Constructions of Nonbinary Quasi-Cyclic LDPC Codes: A Finite Field Approach*

Shu Lin, Shumei Song, Lan Lan, Lingqi Zeng and Ying Y. Tai
Department of Electrical & Computer Engineering
University of California, Davis
Davis, CA 95616
Email: shulin,ssmsong,squash,lqzeng,yytai@ece.ucdavis.edu

***Abstract*— In the late 1950's and early 1960's, finite fields were successfully used to construct linear block codes, especially cyclic codes, with large minimum distances for correcting random errors with algebraic decoding, such as Bose-Chaudhuri-Hocqenghem (BCH) and Reed-Solomon (RS) codes. Recently it has been shown that finite fields can also be used successfully to construct binary quasi-cyclic (QC)-LDPC codes that perform very well not only over the AWGN channel but also over the binary erasure channel with iterative decoding, besides being efficiently encodable. This paper is concerned with constructions of nonbinary QC-LDPC codes based on finite fields.**

I. Introduction

LDPC codes, discovered by Gallager in 1962 [1], were rediscovered and shown to form a class of Shannon-limit approaching codes in the late 1990's and early 2000's [2-7]. Ever since their rediscovery, a great deal of research effort has been expended in the design and construction of these codes. However, most of the research effort has been focused on the design and construction of binary LDPC codes, very little on the design and construction of nonbinary LDPC codes.

Nonbinary LDPC codes and their iterative decoding using the sum-product algorithm (SPA) were first investigated by Davey and MacKay in 1998 [8]. Since their work, very little progress has been made in either construction or decoding of nonbinary LDPC codes. Most recently, a *Fast Fourier Transform* based q-ary SPA has been devised by Barnault, Declercq and Fossorier [9,10] for decoding q-ary LDPC codes. This new decoding algorithm, called FFT-QSPA, is more effective than the q-ary SPA (QSPA) devised by Davey and MacKay [8]. It significantly reduces the computational complexity of QSPA without performance degradation. This new effective decoding algorithm for nonbinary LDPC codes may motivate more research effort on the construction of nonbinary LDPC codes.

This paper is concerned with algebraic constructions of QC-LDPC codes with symbols from nonbinary finite fields.

Let GF(q) be a finite field with q elements where q is a power of a prime. A q-ary regular LDPC code $\mathcal{C}$ is given by the null space over GF(q) of a *sparse parity-check matrix* $\mathbf{H} = [h_{i,j}]$ over GF(q) that has the following structural properties: (1) each row has weight ρ; (2) each column has weight γ; and (3) no two rows (or two columns) have more than one place where they both have *nonzero* components. Such a parity-check matrix 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*. If the columns and/or rows of $\mathbf{H}$ have *varying weights*, then the null space of $\mathbf{H}$ gives an *irregular* LDPC code. A q-ary QC-LDPC code is given by the null space of an *array* of *sparse circulants* over GF(q) of the same size.

The Tanner graph [11] of a q-ary LDPC code given by the null space of a sparse parity-check matrix $\mathbf{H} = [h_{i,j}]$ over GF(q) consists of two levels of nodes, *variable and check nodes*. Variable nodes correspond to the columns of $\mathbf{H}$ and check nodes correspond to the rows of $\mathbf{H}$. The jth variable node is connected to the ith check node by an edge if and only if the entry $h_{i,j}$ at the intersection of the ith row and jth column is a nonzero element in GF(q). The RC-constraint ensures that: (1) the minimum distance of the LDPC code given by the null space of $\mathbf{H}$ is at least $\gamma + 1$ [7, 12]; and (2) the Tanner graph of the code is free of cycles of length 4 and hence its girth is at least 6. For an LDPC code to perform well with iterative decoding, its Tanner graph must not contain short cycles. The shortest cycles that affect the code performance the most are the cycles of length 4. Therefore, cycles of length 4 must be prevented in code construction. This is the case for every method of constructing LDPC codes that has been proposed.

