight w_j as the first row (or first column) and its $\gamma - 1$ right cyclic-shifts (or downward cyclic shifts) as the other $\gamma - 1$ rows (or other $\gamma - 1$ columns). The primitive γ-tuple $\mathbf{g}_j$ over GF(2) is called the *generator* of jth circulant $\mathbf{G}_j$. In computer search, it is desired to find k generators such that the Tanner graph of $\mathbf{Z}(\gamma, k\gamma)$ has a girth as large as possible and the number of short cycles is as small as possible.

Example 2. Consider the 31×31 array $\mathbf{H}^{(1)}$ of α-multiplied 31×31 CPMs constructed in Example 1 based on the universal RS parity-check matrix over GF(2^5). Suppose we choose $\gamma = 14$ and $\rho = 28$. Take a 14×28 subarray $\mathbf{H}^{(1)}(14, 28)$ from $\mathbf{H}^{(1)}$. Construct a 14×28 circular masking matrix $\mathbf{Z}(14, 28)$ that consists of two 14×14 circulants, $\mathbf{G}_1$ and $\mathbf{G}_2$, in a row, each having both column and row weights 3. By computer search, we find two primitive generators of the two circulants in $\mathbf{Z}(14, 28)$, which are $\mathbf{g}_1 = (00001000010001)$ and $\mathbf{g}_2 = (00001010000100)$, respectively. Masking $\mathbf{H}^{(1)}(14, 28)$ with $\mathbf{Z}(14, 28)$, we obtain a 14×28 masked array $\mathbf{M}^{(1)}(14, 28) = \mathbf{Z}(14, 28) \otimes \mathbf{H}^{(1)}(14, 28)$ which is a 434×868 matrix over GF(2^5) with column and row weights 3 and 6, respectively. The null space of $\mathbf{M}^{(1)}(14, 28)$ gives a 32-ary (868,434) QC-LDPC code with rate 0.5. The bit, symbol, and word error performances of this code over the AWGN channel with iterative decoding using the FFT-QSPA (50 iterations) are shown in Figure 2 which also includes the word error performances of the (868,434,435) shortened RS code over GF(2^{10}) decoded with the HD BM-algorithm and the ASD KV-algorithm with interpolation complexity coefficients 4.99 and infinity, respectively. At the WER of 10^{-5}, the 32-ary (868,434) QC-LDPC code achieves a 3.98 dB coding gain over the (868,434,435) shortened RS code decoded with HD BM-algorithm, while achieves a 3.39 and a 2.90 dB coding gains over the shortened RS code decoded using the ASD KV-algorithm with interpolation complexity coefficients 4.99 and infinity, respectively. The word error performance of the 32-ary (868,434) QC-LDPC code decoded with 10 iterations of the FFT-QSPA is also included in Figure 2. We see that even with 10 iterations, the 32-ary (868,434) achieves a 3.03 dB coding gain over the shortened RS code decoded using the ASD KV-algorithm with interpolation complexity coefficient 4.99.

The numbers of computations required to decode the 32-ary (868,434) QC-LDPC code with the FFT-QSPA using 10 and 50 iterations are in the orders of $4,166,400$ and $20,832,000$, respectively. However, the required number of computations to carry out the interpolation step of the KV-algorithm with interpolation complexity coefficient 4.99 in decoding the (868,434,435) shortened RS code is in the order of $192,876,544$ which is much larger than $4,166,400$ and $20,832,000$, the orders of numbers of computations required to decode the 32-ary (868,434) QC-LDPC code using the FFT-QSPA with 10 and 50 iterations, respectively. △△

VI. Construction of Q-ary QC-LDPC Codes Based on RS Codes with Two Information Symbols

Consider a (q − 1,2,q − 2) RS code $\mathcal{C}_b$ over GF(q) with two information symbols. Let α be a primitive element of GF(q). The generator polynomial of this RS code $\mathcal{C}_b$ has $\alpha, \alpha^2, \ldots, \alpha^{q-3}$ as roots. This RS code has two nonzero weights, $q - 1$ and $q - 2$. Therefore, the minimum weight of this code is $q - 2$. There are $(q - 1)^2$ code words of weight $q - 2$. It can be easily proved that $(1, 1, \ldots, 1)$ and $(\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{q-2})$ are two linearly independent code words

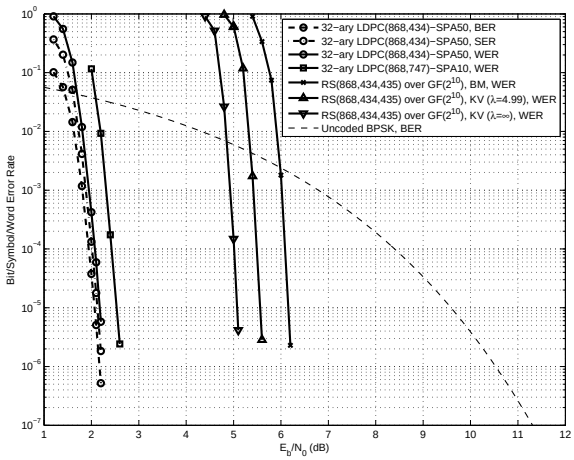

Fig. 2. Error performances of the 32-ary (868,434) QC-LDPC code and the (868,434,435) shortened RS code given in Example 2.

of weight $q-1$ in $\mathcal{C}_b$. Then, $\mathbf{w}_0 = (\alpha^0-1, \alpha-1, \ldots, \alpha^{q-2}-1)$ is a minimum weight code word in $\mathcal{C}_b$ whose first component is equal to 0 and all the other $q-2$ components are nonzero. Form the following $(q-1)\times(q-1)$ matrix $\mathbf{W}^{(2)}$ over GF(q) with $\mathbf{w}_0$ and its right cyclic-shifts $\mathbf{w}_1, \ldots, \mathbf{w}_{q-2}$ as rows:

$$\mathbf{W}^{(2)} = \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{q-2} \end{bmatrix} = \begin{bmatrix} \alpha^0-1 & \alpha-1 & \cdots & \alpha^{q-2}-1 \\ \alpha^{q-2}-1 & \alpha^0-1 & \cdots & \alpha^{q-3}-1 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha-1 & \alpha^2-1 & \cdots & \alpha^0-1 \end{bmatrix}. \quad (5)$$

