Algebraic Constructions of Nonbinary Quasi-Cyclic LDPC Codes: Array Masking and Dispersion *

Shu Lin, Shumei Song, Bo Zhou, Jingyu Kang and Ying Y. Tai
Department of Electrical and Computer Engineering
University of California, Davis,
Davis, CA 95616, U.S.A.
Email: {shulin, ssmsong, bozhou, jykang, yytai}@ece.ucdavis.edu

Qin Huang
School of Information Science and Engineering
Southeast University
Nanjing, China
Email: hq@seu.edu.cn

***Abstract*— This paper is concerned with algebraic constructions of nonbinary quasi-cyclic (QC) LDPC codes based on arrays of circulant permutation matrices constructed from finite fields. Two methods, array masking and dispersion, are presented for constructing nonbinary QC-LDPC codes. Simulation results show that codes constructed by these methods perform very well with iterative decoding based on belief propagation. They achieve significant coding gains over Reed-Solomon codes of the same lengths and rates decoded with either algebraic hard-decision decoding or algebraic soft-decision decoding at the expense of larger decoding complexity.**

I. Introduction

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 $\mathbf{H}$ 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 position 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 Tanner graph of the LDPC code $\mathcal{C}$ given by the null space of $\mathbf{H}$ has a girth of at least 6. If the columns and/or rows of $\mathbf{H}$ have varying weights, then the null space of $\mathbf{H}$ gives a q-ary 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).

This paper is a continuation of [1] concerning with constructions of nonbinary QC-LDPC codes based on RC-constrained arrays of special circulant permutation matrices over nonbinary finite fields. Experimental results show that codes constructed perform very well with iterative decoding and they achieve significant coding gains over the Reed-Solomon (RS) codes of the same lengths and rates with either the algebraic Berlekamp-Massey (BM) [2],[3] hard-decision decoding or the algebraic Köetter-Vardy (KV) [4] soft-decision decoding.

*This research was supported by NASA under the Grant NNG05GD13G and a gift grant from Norhtrop Grumman Space Technology.

II. A General Construction of Q-ary QC-LDPC Codes

Consider the Galois field GF(q) with α as a primitive element. Then $\alpha^{-\infty} \triangleq 0, \alpha^0 = 1, \alpha, \ldots, \alpha^{q-2}$ 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 unit-weight $(q-1)$-tuple over GF(q) is called the q-ary *location-vector* of the field element α^i. The single nonzero components of the q-ary location-vectors of two nonzero elements of 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 $\mathbf{Q}$ over GF(q) with the q-ary location-vectors of $\delta, \alpha\delta, \ldots, \alpha^{q-2}\delta$ as rows. Matrix $\mathbf{Q}$ is a special type of *circulant permutation matrix* 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 circulant permutation matrix*. Since $\mathbf{Q}$ is obtained by dispersing (or expanding) δ horizontally and vertically, $\mathbf{Q}$ is referred as the *two-dimensional* $(q-1)$-fold array dispersion of δ (simply array dispersion of δ). It is clear that the array dispersion of the 0-element is a $(q-1) \times (q-1)$ zero matrix.

Code construction begins with an $m \times n$ matrix over GF(q) [1],

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

whose rows satisfies the following constraints: (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; and (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. The two constraints on the rows of $\mathbf{W}$ are called the *α-multiplied row-constraints* 1 and 2. Dispersing each nonzero entry of $\mathbf{W}$ into an $(q-1) \times (q-1)$ α-multiplied circulant permutation matrix and each 0-entry into a $(q-1)\times(q-1)$ zero matrix, we obtain the following $m \times n$ array of $(q-1)\times(q-1)$ α-multiplied circulant permutation and zero matrices:

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

It 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. $\mathbf{H}$ is called the *two-dimensional $(q-1)$-fold array dispersion* of matrix $\mathbf{W}$.