II. Special Vector Representations of Finite Field Elements

Consider the Galois field GF(q). Let α be a primitive element of GF(q). Then the powers of $\alpha, \alpha^{-\infty} \triangleq 0, \alpha^0 = 1, \alpha, \ldots, \alpha^{q-2}$, give all the elements of GF(q) and $\alpha^{q-1} = 1$. The $q-1$ nonzero elements of GF(q) form the *multiplicative group* of GF(q) under the multiplication operation. 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 elements of GF(q), where the ith component $z_i = \alpha^i$ and all the other components are equal to zero. The weight of $\mathbf{z}(\alpha^i)$ is equal to one. This $(q-1)$-tuple over GF(q) is called the *q-ary location-vector*

*This research was supported by NASA under the Grant NNG05GD13G and NSF under the Grants CCR-0117891 and ECS-0121469.

of the field element α^i. 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 in GF(q). Then the q-ary location-vector $\mathbf{z}(\alpha)$ 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-vectors of $\delta, \alpha\delta, \ldots, \alpha^{q-2}\delta$ as rows. Each row (or each column) of $\mathbf{A}$ has one and only one nonzero element. The Matrix $\mathbf{A}$ is a *special type of circulant permutation matrix* in 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. We call $\mathbf{A}$ a q-ary α-*multiplied circulant permutation matrix*. This type of matrices will serve as the backbone for our construction of q-ary LDPC codes.

III. A General Construction of q-ray QC-LDPC Codes

Let α be a primitive element of $GF(q)$. The code construction begins with an $m \times n$ matrix $\mathbf{W}$ over $GF(q)$,

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

which has the following structural properties: (1) for $0 \leq i < m$ and $0 \leq k, l < q-1$ and $k \neq l$, $\alpha^k\mathbf{w}_i$ and $\alpha^l\mathbf{w}_i$ differ in at least $n-1$ places (i.e., $\alpha^k\mathbf{w}_i$ and $\alpha^l\mathbf{w}_i$ have at most one place where they both have the same symbol from $GF(q)$); (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. Structural property (1) implies that each row of $\mathbf{W}$ has at most one 0-element of $GF(q)$. Structural property (2) implies that any two rows in $\mathbf{W}$ differ in at least $n-1$ places. The structural properties (1) and (2) are constraints on the rows of $\mathbf{W}$ and referred to as the α-*multiplied row-constraints*, 1 and 2.

For each row $\mathbf{w}_i$ of $\mathbf{W}$ with $0 \leq i < m$, we form the following $(q-1) \times n$ matrix $\mathbf{W}_i$ over $GF(q)$:

$$\mathbf{W}_i = \begin{bmatrix} \mathbf{w}_i \\ \alpha\mathbf{w}_i \\ \vdots \\ \alpha^{q-2}\mathbf{w}_i \end{bmatrix} = \begin{bmatrix} w_{i,0} & w_{i,1} & \cdots & w_{i,n-1} \\ \alpha w_{i,0} & \alpha w_{i,1} & \cdots & \alpha w_{i,n-1} \\ \cdots & \cdots & \ddots & \cdots \\ \alpha^{q-2}w_{i,0} & \alpha^{q-2}w_{i,1} & \cdots & \alpha^{q-2}w_{i,n-1} \end{bmatrix} \quad (2)$$

It follows from the α-multiplied row-constraint-1 on $\mathbf{W}$ that any two different rows of $\mathbf{W}_i$ differ in at least $n-1$ places. We also note that for $0 \leq j < n$, if $w_{i,j}$ is a nonzero element of $GF(q)$, then the $q-1$ entries of the jth column form the $q-1$ nonzero elements of $GF(q)$. However, if $w_{i,j} = 0$, the $q-1$ entries of jth columns are all zeros. It follows from the α-multiplied row-constraint-2 that any two rows, $\alpha^k\mathbf{w}_i$ and $\alpha^l\mathbf{w}_j$, from two different matrices $\mathbf{W}_i$ and $\mathbf{W}_j$ differ in at least $n-1$ places. The matrix $\mathbf{W}_i$ is simply obtained by expanding the ith row $\mathbf{w}_i$ of $\mathbf{W}$ $q-1$ times (including $\mathbf{w}_i$ itself). This row expansion is referred to as the $(q-1)$-*fold vertical expansion* of $\mathbf{w}_i$.