The matrix $\mathbf{W}^{(2)}$ has the following structural properties: 1) any two rows (or two columns) differ in all positions; 2) all the $q-1$ elements in each row (or each column) are distinct elements in GF(q); 3) each row (or each column) contains one and only one 0-element; 4) all the 0-elements lie on the main diagonal of $\mathbf{W}^{(2)}$. Note that the rows of $\mathbf{W}^{(2)}$ are minimum weight codewords of the $(q-1,2,q-2)$ RS-based code $\mathcal{C}_b$. It can be easily proved that $\mathbf{W}^{(2)}$ satisfies the α-multiplied row-constraints 1 and 2.

The two-dimensional $(q-1)$-fold array dispersion of matrix $\mathbf{W}^{(2)}$ given by (5) results in the following RC-constrained $(q-1)\times(q-1)$ array of α-multiplied $(q-1)\times(q-1)$ CP and zero matrices over GF(q):

$$\mathbf{H}^{(2)} = \begin{bmatrix} \mathbf{O} & \mathbf{A}_{0,1} & \cdots & \mathbf{A}_{0,q-2} \\ \mathbf{A}_{0,q-2} & \mathbf{O} & \cdots & \mathbf{A}_{0,q-3} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{0,1} & \mathbf{A}_{0,2} & \cdots & \mathbf{O} \end{bmatrix}, \quad (6)$$

Note that the zero submatrices of $\mathbf{H}^{(2)}$ lie on the main diagonal of $\mathbf{H}^{(2)}$. Each row of submatrices of $\mathbf{H}^{(2)}$ is a right cyclic-shift of the row above it and the first row is the right cyclic-shift of the last row. The matrix $\mathbf{H}^{(2)}$ is a $(q-1)^2\times(q-1)^2$ matrix over GF(q) with both column and row weights $q-2$ for which each row corresponds to a minimum weight code word of the RS code $\mathcal{C}_b$.

For any pair (γ,ρ) of integers with $1 \le \gamma, \rho \le q-1$, let $\mathbf{H}^{(2)}(\gamma,\rho)$ be a $\gamma\times\rho$ subarray of $\mathbf{H}^{(2)}$. Then, $\mathbf{H}^{(2)}(\gamma,\rho)$ is $\gamma(q-1)\times\rho(q-1)$ matrix over GF(q). The null space over GF(q) of $\mathbf{H}^{(2)}(\gamma,\rho)$ gives a q-ary regular RS-based QC-LDPC code $\mathcal{C}_{qc}^{(2)}$ of length $\rho(q-1)$ with rate at least $(\rho-\gamma)/\rho$, whose Tanner graph has a girth of at least 6. For a given $(q-1,2,q-2)$ RS code over GF(q), a family of structurally compatible q-ary RS-based QC-LDPC codes of various lengths and rates can be constructed.

Example 3. Let the (63,2,62) RS code over GF(2^6) be the base code for code construction. Based on $\mathcal{C}_b$, (5), (6), and using array dispersion, we can construct a 63×63 RC-constrained array $\mathbf{H}^{(2)}$ of α-multiplied 63×63 CPMs over GF(2^6). Choose $\gamma = 8$ and $\rho = 16$. Take an 8×16 subarray $\mathbf{H}^{(2)}(8,16)$ from $\mathbf{H}^{(2)}$, avoiding zero matrices. We use $\mathbf{H}^{(2)}(8,16)$ as the base array for masking. Construct an 8×16 circular masking matrix $\mathbf{Z}(8,16)$ that consists of two 8×8 circulants, $\mathbf{G}_0$ and $\mathbf{G}_1$, in a row, each having both column and row weights 3. By computer search, we find two primitive generators of the two circulants in $\mathbf{Z}(8,16)$, which are $\mathbf{g}_1 = (01011000)$ and $\mathbf{g}_2 = (00101010)$, respectively. Masking $\mathbf{H}^{(2)}(8,16)$ with $\mathbf{Z}(8,16)$, we obtain an 8×16 masked array $\mathbf{M}^{(2)}(8,16) = \mathbf{Z}(8,16)\otimes\mathbf{H}^{(2)}(8,16)$ which is a 504×1008 matrix over GF(2^6) with column and row weights 3 and 6, respectively. The null space of $\mathbf{M}^{(2)}(8,16)$ gives a 64-ary (1008,504) QC-LDPC code over GF(2^6) with rate 0.5. The bit, symbol, and word error performances of this code over the AWGN channel with iterative decoding using the FFT-QSPA (5 and 50 iterations) are shown in Figure 3, which also includes the word error performances of the (1008,504,505) shortened RS code over GF(2^{10}) decoded with the HD BM-algorithm and the ASD KV-algorithm with interpolation complexity coefficients 4.99 and ∞, respectively. At a WER of 10^{-5}, the 64-ary (1008,504) QC-LDPC code achieves a 4 dB coding gain over the (1008,504,505) shortened RS code decoded with the HD BM-algorithm, while achieves a 3.3 dB and a 2.8 dB coding gains over the shortened RS code decoded with the ASD KV-algorithm. With 5 iterations of FFT-QSPA, the 64-ary (1008,504) code has a 2.3 dB coding gain over the (1008,504,505) shortened RS code decoded using the ASD KV-algorithm with interpolation complexity coefficient 4.99.