For any pair (γ, ρ) of integers γ and ρ with $1 \leq \gamma \leq m$ and $1 \leq \rho \leq n$, let $\mathbf{H}(\gamma, \rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}$. $\mathbf{H}(\gamma, \rho)$ is a $\gamma(q-1) \times \rho(q-1)$ matrix over GF(q) and also satisfies the RC-constraint. Then the null space of $\mathbf{H}(\gamma, \rho)$ gives a (γ, ρ)-regular q-ary QC-LDPC code $\mathcal{C}$ of length $\rho(q-1)$. If $\mathbf{H}(\gamma, \rho)$ has constant column and row weights, then $\mathcal{C}$ is a regular QC-LDPC code, otherwise it is an irregular QC-LDPC code. The above construction gives a class of q-ary QC-LDPC codes. The matrix $\mathbf{W}$ is called the *base matrix* for dispersion. In Sections III and IV, we present two specific methods for constructing base matrices for dispersion.

III. Two Classes of Nonbinary QC-LDPC Codes

In this section, we present two specific methods for constructing RC-constrained arrays of α-multiplied circulant permutation matrices. Based on these arrays, two classes of QC-LDPC codes are constructed.

A. Construction Based on Additive Subgroups of Finite Field

Let $q = 2^m$. Consider the field GF(2^m) that is an extension field of the binary field GF(2). Let α be a primitive element of GF(2^m). Then $\alpha^0, \alpha, \cdots, \alpha^{m-1}$ are linearly independent elements of GF(2^m). These m elements form a basis of GF(2^m). Any element α^i of GF(2^m) can be expressed as linear combination of $\alpha^0, \alpha, \cdots, \alpha^{m-1}$ as follows: $\alpha^i = c_{i,0}\alpha^0 + c_{i,1}\alpha + \cdots + c_{i,m-1}\alpha^{m-1}$ with $c_{i,j} \in \mathrm{GF}(2^m)$. For $1 \leq t < m$, let $\mathcal{G}_1 = \{\beta_0 = 0, \beta_1, \cdots, \beta_{2^t-1}\}$ and $\mathcal{G}_2 = \{\lambda_0 = 0, \lambda_1, \cdots, \lambda_{2^{m-t}-1}\}$ be two additive subgroups of GF(q) that are spanned by the elements in $\{\alpha^0, \alpha, \cdots, \alpha^{t-1}\}$ and the elements in $\{\alpha^t, \alpha^{t+1}, \cdots, \alpha^{m-1}\}$, respectively. Form the following $2^{m-t} \times 2^t$ matrix over GF(2^m):

$$\mathbf{W}^{(1)} = \begin{bmatrix} 0 & \beta_1 & \cdots & \beta_{2^t-1} \\ \lambda_1 & \lambda_1+\beta_1 & \cdots & \lambda_1+\beta_{2^t-1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{2^{m-t}-1} & \lambda_{2^{m-t}-1}+\beta_1 & \cdots & \lambda_{2^{m-t}-1}+\beta_{2^t-1} \end{bmatrix}, \quad (3)$$

where (1) the entries of the first row are elements of the group $\mathcal{G}_1$, and (2) the entries of the ith row are the elements of the coset $\lambda_i + \mathcal{G}_1$ of $\mathcal{G}_1$ with coset leader $\lambda_i \in \mathcal{G}_2$. Every element of GF($2^m$) appears once and only once in $\mathbf{W}^{(1)}$. We readily see that $\mathbf{W}^{(1)}$ satisfies the α-multiplied row-constraints 1 and 2. Dispersing the $2^m - 1$ nonzero entries of $\mathbf{W}^{(1)}$ into $(2^m-1)\times(2^m-1)$ α-multiplied circulant permutation matrices and the single 0-element into a zero matrix, we obtain the following $2^{m-t} \times 2^t$ array of $2^m - 1$ α-multiplied circulant matrices and a single zero matrix of size $(2^m-1)\times(2^m-1)$:

$$\mathbf{H}^{(1)} = \begin{bmatrix} \mathbf{O} & \mathbf{Q}_{0,1} & \cdots & \mathbf{Q}_{0,2^t-1} \\ \mathbf{Q}_{1,0} & \mathbf{Q}_{1,1} & \cdots & \mathbf{Q}_{1,2^t-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{Q}_{2^{m-t}-1,0} & \mathbf{Q}_{2^{m-t}-1,1} & \cdots & \mathbf{Q}_{2^{m-t}-1,2^t-1} \end{bmatrix}, \quad (4)$$

where the zero matrix is at the upper left corner of the array.