For $0 \leq i < m$, replacing each entry in $\mathbf{W}_i$ by its q-ary location-vectors, we obtain a $(q-1) \times n(q-1)$ matrix $\mathbf{Q}_i$ over $GF(q)$, $\mathbf{Q}_i = [\mathbf{Q}_{i,0}, \mathbf{Q}_{i,1}, \cdots \mathbf{Q}_{i,n-1}]$, which consists of a row of n $(q-1) \times (q-1)$ submatrices over $GF(q)$, $\mathbf{Q}_{i,0}, \cdots, \mathbf{Q}_{i,n-1}$, where jth submatrix $\mathbf{Q}_{i,j}$ is formed by the q-ary location-vectors of the $q-1$ entries of the jth column of $\mathbf{W}_i$ as rows. If the first component $w_{i,j}$ of the jth column of $\mathbf{W}_i$ is a nonzero element in $GF(q)$, $\mathbf{Q}_{i,j}$ is a q-ary α-multiplied $(q-1) \times (q-1)$ circulant permutation matrix over $GF(q)$, otherwise it is a $(q-1) \times (q-1)$ zero matrix. The replacement of the entries of $\mathbf{W}_i$ by their q-ary location-vector is referred to as q-ary *horizontal expansion*. Next, we form the following $m \times n$ array $(q-1) \times (q-1)$ submatrices over $GF(q)$:

$$\mathbf{H} = \begin{bmatrix} \mathbf{Q}_0 \\ \mathbf{Q}_1 \\ \vdots \\ \mathbf{Q}_{m-1} \end{bmatrix} = \begin{bmatrix} \mathbf{Q}_{0,0} & \mathbf{Q}_{0,1} & \cdots & \mathbf{Q}_{0,n-1} \\ \mathbf{Q}_{1,0} & \mathbf{Q}_{1,1} & \cdots & \mathbf{Q}_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{Q}_{m-1,0} & \mathbf{Q}_{m-1,1} & \cdots & \mathbf{Q}_{m-1,n-1} \end{bmatrix}, \quad (3)$$

in which each submatrix $\mathbf{Q}_{i,j}$ is either a q-ary α-multiplied $(q-1) \times (q-1)$ circulant permutation matrix over $GF(q)$ or a $(q-1) \times (q-1)$ zero matrix. It is an $m(q-1) \times n(q-1)$ matrix over $GF(q)$. It follows from the structural properties of $\mathbf{W}$ and q-ary location-vectors of field elements that $\mathbf{H}$ satisfies the RC-constraint. $\mathbf{H}$ is obtained by the combination of $(q-1)$-fold vertical and q-ary horizontal expansions of $\mathbf{W}$. Each entry in $\mathbf{W}$ is dispersed into either a q-ary α-multiplied $(q-1) \times (q-1)$ circulant permutation matrix or a $(q-1) \times (q-1)$ zero matrix. We call $\mathbf{H}$ the q-ary $(q-1)$-fold *dispersion* of $\mathbf{W}$.

For any pair (γ, ρ) of integers γ and ρ with $1 \leq \gamma \leq m$ and $1 \leq r \leq n$, let $\mathbf{H}(\gamma, \rho)$ be a subarray of $\mathbf{H}$ such that each column contains at least one q-ary α-multiplied circulant permutation matrix and each row contains at least one q-ary α-multiplied circulant permutation matrix. $\mathbf{H}(\gamma, \rho)$ also satisfies the RC-constraint. Then the null space over $GF(q)$ of $\mathbf{H}(\gamma, \rho)$ gives a q-ary QC-LDPC code of length of $\rho(q-1)$ whose Tanner graph has a girth of at least 6.

The above constructions of q-ary QC-LDPC codes are based on the $(q-1)$-fold dispersion of a specific matrix $\mathbf{W}$ over $GF(q)$ whose rows satisfy two row-constraints. The matrix $\mathbf{W}$ is called the *base matrix*. There are a number of methods for constructing base matrices that satisfy the α-multiplied row-constraints, 1 and 2. Three of these methods are presented in the next three sections.

IV. First Class of q-ary QC-LDPC Codes

Suppose $q-1$ is not a prime. We can factor $q-1$ into two relatively prime factors k and m such that $q-1 = km$. Let $\beta = \alpha^k$ and $\delta = \alpha^m$. Then $B = \{\beta^0 = 1, \beta, \cdots, \beta^{m-1}\}$ and $D = \{\delta^0 = 1, \delta, \cdots, \delta^{k-1}\}$ form two cyclic subgroups of the multiplicative group of $GF(q)$ and $B \bigcap D = \{1\}$. For $0 \leq i < k$, $\delta^i B \triangleq \{\delta^i, \delta^i\beta, \cdots, \delta^i\beta^{m-1}\}$ forms a *multiplicative* coset of B. Form the following $k \times (m+1)$ matrix over $GF(q)$:

$$\mathbf{W}^{(1)} = \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{k-1} \end{bmatrix} = \begin{bmatrix} 0 & \beta-1 & \cdots & \beta^{m-1}-1 & -1 \\ \delta-1 & \delta\beta-1 & \cdots & \delta\beta^{m-1}-1 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \delta^{k-1}-1 & \delta^{k-1}\beta-1 & \cdots & \delta^{k-1}\beta^{m-1}-1 & -1 \end{bmatrix}. \quad (4)$$

$\mathbf{W}^{(1)}$ has the following structural properties: (1) two rows differ in exactly m places; (2) any two columns differ in every position; (3) all the k elements in a column (except the last column) are different; (4) All the elements in a row are different; (5) except for the element "-1" in the last column, every other element of $GF(q)$ appears once and only once; and (6) the zero element of $GF(q)$ appears at the upper left corner of $\mathbf{W}^{(1)}$. It can be readily proved that the rows of $\mathbf{W}^{(1)}$ satisfy the α-multiplied row-constraint-1 and -2.

If we disperse matrix $\mathbf{W}^{(1)}$ with $(q-1)$-fold vertical and horizontal expansions, we obtain a $k \times (m+1)$ array $\mathbf{H}^{(1)} = [\mathbf{Q}_{i,j}]$ of $k(m+1)-1$ α-multiplied $(q-1)\times(q-1)$ circulant permutation matrices over GF(q) and a single $(q-1)\times(q-1)$ zero matrix $\mathbf{Q}_{0,0}$ at the upper left corner of the array. $\mathbf{H}^{(1)}$ is $k(q-1) \times (m+1)(q-1)$ matrix over GF(q). The first $q-1$ columns of $\mathbf{H}^{(1)}$ have weights equal to $k-1$ and all the other columns have weights equal to k. The first $q-1$ rows of $\mathbf{H}^{(1)}$ have weights equal to m and all the other rows have weights equal to $m+1$.

For any pair of integers, γ and ρ, with $1 \le \gamma \le k$ and $1 \le \rho \le m+1$, let $\mathbf{H}^{(1)}(\gamma,\rho)$ be a $\gamma \times \rho$ subarray $\mathbf{H}^{(1)}$. $\mathbf{H}^{(1)}(\gamma,\rho)$ is a $\gamma(q-1)\times\rho(q-1)$ matrix over GF(q). If $\mathbf{H}^{(1)}(\gamma,\rho)$ does not contain the zero submatrix $\mathbf{Q}_{0,0}$, $\mathbf{H}^{(1)}(\gamma,\rho)$ is a regular matrix with column and row weights γ and ρ, respectively, otherwise, it has two column weights $\gamma-1$ and γ and two row weights, $\rho-1$ and ρ. The null space over GF(q) of $\mathbf{H}^{(1)}(\gamma,\rho)$ gives a QC-LDPC code $\mathcal{C}$ over GF(q) of length $\rho(q-1)$ with rate at least $(\rho-\gamma)/\gamma$ and minimum distance at least $\gamma+1$ for regular case and γ for irregular case. The above construction gives a class of nonbinary QC-LDPC codes.

Example 1: Consider the field $GF(2^6)$. We can factor $2^6-1=63$ into two relatively prime factors 7 and 9. Let $k=7$ and $m=9$. We can construct a 7×10 array $\mathbf{H}_q^{(1)} = [\mathbf{Q}_{i,j}]$ of 69 α-multiplied 63×63 circulant permutation matrices over $GF(2^6)$ and a single 63×63 zero matrix $\mathbf{Q}_{0,0}$. Choose $\gamma = 4$ and $\rho = 9$. We take a 4×9 subarray $\mathbf{H}^{(1)}(4,9)$ from $\mathbf{H}^{(1)}$, avoiding the zero matrix $\mathbf{Q}_{0,0}$, say taking the first 4 rows of $\mathbf{H}^{(1)}$ and deleting the first column. $\mathbf{H}^{(1)}(4,9)$ is a 252×567 matrix over $GF(2^6)$ with column and row weights 4 and 9, respectively. The null space over $GF(2^6)$ of $\mathbf{H}^{(1)}(4,9)$ gives a 64-ary $(567, 333)$ QC-LDPC code $\mathcal{C}$ with rate 0.5873. Assume BPSK transmission over the AWGN channel. Each code symbol is expanded into 6 bits. The performance of this code decoded with the FFT-QSPA is shown in Figure 1. Also included in Figure 1 is the performance of a $(567, 333, 235)$ shortened RS code [13] over $GF(2^{10})$ decoded with Euclidean algorithm [12]. At the BER (bit-error rate) or SER (symbol-error rate) of 10^{-6}, the 64-ary QC-LDPC code $\mathcal{C}$ achieves a 2.7 dB coding gain over the $(567, 333, 235)$ shortened RS code over $GF(2^{10})$ at the expense of a larger decoding computational complexity. $\triangle\triangle$