The numbers of computations required in decoding the 64-ary (1008,504) QC-LDPC code with 5 and 50 iterations of the FFT-QSPA are $5,806,080$ and $58,060,800$, respectively. However, for decoding the (1008,504,505) shortened RS code over GF(2^{10}) using the ASD KV-algorithm with interpolation coefficient 4.99, the number of computations required to carry out the interpolation step is in the order of $260,112,384!$ △△

Example 4. In this example, we construct a high rate code based on the 63×63 array of α-multiplied 63×63 CPMs constructed in Example 3. Choose $\gamma = 4$ and $\rho = 32$. Take a 4×32 subarray $\mathbf{H}^{(2)}(4,32)$ from $\mathbf{H}^{(2)}$ that does not contain zero submatrices on the main diagonal of $\mathbf{H}^{(2)}$. The array $\mathbf{H}^{(2)}(4,32)$ is a 252×2016 matrix over GF(2^6) with column and row weights 4 and 32, respectively. The null space over

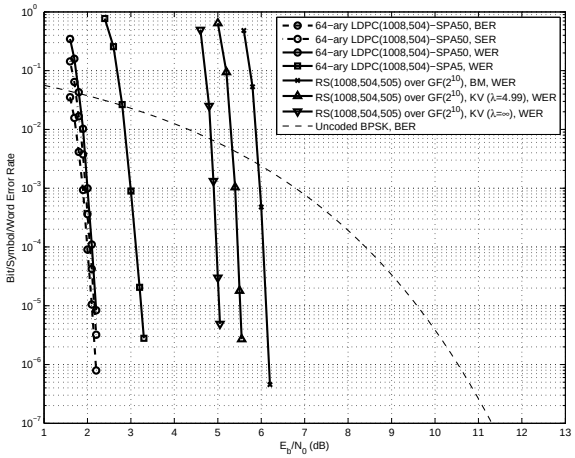

Fig. 3. Error performances of the 64-ary (1008,504) QC-LDPC code and the (1008,504,505) shortened RS code given in Example 3.

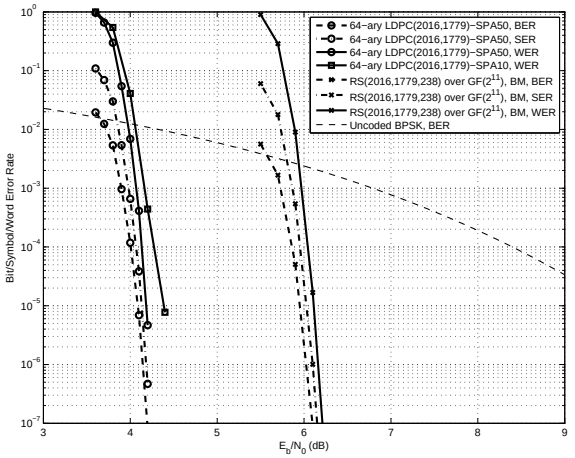

Fig. 4. Error performances of the 64-ary (2016,1779) QC-LDPC code and the (2016,1779,238) shortened RS code given in Example 4.

GF(2^6) of $\mathbf{H}^{(2)}(4,8)$ gives a 64-ary (2016,1779) QC-LDPC code with rate 0.8824. The bit, symbol, and word error performances of this code decoded with the FFT-QSPA are shown in Figure 4 which also includes the bit, symbol, and word error performances of the (2016,1779,238) shortened RS code over GF(2^{11}) decoded with the HD BM-algorithm. At the SER of 10^{-6} (or WER of 10^{-5}), the 64-ary (2016,1779) QC-LDPC code achieves a 2 dB coding gain over the (2016,1779,238) shortened RS code over GF(2^{11}).

The performance of the (2016,1779,238) shortened RS code over GF(2^{11}) with the ASD KV-algorithm is not available because the number of computations required to carry out the interpolation step of the KV-algorithm is simply too large, $1,040,449,536$. The numbers of computations required for 10 and 50 iterations in decoding the 64-ary (2016,1779) QC-LDPC codes with the FFT-QSPA are in the orders of $30,965,760$ and $154,828,800$, respectively, which are much smaller than $1,040,449,536$. △△

VII. Construction by Array Dispersion

A subarray of an RC-constrained array $\mathbf{H}$ of α-multiplied CPMs constructed in the previous sections (either $\mathbf{H}^{(1)}$ given by (4) or $\mathbf{H}^{(2)}$ given by (6)) can be dispersed into a larger array with a lower density to construct new q-ary QC-LDPC codes. In this section, we present an array dispersion technique to construct a large class of q-ary QC-LDPC. Codes constructed by this array dispersion technique not only perform well over the AWGN channel and some fading channels but also have good *erasure-burst* correction capabilities.

For $3 \leq t < q$ and $1 \leq k$, let $\mathbf{H}(t, kt)$ be a $t \times kt$ subarray of the RC-constrained array $\mathbf{H}$ of α-multiplied $(q-1) \times (q-1)$ CPMs over GF(q) constructed in Section VI. Since $\mathbf{H}$ is a $(q-1) \times (q-1)$ array and $\mathbf{H}(t, kt)$ is a subarray of $\mathbf{H}$, the parameters k and t must satisfy the constraint $kt \leq q-1$. We assume that $\mathbf{H}(t, kt)$ does not contain any zero matrix. Divide $\mathbf{H}(t, kt)$ into k $t \times t$ subarrays, $\mathbf{H}_1(t,t), \mathbf{H}_2(t,t), \ldots, \mathbf{H}_k(t,t)$, such that

$$\mathbf{H}(t, kt) = [\mathbf{H}_1(t,t)\ \mathbf{H}_2(t,t)\ \ldots\ \mathbf{H}_k(t,t)], \tag{7}$$

where for $1 \leq j \leq k$, the jth $t \times t$ subarray $\mathbf{H}_j(t,t)$ is expressed in the following form:

$$\mathbf{H}_j(t,t) = \begin{bmatrix} \mathbf{A}_{0,0}^{(j)} & \mathbf{A}_{0,1}^{(j)} & \cdots & \mathbf{A}_{0,t-1}^{(j)} \\ \mathbf{A}_{1,0}^{(j)} & \mathbf{A}_{1,1}^{(j)} & \cdots & \mathbf{A}_{1,t-1}^{(j)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{t-1,0}^{(j)} & \mathbf{A}_{t-1,1}^{(j)} & \cdots & \mathbf{A}_{t-1,t-1}^{(j)} \end{bmatrix}, \tag{8}$$

where each $\mathbf{A}_{i,l}^{(j)}$ with $0 \leq i, l < t$ is an α-multiplied $(q-1) \times (q-1)$ CPM over GF(q). Since $\mathbf{H}(t, kt)$ satisfies the RC-constraint, each subarray $\mathbf{H}_j(t,t)$ of $\mathbf{H}(t, kt)$ also satisfies the RC-constraint.

Cut $\mathbf{H}_j(t,t)$ into two *triangles*, *upper* and *lower triangles*, along its main diagonal, where the lower triangle contains the α-multiplied CPMs on the main diagonal of $\mathbf{H}_j(t,t)$. Form two $t \times t$ arrays of α-multiplied CP and zero matrices as follows:

$$\mathbf{H}_{j,U}(t,t) = \begin{bmatrix} \mathbf{O} & \mathbf{A}_{0,1}^{(j)} & \mathbf{A}_{0,2}^{(j)} & \cdots & \mathbf{A}_{0,t-1}^{(j)} \\ \mathbf{O} & \mathbf{O} & \mathbf{A}_{1,2}^{(j)} & \cdots & \mathbf{A}_{1,t-1}^{(j)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{A}_{t-2,t-1}^{(j)} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix}, \tag{9}$$

and

$$\mathbf{H}_{j,L}(t,t) = \begin{bmatrix} \mathbf{A}_{0,0}^{(j)} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{A}_{1,0}^{(j)} & \mathbf{A}_{1,1}^{(j)} & \mathbf{O} & \cdots & \mathbf{O} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{t-2,0}^{(j)} & \mathbf{A}_{t-2,1}^{(j)} & \mathbf{A}_{t-2,2}^{(j)} & \cdots & \mathbf{O} \\ \mathbf{A}_{t-1,0}^{(j)} & \mathbf{A}_{t-1,1}^{(j)} & \mathbf{A}_{t-1,2}^{(j)} & \cdots & \mathbf{A}_{t-1,t-1}^{(j)} \end{bmatrix}, \tag{10}$$

where $\mathbf{O}$ is a $(q-1)\times(q-1)$ zero matrix. From (9), we see that the upper triangle of the $t\times t$ array $\mathbf{H}_{j,U}(t,t)$ above the main diagonal line is identical to the upper triangle of $\mathbf{H}_j(t,t)$ above the main diagonal line, and the rest of the submatrices in $\mathbf{H}_{j,U}(t,t)$ are zero matrices. From (10), we see that the lower triangle of $\mathbf{H}_{j,L}(t,t)$ including the submatrices on the main diagonal line is identical to that of $\mathbf{H}_j(t,t)$, and the submatrices above the main diagonal line are zero matrices. Since $\mathbf{H}_j(t,t)$ satisfies the RC-constraint, it is clear that $\mathbf{H}_{j,U}(t,t)$ and $\mathbf{H}_{j,L}(t,t)$ also satisfy the RC-constraint.

For $1\le j\le k$ and $2\le l$, we form the following $l\times l$ array of $t\times t$ subarrays:

$$\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)= \begin{bmatrix} \mathbf{H}_{j,L}(t,t) & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{H}_{j,U}(t,t) \\ \mathbf{H}_{j,U}(t,t) & \mathbf{H}_{j,L}(t,t) & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{H}_{j,U}(t,t) & \mathbf{H}_{j,L}(t,t) & \cdots & \mathbf{O} & \mathbf{O} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{H}_{j,U}(t,t) & \mathbf{H}_{j,L}(t,t) \end{bmatrix}, \tag{11}$$

where $\mathbf{O}$ is a $t\times t$ array of $(q-1)\times(q-1)$ zero matrices. From (11), we see that each row of $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ is a right cyclic-shift of the row above it and the first row is the right cyclic-shift of the last row. Also, the $t\times t$ subarrays, $\mathbf{H}_{j,L}(t,t)$ and $\mathbf{H}_{j,U}(t,t)$, in $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ are separated by a *span* of $l-2$ $t\times t$ zero subarrays, including the *end-around* case, with $\mathbf{H}_{j,L}(t,t)$ as the starting subarray and $\mathbf{H}_{j,U}(t,t)$ as the ending subarray. From (9), (10), and (11), we readily see that all the α-multiplied CPMs in each row (or each column) of $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ together form the jth subarray $\mathbf{H}_j(t,t)$ of the $t\times kt$ array $\mathbf{H}(t,kt)$ given by (8). The array $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ is called the *l-fold array dispersion* of $\mathbf{H}_j(t,t)$, where the subscripts, "*l-f*" and "*$disp$*" of $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ stand for "l-fold" and "dispersion", respectively. The array $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ is an $lt(q-1)\times lt(q-1)$ matrix over GF(q) with both column and row weights t. Since $\mathbf{H}_j(t,t)$ satisfies the RC-constraint, it follows from (11) that the l-fold array dispersion $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ of $\mathbf{H}_j(t,t)$ also satisfies the RC-constraint. Since any two subarrays in $\mathbf{H}(t,kt)$ given by (7) jointly satisfy the RC-constraint, their corresponding l-fold array dispersions jointly satisfy the RC-constraint.