For any pair (γ, ρ) of integers, with $1 \leq \gamma \leq 2^{m-t}$ and $1 \leq \rho \leq 2^t$, let $\mathbf{H}^{(1)}(\gamma, \rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}^{(1)}$. Then $\mathbf{H}^{(1)}(\gamma, \rho)$ is a $\gamma(q-1) \times \rho(q-1)$ matrix over GF(2^m) with column and row weights γ and ρ, respectively. The null space of $\mathbf{H}^{(1)}(\gamma, \rho)$ gives a 2^m-ary QC-LDPC code. The above construction gives a class of 2^m-ary QC-LDPC codes.

In the following, we use an example to illustrate the above code construction. In all the examples given in this paper, we compute the error performance of a code with iterative decoding using the fast Fourier transform based q-ary sum-product algorithm (FFT-QSPA) [5]-[7] and set the maximum number of iterations to 50. We also assume BPSK signaling for transmission over the AWGN channel.

Example 1: In this example, we choose $m = 5$ and use GF(2^5) as the code construction field. Let α be a primitive element of GF(2^5). Set $t = 3$. Then $m - t = 2$. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two additive groups of orders 8 and 4 spanned by the elements in $\{\alpha^0, \alpha, \alpha^2\}$ and the elements in $\{\alpha^3, \alpha^4\}$, respectively. Based on these two groups, we can form a 4×8 array $\mathbf{H}^{(1)}$ of 31 α-multiplied circulant permutation matrices of size 31×31 and a single zero matrix. Choose $\gamma = 4$ and $\rho = 8$. Then $\mathbf{H}^{(1)}(4, 8) = \mathbf{H}^{(1)}$ which is a 124×248 matrix over GF(2^5). $\mathbf{H}^{(1)}(4, 8)$ has 31 columns of weight three, 217 columns of weight four, 31 rows of weight 7 and 93 rows of weight 8. The null space of $\mathbf{H}^{(1)}(4, 8)$ gives a near regular 32-ary $(248, 136)$ QC-LDPC code. The block error performance of this code decoded with the FFT-QSPA is shown in Figure 1. For comparison, Figure 1 also includes the block error performances of the $(248, 136, 113)$ shortened RS code over GF(2^8) decoded with the algebraic hard-decision BM algorithm and the algebraic soft-decision KV algorithm with maximum interpolation multiplicity (MIM) λ [8] equal to 4.99 and infinity, respectively. At the block error rate (BLER) of 10^{-5}, the 32-ary QC-LDPC code achieves a 2.7 dB coding gain over the $(248, 136, 113)$ RS code with the hard-decision BM decoding, while achieves a 2.1 dB and a 1.6 dB coding gains over the RS code using the algebraic soft-decision KV decoding with MIM λ equal to 4.99 and infinity, respectively.

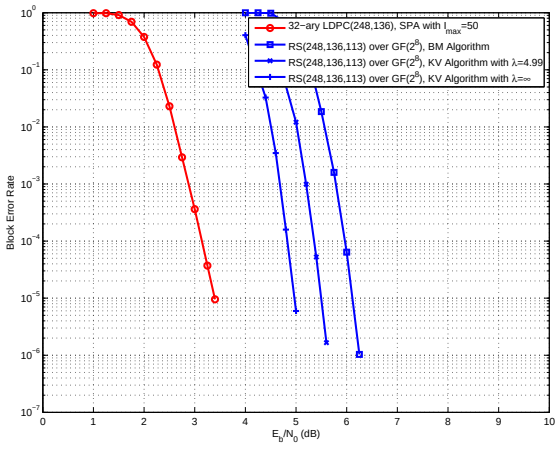

Fig. 1. Block error performances of the 32-ary $(248, 136)$ QC-LDPC code and the $(248, 136, 113)$ shortened RS code over GF(2^8) over the AWGN channel.