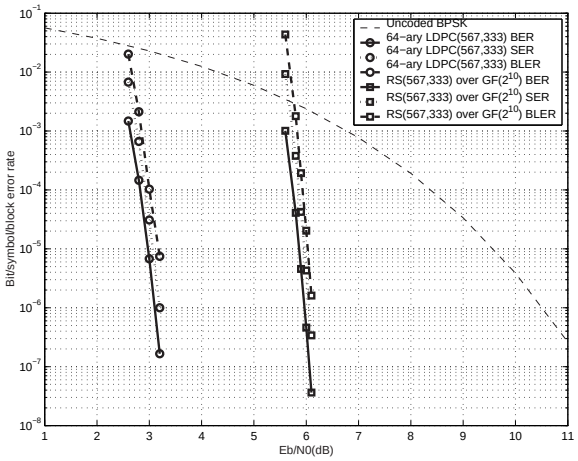

Fig. 1. The performance of the $(567, 333)$ QC-LDPC code over $GF(2^6)$ given in Example 1

V. Second Class of q-ary QC-LDPC Codes

Again we consider the Galois field GF(q). Let α be a primitive element of GF(q). Then the $q-1$ nonzero elements, $\alpha^0 = 1, \alpha, \ldots, \alpha^{q-2}$, form the multiplicative group of GF(q). Define the following $(q-1)$-tuple over GF(q), $\mathbf{w}_0 = (\alpha^0 - 1, \alpha-1, \ldots, \alpha^{q-2}-1)$. Form the following $(q-1)\times(q-1)$ matrix $\mathbf{W}^{(2)}$ over GF(q) with $\mathbf{w}_0$ and its $q-2$ right cyclic-shifts, $\mathbf{w}_1$, …, $\mathbf{w}_{q-2}$, as rows:

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

Label the columns of $\mathbf{W}^{(2)}$ from 0 to $q-2$. The matrix $\mathbf{W}$ has the following structural properties: (1) any two rows differ in all positions; (2) any two columns differ in all positions; (3) all $q-1$ elements in each column (or in each row) are distinct elements in GF(q); (4) each row (or each column) contains one and only one 0-element; and (5) all the 0-elements lie on the main diagonal of $\mathbf{W}$. Property (1) implies that the rows of $\mathbf{W}^{(2)}$ satisfy the row-constraint-1 defined in Section IV. The rows of $\mathbf{W}^{(2)}$ also satisfy the row-constraint-2 whose proof is given in Lemma 1.

Lemma 1: For $0 \le i, j, k, l < q-1$ with $i \ne j$, the two $(q-1)$-tuples $\alpha^k\mathbf{w}_i$ and $\alpha^l\mathbf{w}_j$ can not have more than one position with identical components, i.e., they differ in at least $q-2$ positions.

Proof: Suppose there are two different positions, say s and t with $0 \leq s,t < q-1$, where $\alpha^k \mathbf{w}_i$ and $\alpha^l \mathbf{w}_j$ have identical components. Then $\alpha^k(\alpha^{s-i}-1) = \alpha^l(\alpha^{s-j}-1)$ and $\alpha^k(\alpha^{t-i}-1) = \alpha^l(\alpha^{t-j}-1)$. These two equalities imply that $i = j$ or $s = t$ which contradict the assumptions that $i \neq j$ and $s \neq t$. This proves the theorem. ■

It follows from the structural properties and Lemma 1 that $\mathbf{W}$ satisfies both row-constraints, 1 and 2. Dispersing $\mathbf{W}^{(2)}$ with $(q-1)$-fold vertical and horizontal expansions as described in Section III, we obtain the following $(q-1)\times(q-1)$ array of $(q-1)\times(q-1)$ submatrices over GF(q),