Now, we view $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ as an $lt\times lt$ array of α-multiplied $(q-1)\times(q-1)$ CP and zero matrices. From the structures of $\mathbf{H}_{j,U}(t,t)$, $\mathbf{H}_{j,L}(t,t)$ and $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ given by (9), (10), and (11), respectively, we readily see that each row of $\mathbf{H}_{j,l\text{-}f,disp}(lt,lt)$ contains a single span of $(l-1)t$ zero matrices of size $(q-1)\times(q-1)$ between two α-multiplied CPMs, including the end-around case. For $0\le s<t$, replacing the s α-multiplied CPMs right after the single span of zero matrices by s zero matrices, we obtain a new $lt\times lt$ array $\mathbf{H}_{j,l\text{-}f,disp,s}(lt,lt)$ of α-multiplied CP and zero matrices. The array $\mathbf{H}_{j,l\text{-}f,disp,s}(lt,lt)$ is called the *s-masked* and *l-fold array dispersion* of $\mathbf{H}_j(t,t)$. Each row of $\mathbf{H}_{j,l\text{-}f,disp,s}(lt,lt)$ contains a single span of $(l-1)t+s$ zero matrices of size $(q-1)\times(q-1)$.

Replacing each $t\times t$ subarray in the $t\times kt$ array $\mathbf{H}(t,kt)$ of (7) by its s-masked l-fold array dispersion, we obtain the following $lt\times klt$ array of α-multiplied $(q-1)\times(q-1)$ CP and zero matrices over GF(q):

$$\mathbf{H}_{l\text{-}f,disp,s}(lt,lkt)= [\mathbf{H}_{1,l\text{-}f,disp,s}(lt,lt)\ \mathbf{H}_{2,l\text{-}f,disp,s}(lt,lt)\cdots\mathbf{H}_{k,l\text{-}f,disp,s}(lt,lt)]. \tag{12}$$

$\mathbf{H}_{l\text{-}f,disp,s}(lt,klt)$ is referred to as the *s-masked* and *l-fold dispersion* of the array $\mathbf{H}(t,kt)$ given by (7). As an $lt\times klt$ array of α-multiplied CP and zero matrices, each row of $\mathbf{H}_{l\text{-}f,disp,s}(lt,klt)$ contains k spans of zero matrices, each consisting of $(l-1)t+s$ zero matrices of size $(q-1)\times(q-1)$, including the end-around case. The array $\mathbf{H}_{l\text{-}f,disp,s}(lt,klt)$ is an $lt(q-1)\times klt(q-1)$ matrix over GF(q) with column and row weights, $t-s$ and $k(t-s)$, respectively. It satisfies the RC-constraint.

The null space over GF(q) of $\mathbf{H}_{l\text{-}f,disp,s}(lt,klt)$ gives a $(t-s,k(t-s))$-regular q-ary QC-LDPC code $\mathcal{C}_{l\text{-}f,disp,s}$ of length $klt(q-1)$ with rate at least $(k-1)/k$, whose Tanner graph has a girth of at least 6. The above construction by multi-fold array dispersion gives a large class of non-binary QC-LDPC codes. This multi-fold array dispersion allows us to construct long codes of various rates from small non-binary fields. There are five degrees of freedoms in code construction, namely q, k, l, s, and t. The parameters k and t are limited by q, i.e., $kt\le q-1$. To avoid column weight of $\mathbf{H}_{l\text{-}f,disp,s}(kt,klt)$ less than 3, we need to choose s such that $t-s\ge 3$. However, there is no limitation on l. Therefore, for given q, k, s, and t, we can construct very long codes over the same field GF(q) by varying l. This means that we can construct long QC-LDPC codes over small non-binary fields.

Example 5. Based on the (63,2,62) RS code over GF(2^6), (5), and (6), we first construct a 63×63 array $\mathbf{H}^{(2)}$ of α-multiplied 63×63 CPMs. Set $k=2$, $l=3$, $k=5$, and $s=1$. Take a 5×10 subarray $\mathbf{H}^{(2)}(5,10)$ from $\mathbf{H}^{(2)}$ (avoiding zero matrices on the main diagonal of $\mathbf{H}^{(2)}$). The 1-masked and 3-fold array dispersion of $\mathbf{H}^{(2)}(5,10)$ gives a 15×30 array $\mathbf{H}^{(2)}_{3\text{-}f,disp,1}(15,30)$ of α-multiplied 63×63 CP and zero matrices over GF(2^6). It is a 945×1890 matrix over GF(2^6) with column and row weights 4 and 8, respectively. The null space over GF(2^6) of this matrix gives a 64-ary (4,8)-regular (1890,946) QC-LDPC code with rate 0.5005. The bit, symbol, and word error performances of the 64-ary (1890,946) QC-LDPC code decoded using the FFT-QSPA with 50 iterations are shown in Figure 5, which also include the word error performance of the (1890,946,945) shortened RS code over GF(2^{11}). At the WER of 10^{-4}, the (1890,946,945) shortened RS code decoded with the FFT-QSPA achieves a 3.1 dB gain over the (1890,946,945) shortened RS code decoded with the HD BM-algorithm, while achieves a 2.5 dB and a 2 dB coding gains over the shortened RS code decoded using the KV-algorithm with interpolation complexity coefficients 4.99 and infinity. Also included in Figure 5 is the word error performance of the 64-ary (1890,946) QC-LDPC code with 5 iterations of the FFT-QSPA. We see that, even with 5 iterations, the 64-ary (1890,946) QC-LDPC code achieves

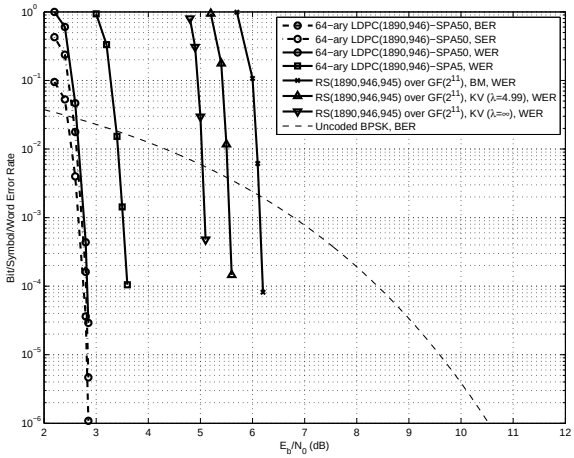

Fig. 5. Error performances of the 64-ary (1890,946) QC-LDPC code decoded with the FFT-QSPA and the word error performances of the (1890,946,945) shortened RS code decoded with the BM- and KV-algorithms given in Example 5.