B. *Construction Based on the Multiplicative Group of a Finite Field*

Consider the $(q-1)$-tuple $\mathbf{w}_0 = (\alpha^0-1, \alpha-1, \cdots, \alpha^{2^m-2}-1)$ over GF(2^m). It can be easily proved that this $(q-1)$-tuple $\mathbf{w}_0$ is a minimum weight codeword of the $(2^m-1, 2, 2^m-2)$ RS code over GF(2^m) with two information symbols and minimum distance 2^m-2. The first component of $\mathbf{w}_0$ is zero. Form the following $(2^m-1)\times(2^m-1)$ matrix over GF(2^m) with $\mathbf{w}_0$ and its $q-2$ right cyclic-shifts, $\mathbf{w}_1, \cdots, \mathbf{w}_{2^m-2}$ as rows:

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

with zero entries on the main diagonal. Since $\mathbf{w}_0, \mathbf{w}_1, \cdots, \mathbf{w}_{2^m-2}$ are minimum weight codewords of the $(2^m-1, 2, 2^m-2)$ RS code over GF(2^m). It can be easily proved that $\mathbf{W}^{(2)}$ satisfies the α-multiplied row-constraints 1 and 2.

Dispersing the nonzero entries into $(2^m-1)\times(2^m-1)$ α-multiplied circulant permutation matrices and the zero entries into $(2^m-1)\times(2^m-1)$ zero matrices, we obtain the follwing $(2^m-1)\times(2^m-1)$ array of α-multiplied circulant permutation and zero matrices of size $(2^m-1)\times(2^m-1)$:

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

where the zero matrices are on the main diagonal of the array.

For any pair (γ, ρ) of integers with $1 \le \gamma, \rho < q$, let $\mathbf{H}^{(2)}(\gamma, \rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}^{(2)}$. Then the null space over GF(2^m) of $\mathbf{H}^{(2)}(\gamma, \rho)$ gives a 2^m-ary QC-LDPC code. The above construction gives another class of nonbinay QC-LDPC codes.

Example 2: Let GF(2^4) be the code construction field. Based on the method given above, we can construct a 15×15 array $\mathbf{H}^{(2)}$ of α-multiplied circulant permutation and zero matrices of size 15×15 with the zero matrices on its main diagonal. Choose $\gamma = 4$ and $\rho = 8$. Take a 4×8 subarray $\mathbf{H}^{(2)}(4,8)$ from $\mathbf{H}^{(2)}$ that contains no zero matrices. Then $\mathbf{H}^{(2)}(4,8)$ is a 60×120 matrix over GF(2^4) with column and row weights 4 and 8, respectively. The null space of $\mathbf{H}^{(2)}(4,8)$ gives a $(4,8)$-regular 16-ary $(120, 71)$ QC-LDPC code. The block error performance of the code decoded with the FFT-QSPA is shown in Figure 2. Also included in Figure 2 are the block error performances of the $(120, 71, 50)$ shortened RS code over GF(2^7) with the algebraic hard-decision BM and the algebraic soft-decision KV decodings. At the BLER of 10^{-5}, the 16-ary $(120, 71, 50)$ QC-LDPC code achieves a 2.6 dB coding gain over the $(120, 71, 50)$ shortened RS code with the hard-decision BM decoding, while it achieves a 2.1 dB and 1.6 dB coding gains over the RS code using the algebraic soft-decision KV decoding with MIM λ equal to 4.99 and infinity, respectively.

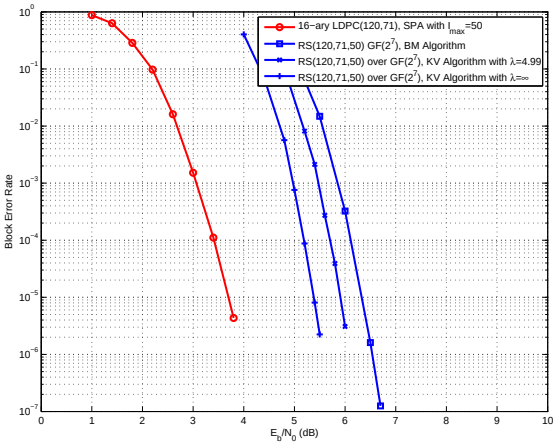

Fig. 2. Block error performances of the 16-ary $(120, 71)$ QC-LDPC code and the $(120, 71, 50)$ shortened RS code over GF(2^7) over the AWGN channel.

IV. Code Construction Based on Array Masking and Dispersion

In Section III, we have presented two classes of q-ary QC-LDPC codes based on RC-constrained arrays of α-multiplied circulant permutation matrices that are constructed from finite fields. Although these arrays are highly structured, their constituent circulant permutation matrices are densely packed. In this section, we present two techniques, *array masking* and *dispersion*, to reduce the density of circulant permutation matrices of an RC-constrained array constructed in Section III. The reduction of the density of circulant permutation matrices of an array results in a sparser array whose associated

Tanner graph has fewer edges and hence fewer short cycles and probably larger girth. As a result, the performance of the code given by the sparser array my be improved and computational complexity is reduced.