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

where the submatrices on the main diagonal are $(q-1)\times(q-1)$ zero matrices and all the other submatrices are α-multiplied $(q-1)\times(q-1)$ circulant permutation matrices. $\mathbf{H}^{(2)}$ is a $(q-1)^2 \times (q-1)^2$ matrix over GF(q) with both column and row weights $q-2$. Since $\mathbf{W}^{(2)}$ satisfies both row-constraints, 1 and 2, $\mathbf{H}^{(2)}$ satisfies the RC-constraint and consequently its associated Tanner graph is free of cycles of length 4.

For any pair of integers, (γ,ρ), with $1 \leq \gamma,\rho < q$, let $\mathbf{H}^{(2)}(\gamma,\rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}^{(2)}$. Then $\mathbf{H}^{(2)}(\gamma,\rho)$ is a $\gamma(q-1)\times\rho(q-1)$ matrix over GF(q). If $\mathbf{H}^{(2)}(\gamma,\rho)$ lies above or below the main diagonal of $\mathbf{H}^{(2)}$, it does not contain any of the zero submatrices of $\mathbf{H}^{(2)}$ and hence it is a (γ,ρ)-regular matrix over GF(q) with column and row weights γ and ρ, respectively. Since $\mathbf{H}^{(2)}$ satisfies the RC-constraint, $\mathbf{H}^{(2)}(\gamma,\rho)$ also satisfies the RC-constraint. Consequently, the null space over GF(q) of $\mathbf{H}^{(2)}(\gamma,\rho)$ gives a q-ary regular QC-LDPC code $\mathcal{C}$ of length $\rho(q-1)$ with rate at least $(\rho-\gamma)/\rho$ and minimum distance at least $\gamma+1$, whose Tanner graph has a girth of at least 6. If $\mathbf{H}^{(2)}(\gamma,\rho)$ contains some zero submatrices of $\mathbf{H}^{(2)}$ but not all, it has two different column weights, $\gamma-1$ and γ, and it may have two different row weights, $\rho-1$ and ρ. In this case, the null space over GF(q) of $\mathbf{H}^{(2)}(\gamma,\rho)$ gives a near-regular q-ary QC-LDPC code with minimum distance at least γ. For a given field GF(q), a family of structurally compatible q-ary QC-LDPC codes of various lengths, rates and minimum distances can be constructed.

Example 2: Let GF(2^4) be the code construction field. Based on (5) to (6), we can construct a 15×15 array $\mathbf{H}^{(2)}$ of α-multiplied 15×15 circulant permutation matrices over GF(2^4). Suppose we choose $\gamma = 4$ and $\rho = 15$. Take a 4×15 subarray $\mathbf{H}^{(2)}(4,15)$ from $\mathbf{H}_{qc}$, say the first 4 rows of α-multiplied circulant permutation matrices of $\mathbf{H}^{(2)}$. Then $\mathbf{H}^{(2)}(4,15)$ is a 60×225 matrix over GF(2^4) with row weight 15 and two different column weights 3 and 4. The null space over GF(2^4) of $\mathbf{H}^{(2)}(4,15)$ gives a 16-ary $(225,173)$ QC-LDPC code with rate 0.7689. Assume BPSK transmission (each symbol of GF(2^4) is expanded into 4 bits) over the AWGN channel. The error performance of this code decoded with the FFT-QSPA with a maximum number of iterations set to 50 are shown in Figure 2. Also included in Figure 2 is the error performance of a $(225,173,53)$ shortened RS code over GF(2^8) decoded with the Euclidean algorithm. We see that at the BER or BLER (block-error rate) of 10^{-6}, the 16-ary $(225,173)$ QC-LDPC code achieves a 2.1 dB coding gain over the $(225,173,53)$ shortened RS code over GF(2^8). This coding gain is achieved at the expense of a larger computational complexity. However, the shortened RS code over GF(2^8) has a much larger symbol size than the 16-ary QC-LDPC code. In terms of bits, the shortened RS code over GF(2^8) is twice as long as the 16-ary QC-LDPC code. △△