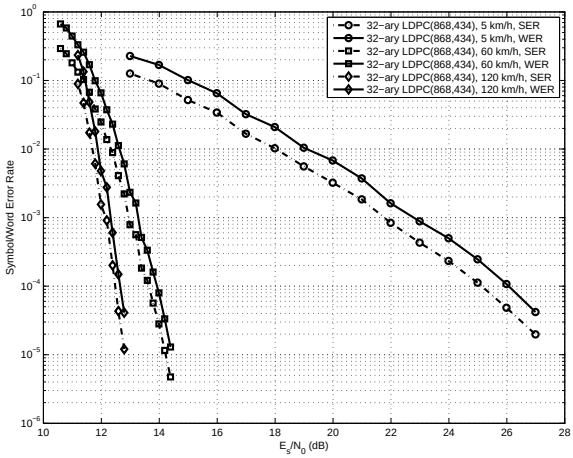

Fig. 6. Error performances of the 32-ary (868,434) QC-LDPC code decoded with the FFT-QSPA with CSI over the uncorrelated Rayleigh fading channel (32-QAM) given in Example 1.

a 2 dB coding gain over its corresponding shortened RS code decoded using the ASD KV-algorithm with interpolation complexity coefficient 4.99.

The numbers of computations required in decoding the 64-ary (1890,946) QC-LDPC code with the FFT-QSPA using 5 and 50 iterations are in the orders of $14,515,200$ and $145,152,000$, respectively. However, decoding the (1890,956,945) shortened RS code with the KV-algorithm, the number of computations required to carry out the interpolation step is in the order of $914,457,600$! △△

VIII. Applications to Fading Channels

Some communication environments are characterized by multipath channels. A multipath channel has more than one path from the transmitter to the receiver. Such multiple paths may be caused by atmospheric reflection or refraction, fractions from buildings or other obstacles. Signal components arriving via different paths may add destructively, resulting in a phenomenon called fading. A typical communication environment characterized by a multipath fading channel is a wireless communication system. Rayleigh fading is widely used for modeling a wireless channel. In [19]–[21], binary LDPC codes have been shown to perform well over Rayleigh fading channels with BPSK signaling.

In following, we use some q-ary QC-LDPC codes constructed in early sections to show that they perform well over a correlated fading channel. There are different approaches to modeling a correlated fading channel. In our performance computation, we use an improved Jakes' channel model proposed in [22]. We apply the codes constructed in Examples 2 and 5 to mobile communications. We assume that the carrier frequency is 900 MHz and the source rate is 9.6 kb/s. Three typical speeds are considered: 5 km/h, 60 km/h, and 120 km/h. The Doppler shifts are listed in Table I. We also

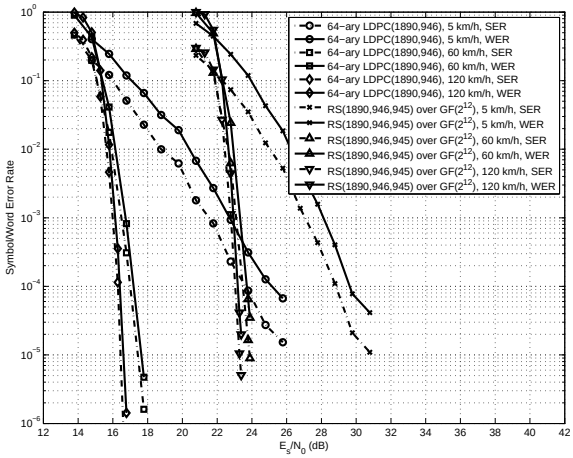

Fig. 7. Error performances of the 64-ary (1890,946) QC-LDPC code decoded with the FFT-QSPA with CSI over the uncorrelated Rayleigh fading channel (64-QAM) given in Example 5.

assume perfect channel side information (CSI) at the receiver. The performances of the 32-ary (868,434) QC-LDPC code given in Example 2 and the 64-ary (1890,946) QC-LDPC code given in Example 5 are shown in Figures 6 and 7, respectively, decoded with the FFT-QSPA with 50 iterations. Also included in these two figures are the performance of their corresponding shortened RS codes decoded with the HD BM-algorithm. We see that two non-binary QC-LDPC codes significantly outperform their corresponding shortened RS codes decoded with the HD BM-algorithm. Of course, the performance improvements are at the expense of much larger decoding computational complexities.

TABLE I
DOPPLER SHIFTS

Q-ary LDPC Codes	Mobile Speed v (km/h)	Maximum Doppler Frequency f_D (Hz)	Symbol Duration T_s (s)	Normalized Doppler $f_D \cdot T_s$
32-ary (868,434)	5	4.170	5.208×10^{-5}	2.172×10^{-4}
32-ary (868,434)	60	50.035	5.208×10^{-5}	2.606×10^{-3}
32-ary (868,434)	120	100.069	5.208×10^{-5}	5.212×10^{-3}
64-ary (1890,946)	5	4.170	5.214×10^{-5}	2.174×10^{-4}
64-ary (1890,946)	60	50.035	5.214×10^{-5}	2.609×10^{-3}
64-ary (1890,946)	120	100.069	5.214×10^{-5}	5.217×10^{-3}
16-ary (960,491)	5	4.170	5.328×10^{-5}	2.221×10^{-4}
16-ary (960,491)	60	50.035	5.328×10^{-5}	2.666×10^{-3}
16-ary (960,491)	120	100.069	5.328×10^{-5}	5.331×10^{-3}

IX. CORRECTION OF BURSTS OF SYMBOL ERASURES

In [13] and [14], binary QC-LDPC codes for correction of bursts of erasures were constructed in terms of the *zero-covering spans* of the parity-check matrices of the codes. If the length of the zero-covering span of the parity-check matrix of a binary LDPC is λ, then the code is capable of correcting any erasure-burst of length up to at least $\lambda + 1$ bits.