A. *Array Masking*

Array masking is simply to replace a set of α-multiplied circulant permutation matrices by a set of zero matrices. Consider an RC-constrained $\gamma \times \rho$ array $\mathbf{H}(\gamma, \rho) = [\mathbf{Q}_{i,j}]$ of α-multiplied $(q-1) \times (q-1)$ circulant permutation matrices over GF(q). 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: $\mathbf{M}(\gamma, \rho) = \mathbf{Z}(\gamma, \rho) \bigotimes \mathbf{H}(\gamma, \rho) = [z_{i,j}\mathbf{Q}_{i,j}]$ where $z_{i,j}\mathbf{Q}_{i,j} = \mathbf{Q}_{i,j}$ for $z_{i,j} = 1$ and $z_{i,j}\mathbf{Q}_{i,j} = \mathbf{O}$ (a $(q-1) \times (q-1)$ zero matrix). In this matrix product operation, a set of α-multiplied circulant permutation matrices 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*. In masking, we avoid masking zero matrices in the base array $\mathbf{H}(\gamma, \rho)$. If $\mathbf{H}(\gamma, \rho)$ does not contain zero matrices. Then the distribution of the α-multiplied circulant permutation matrices 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 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 $g > 6$, the girth of the associated Tanner graph of the masked array $\mathbf{M}(\gamma, \rho)$ is at least g. The concept of masking was recently intorduced in [9], [10].

The null space of $\mathbf{M}(\gamma, \rho)$ gives a q-ary QC-LDPC code $\mathcal{C}_m$ which is different from the code given by the null space of $\mathbf{H}(\gamma, \rho)$. The error performance of $\mathcal{C}_m$ depends on the distribution of 1-entries (or the 0-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. $\mathbf{Z}(\gamma, \rho)$ should be a very sparse matrix. If $\mathbf{Z}(\gamma, \rho)$ is regular, then the null space of $\mathbf{M}(\gamma, \rho)$ gives a regular code, otherwise it gives an irregular code. Regular masking matrices can be constructed algebraically [10].

Example 3: Let GF(2^7) be the code construction field. Let α be a primitive element in GF(2^7). Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two additive groups of orders 16 and 8 spanned by $\{\alpha^0, \alpha, \alpha^2, \alpha^3\}$ and $\{\alpha^4, \alpha^5, \alpha^6\}$, respectively. Based on these two groups, we form an 8×16 array $\mathbf{H}^{(1)}$ of 127 α-multiplied circulant permutation matrices over GF(2^7) of size 127×127 and a single zero matrix at the upper left corner of $\mathbf{H}^{(1)}$. Choose $\gamma = 8$ and $\rho = 16$. Then $\mathbf{H}^{(1)}(8, 16)$ is the entire array $\mathbf{H}^{(1)}$. We use $\mathbf{H}^{(1)}(8, 16)$ as the base array for masking. Construct a 8×16 masking matrix $\mathbf{Z}(8, 16)$ that consists of two 8×8 circulants side by side. The *generator vectors* (or top rows) of these two circulants are (01011000) and (00101010), respectively. Masking $\mathbf{H}^{(1)}(8, 16)$ with $\mathbf{Z}(8, 16)$, we obtain an 8×16 masked array $\mathbf{M}(8, 16) = \mathbf{Z}(8, 16) \bigotimes \mathbf{H}^{(1)}(8, 16)$ which is a 1016×2032 matrix over GF(2^7) with column and row weights 3 and 6, respectively. The null space over GF(2^7) of $\mathbf{M}(8, 16)$ gives a 128-ary $(2032, 1016)$ QC-LDPC code with rate 0.5. The symbol and block error performances of this code are shown in Figure 3 which also includes the symbol and block error performances of the $(2032, 1026, 1017)$ shortened RS code over GF(2^{11}) with the hard-decision BM decoding. At the SER (symbol error rate) and BLER of 10^{-5}, the 128-ary QC-LDPC code achieves a 4 dB coding gain over the RS code with hard-decision decoding over the AWGN channel.