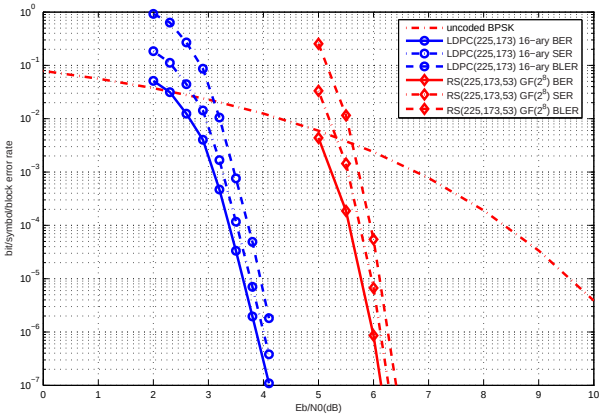

Fig. 2. Performances of the 16-ary $(225,173)$ QC-LDPC code and the $(225,173,53)$ shortened RS code over GF(2^8) over the AWGN channel.

Example 3: In Example 2, suppose we choose $\gamma = 4$ and $\rho = 8$. Take the 4×8 subarray $\mathbf{H}^{(2)}(4,8)$ at the upper right corner of $\mathbf{H}^{(2)}$ as the parity-check matrix. This parity-check matrix is a 60×120 matrix over GF(2^4) with column and row weights 4 and 8, respectively. The null space over GF(2^4) of $\mathbf{H}^{(2)}(4,8)$ gives a 16-ary $(120,71)$ QC-LDPC code with rate 0.5917. The performance of this code decoded with the FFT-QSPA with 50 iterations is shown in Figure 3 which also includes the performance of a $(120,71,50)$ shortened RS code over GF(2^7) decoded with the Euclidean algorithm for comparison. We see that at the BER or SER of 10^{-6}, the 16-ary $(120,71)$ QC-LDPC code achieves a 2.25 dB coding gain over the $(120,71,50)$ shortened RS code over GF(2^7). △△

Example 4: Let GF(2^6) be the code construction field. Based on this field, we can construct a 63×63 array $\mathbf{H}^{(2)}$ of α-multiplied 63×63 circulant permutation matrices. Set $\gamma = 4$ and $\rho = 32$. Take a 4×32 subarray $\mathbf{H}^{(2)}(4,32)$ from $\mathbf{H}^{(2)}$ that does not contain zero submatrices of $\mathbf{H}^{(2)}$. $\mathbf{H}^{(2)}(4,32)$ is 252×2016 matrix over GF(2^6) with column and row weights 4 and 32, respectively. The null space over GF(2^6) of $\mathbf{H}^{(2)}(4,32)$ gives a $(2016,1779)$ QC-LDPC code over GF(2^6) with rate 0.8824. The performance of this code decoded with the FFT-QSPA is shown in Figure 4 which also includes the performance of the $(2016,1779,238)$ shortened RS code over GF(2^{11}) decoded with the Euclidean algorithm. We see that

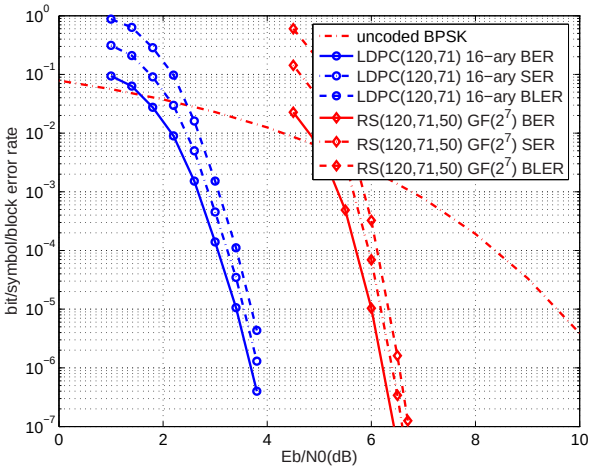

Fig. 3. Performances of the $(120, 71)$ 16-ary QC-LDPC code and the $(120, 71, 50)$ shortened RS code over GF(2^7) over the AWGN channel.

at the SER of 10^{-6}, the $(2016, 1779)$ QC-LDPC code over GF(2^6) achieves a 2 dB coding gain over the $(2016, 1779, 238)$ RS code over GF(2^{11}). △△