Based on the structure and length of the spans of zero matrices in the rows of the array $\mathbf{H}_{l-f,disp,s}(lt, lkt)$ given by (12), it can be proved that the length λ of the zero-covering-span of $\mathbf{H}_{l-f,disp,s}$, as a $lt(q-1) \times klt(q-1)$ matrix over GF(q), is lower bounded by $[(l-1)t+s](q-1)$. Consequently, the q-ary QC-LDPC code $\mathcal{C}_{l\text{-}f,disp,s}$ given by the null space of the $lt(q-1) \times klt(q-1)$ matrix $\mathbf{H}_{l\text{-}f,disp,s}(lt, klt)$ over GF(q) is capable of correcting any erasure-burst of length up to $[(l-1)t+s](q-1)+1$ symbols. Since the row rank of $\mathbf{H}_{l\text{-}f,disp,s}(lt, klt)$ is at most $lt(q-1)$. The erasure-burst correction efficiency η (defined as the ratio of the erasure-burst correction capability of a code to the number of parity-check symbols of the code) is at least

$$\eta \geq \frac{[(l-1)t+s](q-1)+1}{lt(q-1)},$$

which is approximately equal to $[(l-1)t+s]/lt$ for large q, t, and l. For large l, t, and small $t-s$, the erasure-burst correction efficiency η of $\mathcal{C}_{l\text{-}f,disp,s}$ is approaching to one.

Consider the 64-ary (1890,946) QC-LDPC code given in Example 5. Its parity-check matrix has a zero-covering span of length at least 693 and hence the code is capable of correcting any erasure-burst of length up to at least 694 symbols. The burst-erasure correction efficiency of the code is at least 0.735.

Example 6. Suppose we construct a 15×15 RC-constrained array $\mathbf{H}^{(2)}$ based on the (15,2,14) RS code over GF(2^4). Set $k=2$, $l=8$, $s=0$, and $t=4$. Take a 4×8 subarray $\mathbf{H}^{(2)}(4,8)$ from $\mathbf{H}^{(2)}$. The 0-masked and 8-fold dispersion of $\mathbf{H}^{(2)}(4,8)$ gives a 32×64 array $\mathbf{H}^{(2)}_{8\text{-}f,disp,0}(32,64)$ of α-multiplied 15×15 CP and zero matrices. It is a 480×960 matrix over GF(2^4) with column and row weights 4 and 8, respectively, whose zero-covering span has a length of at least 420. The null space of GF(2^4) of this matrix gives a 16-ary (960,491) QC-LDPC code with rate 0.5115. This code is capable of correcting any erasure-burst of length up to at least 421 symbols. The erasure-burst correction efficiency of this code is at least 0.8770. This code also performs well over the AWGN channel and the mobile fading channel specified by Table 1 as shown in Figures 8 and 9. △△

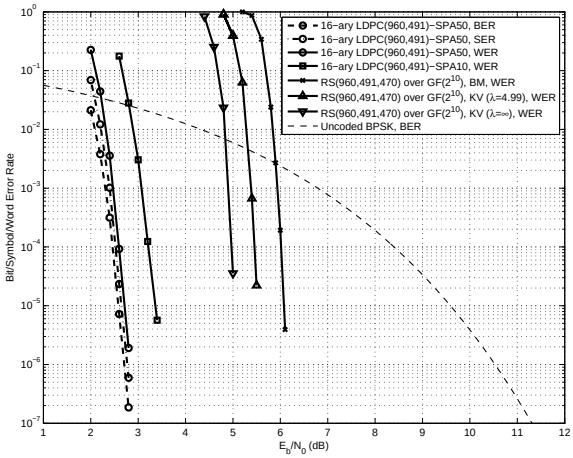

Fig. 8. Error performances of the 16-ary (960,491) QC-LDPC code and the (960,491,470) shortened RS code over GF(2^{10}) given in Example 6.

X. CONCLUSION AND REMARKS

In this paper, we have presented four algebraic methods for constructing of non-binary RS-based QC-LDPC codes. Based on these methods, some non-binary QC-LDPC codes were constructed. Experimental results show that these codes, decoded with iterative decoding using FFT-QSPA, perform very well over the AWGN and a correlated fading channels. They significantly outperform their corresponding shortened RS codes of the same lengths and rates decoded with either the BM-algorithm or the KV-algorithm (regardless of the choice of interpolation complexity coefficient, finite or infinite). Most impressively, the orders of decoding computational complexities of the constructed non-binary QC-LDPC codes, decoded with 5 and 50 iterations of the FFT-QPSA, are much smaller than those of their corresponding shortened RS codes decoded with the KV-algorithm with finite interpolation computer complexity coefficient. The comparison shows that well designed non-binary LDPC codes have a great potential