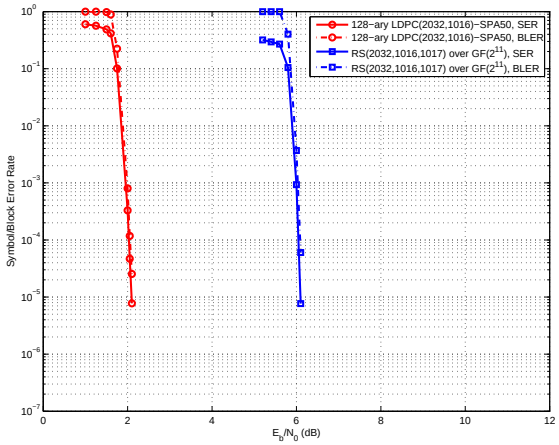

Fig. 3. Symbol and block error performances of the 128-ary $(2032, 1016)$ QC-LDPC code and the $(2032, 1016, 1017)$ shortened RS code over GF(2^{11}) over the AWGN channel.

B. *Array Dispersion*

The sizes of an RC-constrained array and its constituent circulant permutation matrices constructed based on a finite field depend on the size of the field. Using a large field for code construction results in long LDPC codes (especially high rate codes) with large symbol alphabet. Decoding of these codes requires very large computational complexity which makes decoder implementation impractical. Long nonbinary QC-LDPC codes over a small field can be constructed by array dispersion.

Array dispersion is best explained by considering a special case. Let $\mathbf{H}(5, 5k)$ be a $5 \times 5k$ subarray of an RC-constrained array $\mathbf{H}$ of $(2^m - 1) \times (2^m - 1)$ α-multiplied circulant permutation matrices over GF(2^m). Divide this array into k 5×5 subarrays, $\mathbf{H}_0(5, 5), \mathbf{H}_1(5, 5), \cdots, \mathbf{H}_{k-1}(5, 5)$, such that $\mathbf{H}(5, 5k) = [\mathbf{H}_0(5, 5) \ \mathbf{H}_1(5, 5) \cdots \mathbf{H}_{k-1}(5, 5)]$, where for $0 \leq i < k$,

$$\mathbf{H}_i(5, 5) = \begin{bmatrix} \mathbf{Q}_{0,0}^{(i)} & \mathbf{Q}_{0,1}^{(i)} & \mathbf{Q}_{0,2}^{(i)} & \mathbf{Q}_{0,3}^{(i)} & \mathbf{Q}_{0,4}^{(i)} \\ \mathbf{Q}_{1,0}^{(i)} & \mathbf{Q}_{1,1}^{(i)} & \mathbf{Q}_{1,2}^{(i)} & \mathbf{Q}_{1,3}^{(i)} & \mathbf{Q}_{1,4}^{(i)} \\ \mathbf{Q}_{2,0}^{(i)} & \mathbf{Q}_{2,1}^{(i)} & \mathbf{Q}_{2,2}^{(i)} & \mathbf{Q}_{2,3}^{(i)} & \mathbf{Q}_{2,4}^{(i)} \\ \mathbf{Q}_{3,0}^{(i)} & \mathbf{Q}_{3,1}^{(i)} & \mathbf{Q}_{3,2}^{(i)} & \mathbf{Q}_{3,3}^{(i)} & \mathbf{Q}_{3,4}^{(i)} \\ \mathbf{Q}_{4,0}^{(i)} & \mathbf{Q}_{4,1}^{(i)} & \mathbf{Q}_{4,2}^{(i)} & \mathbf{Q}_{4,3}^{(i)} & \mathbf{Q}_{4,4}^{(i)} \end{bmatrix}. \quad (7)$$