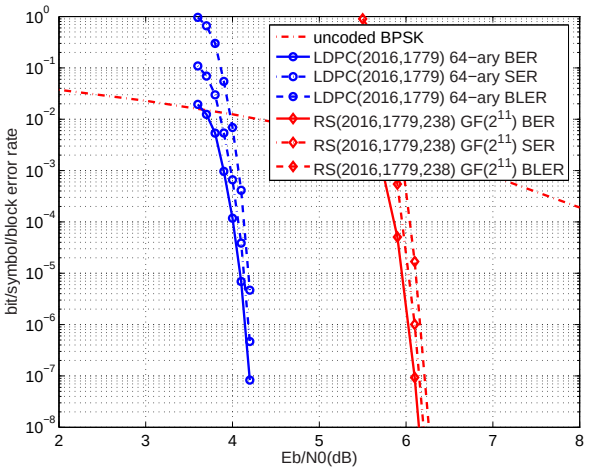

Fig. 4. Performances of the $(2016, 1779)$ 64-ary QC-LDPC code and the $(2016, 1779, 238)$ shortened RS code over GF(2^{11}) over the AWGN channel.

VI. Third Class of q-ary QC-LDPC Codes

Again 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 in GF(q) of order m, i.e., m is the smallest positive 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 of GF(q). For $1 \leq t < m$, we form the following matrix over GF(q):

$$\mathbf{W}^{(3)} = \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{t-1} \end{bmatrix} = \begin{bmatrix} 1 & \beta & \beta^2 & \ldots & \beta^{m-1} \\ 1 & \beta^2 & (\beta^2)^2 & \ldots & (\beta^2)^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^t & (\beta^t)^2 & \ldots & (\beta^t)^{m-1} \end{bmatrix}, \quad (7)$$

where the power of β is taken modulo m.$\mathbf{W}^{(3)}$ is simply the parity-check matrix of an $(m, m-t, t+1)$ nonprimitive cyclic RS code over GF(q). It can be proved that $\mathbf{W}^{(3)}$ satisfies the row constraints, 1 and 2 as given in Section III. Hence it can be dispersed to form parity-check matrices of a class of q-ary QC-LDPC codes. These codes are referred to as dispersed RS codes.

VII. Conclusion and Remarks

In this paper, we have presented a general approach for constructing nonbinary QC-LDPC codes based on dispersing row constrained matrices over finite fields using $(q-1)$-fold vertical and horizontal expansions. Based on this general approach, we have presented two specific methods for constructing two classes of q-ary QC-LDPC codes. Examples have been given. Codes given in these examples have large coding gains over their corresponding RS codes (the same lengths and rates) decoded algebraically. The coding gains are achieved at the expense of larger computational complexities. There are other methods can be used for constructing nonbinary QC-LDPC codes. For examples, we can construct nonbinary QC-LDPC codes based on additive subgroups of finite fields, primitive elements of finite fields, and lines of finite geometries.

References

[1] R. G. Gallager, "Low density parity check codes," *IRE Trans. Inform. Theory*, IT-8, pp. 21-28, Jan. 1962.

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electro. Lett.*, vol. 32, pp. 1645-1646, Aug. 1996.

[3] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399-432, Mar. 1999.

[4] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599-618, Feb., 2001.

[5] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching low density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619-637, Feb., 2001.

[6] S. Y. Chung, T. Richardson and R. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using Gaussian approximation", *IEEE Trans. Inform. Theory*, vol. 47, pp. 657-670, Feb. 2001.

[7] Y. Kou, S. Lin, and M. Fossorier, "Low density parity check codes based on finite geometries: a discovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2711-2736, Nov. 2001.

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

[9] L. Barnault and D. Declercq, "Fast Decoding Algorithm for LDPC over GF(2^q)," *Proceeding of ITW2003*, pp. 70-73, Paris, France, March 31 - April 4,2003.

[10] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," submitted to *IEEE Trans. Commun.*, 2005.

[11] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, pp. 533-547, Sept. 1981.

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

[13] I. S. Reed and G. Solomon, "Polynomial code over certain finite fields," *J. Soc. Ind. Appl. Math.*, 8: 300-304, June 1960.
[14] Lingqi Zeng, Lan Lan, Ying Y. Tai and Shu Lin, "Dispersed Reed-Solomon codes for iterative decoding and construction of q-ary LDPC codes", *IEEE Globecom'05*, St. Louis, MO, Nov. 28- Dec. 2,2005