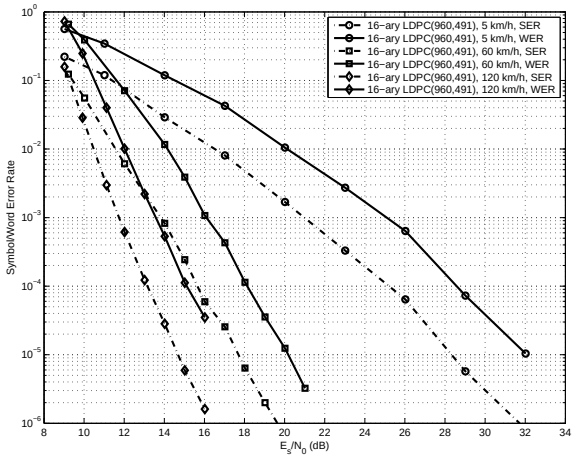

Fig. 9. Error performances of the 16-ary $(960,491)$ QC-LDPC code decoded with the FFT-QSPA with CSI over the uncorrelated Rayleigh fading channel (16-QAM) given in Example 6.

to replace RS codes for some applications in communication or storage systems, at least before a very efficient algorithm for decoding RS codes is devised (a very challenging problem). The QC-LDPC codes constructed based on array dispersions given in Section VII not only perform well over the AWGN and a correlated mobile fading channels but they are also effective in correcting erasure-bursts.

The study given in this paper is by no means conclusive. It is simply a preliminary study of the potential of non-binary LDPC codes for possible replacement of RS codes in some applications. Further study is definitely needed. Further study must include error-floor performance and rate of decoding convergence of non-binary LDPC codes and their performances over other types of channels, such as optical and channels with jamming. For applications in storage systems, codes of a very high rate, say 0.937, with a very low bit-error-rat, say 10^{-15}, is needed. Consequently, error-floor performance of non-binary LDPC codes is an important subject to be investigated.

Since the non-binary LDPC codes presented in this paper are quasi-cyclic, they have the same encoding advantage as the cyclic (or shortened cyclic) RS codes. Encoding can be implemented using simple shift-registers with linear complexity. Hardware implementation of the FFT-QSPA for decoding a non-binary QC-LDPC code may not be a hindering problem with the recent introduction of the new metal chips by Intel and IBM that can process data at a much faster speed and consume much less power than the conventional silicon chips.

REFERENCES

[1] R.G. Gallager, "Low density parity check codes," *IRE Trans. Inform. Theory*, vol. IT-8, no. 1, pp. 21-28, Jan. 1962.

[2] M.C. Davey and D.J.C. MacKay, "Low-density parity check codes over GF(q)," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165-167, Jun. 1998.

[3] D.J.C. MacKay and M.C. Davey, "Evaluation of Gallager codes of short block length and high rate applications," in *Proc. IMA International Conference on Mathematics and Its Applications: Codes, Systems and Graphical Models*, pp. 113-130, Springer-Verlag, New York, 2000.

[4] D. Declercq and M. Fossorier, "Decoding Algorithms for Nonbinary LDPC Codes over GF(q)," *IEEE Trans. Commun.*, vol. 54, no. 4, pp. 633-643, Apr. 2007.

[5] R.M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, no. 5, pp. 533-547, Sep. 1981.

[6] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711-2736, Nov. 2001.

[7] S. Lin and D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, 2nd edition, Prentice Hall, Upper Saddle River, NJ, 2004.

[8] R.M. Tanner, "Spectral graphs for quasi-cyclic LDPC codes," in *Proc. IEEE Int. Symp. Information Theory*, Washington, D.C., Jun. 2001, p. 226.

[9] Z. Li, L. Chen, L. Zeng, S. Lin, and W. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," *IEEE Trans. Commun.*, vol. 54, no. 1, pp. 71-81, Jan. 2006.

[10] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, NY, 1968; revised edition, Aegean Park Press, Laguna Hill, CA, 1984.

[11] J.L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. 15, no. 1, pp. 122-127, Jan. 1969.

[12] R. Kötter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2809-2825, Nov. 2003.

[13] Y.Y. Tai, L. Lan, L. Zeng, S. Lin, and K.A.S. Abdel-Ghaffar, "Algebraic construction of quasi-cyclic LDPC Codes for the AWGN and erasure channels," *IEEE Trans. Commun.*, vol. 54, no. 10, pp. 1765-1774, Oct. 2006.

[14] L. Lan, L. Zeng, Y.Y. Tai,, L. Chen, S. Lin, and K. Abdel-Ghaffar, "Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach," *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2429-2458, Jul. 2007.

[15] W.W. Perterson and E.J. Weldon, Jr., *Error-Correcting Codes*, M.I.T. Press, Cambridge, MA, 1972.

[16] W.J. Gross, F.R. Kschischang, R. Kötter, and P.G. Gulak, "Applications of algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1224-1234, Jul. 2006.

[17] M. El-Khamy and R. McEliece, "Iterative algebraic soft-decision list decoding of RS codes," *IEEE J. Select. Areas Commun.*, vol. 24, pp. 481-490, Mar. 2006.

[18] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar, "Construction of regular and irregular LDPC codes: Geometry decomposition and masking," *IEEE Trans. Inform. Theory*, vol. 53, no. 1, pp. 121-134, Jan. 2007.

[19] J. Hou, P.H. Siegel, and L.B. Milstein, "Performance analysis and code optimization of low density parity-check codes on Rayleigh fading channels," *IEEE J. Select. Areas Commun.*, vol. 19, no. 5, pp. 924-934, May 2001.

[20] C. Jones, T. Tian, A. Matache, R. Wesel, and J. Villasenor, "Robustness of LDPC codes on periodic fading channels," in *Proc. IEEE Global Telecommun. Conf.*, Taipei, Taiwan, Nov. 17-21, 2002, pp. 1284-1288.

[21] X. Jin, A.W. Eckford, and T.E. Fuja, "Design of good low-density parity-check codes for block fading channels," in *Proc. IEEE Military Communications Conference*, Monterey, CA Oct. 31-Nov. 3, 2004, pp. 1054-1059.

[22] Y. Zheng and C. Xiao, "Improved models for the generation of multiple uncorrelated Rayleigh fading waveforms," *IEEE Communications Letters*, vol. 6, no.6, pp. 256-258, Jun. 2002.