For $0 \leq i < k$, disperse $\mathbf{H}_i(5,5)$ into a 10×10 array $\mathbf{G}_i(10,10)$ as follow:

$$\mathbf{G}_i(10,10) =$$

$$\left[\begin{array}{ccccc|ccccc} \mathbf{Q}_{0,0}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & Q_{0,1}^{(i)} & \mathbf{Q}_{0,2}^{(i)} & \mathbf{Q}_{0,3}^{(i)} & \mathbf{Q}_{0,4}^{(i)} \\ \mathbf{Q}_{1,0}^{(i)} & \mathbf{Q}_{1,1}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{1,2}^{(i)} & \mathbf{Q}_{1,3}^{(i)} & \mathbf{Q}_{1,4}^{(i)} \\ \mathbf{Q}_{2,0}^{(i)} & \mathbf{Q}_{2,1}^{(i)} & \mathbf{Q}_{2,2}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{2,3}^{(i)} & \mathbf{Q}_{2,4}^{(i)} \\ \mathbf{Q}_{3,0}^{(i)} & \mathbf{Q}_{3,1}^{(i)} & \mathbf{Q}_{3,2}^{(i)} & \mathbf{Q}_{3,3}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{3,4}^{(i)} \\ \mathbf{Q}_{4,0}^{(i)} & \mathbf{Q}_{4,1}^{(i)} & \mathbf{Q}_{4,2}^{(i)} & \mathbf{Q}_{4,3}^{(i)} & \mathbf{Q}_{4,4}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{Q}_{0,1}^{(i)} & \mathbf{Q}_{0,2}^{(i)} & \mathbf{Q}_{0,3}^{(i)} & \mathbf{Q}_{0,4}^{(i)} & \mathbf{Q}_{0,0}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{Q}_{1,2}^{(i)} & \mathbf{Q}_{1,3}^{(i)} & \mathbf{Q}_{1,4}^{(i)} & \mathbf{Q}_{1,0}^{(i)} & \mathbf{Q}_{1,1}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{2,3}^{(i)} & \mathbf{Q}_{2,4}^{(i)} & \mathbf{Q}_{2,0}^{(i)} & \mathbf{Q}_{2,1}^{(i)} & \mathbf{Q}_{2,2}^{(i)} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{3,4}^{(i)} & \mathbf{Q}_{3,0}^{(i)} & \mathbf{Q}_{3,1}^{(i)} & \mathbf{Q}_{3,2}^{(i)} & \mathbf{Q}_{3,3}^{(i)} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{4,0}^{(i)} & \mathbf{Q}_{4,1}^{(i)} & \mathbf{Q}_{4,2}^{(i)} & \mathbf{Q}_{4,3}^{(i)} & \mathbf{Q}_{4,4}^{(i)} \end{array}\right], \tag{8}$$

where the 5×5 subarrays at the upper left and lower right quadrants of $\mathbf{G}_i(10,10)$ are identical and the 5×5 subarrays at lower left and upper right quadrants of $\mathbf{G}_i(10,10)$ are identical. The upper and lower half subarrays of $\mathbf{G}_i(10,10)$ correspond to $\mathbf{H}_i(5,5)$. Also the left and right half subarrays of $\mathbf{G}_i(10,10)$ correspond to $\mathbf{H}_i(5,5)$. Since $\mathbf{H}_i(5,5)$ satisfies the RC-constraint, all the above 4 half subarrays of $\mathbf{G}_i(10,10)$ satisfy the RC-constraint. From the structure of $\mathbf{G}_i(10,10)$, we can easily see that no 4 α-multiplied circulant permutation matrices from 4 different quadrants of $\mathbf{G}_i(10,10)$ are at the 4 corners of a rectangle. It follows from the above that $\mathbf{G}_i(10,10)$ satisfies the RC constraint. Each row (or column) of $\mathbf{G}_i(10,10)$ consists of a sequence of 5 consecutive $(2^m-1)\times(2^m-1)$ zero matrices between two α-multiplied circulant permutation matrices, including the *end around case*.

For each row of $\mathbf{G}_i(10,10)$, we replace the two α-multiplied circulant permutation matrices right behind the sequence of 5 consecutive zero matrices with two zero matrices. This results in the following 10×10 array $\mathbf{E}_i(10,10)$ of circulant permutation and zero matrices:

$$\mathbf{E}_i(10,10) =$$

$$\left[\begin{array}{ccccc|ccccc} \mathbf{Q}_{0,0}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{0,3}^{(i)} & \mathbf{Q}_{0,4}^{(i)} \\ \mathbf{Q}_{1,0}^{(i)} & \mathbf{Q}_{1,1}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{1,4}^{(i)} \\ \mathbf{Q}_{2,0}^{(i)} & \mathbf{Q}_{2,1}^{(i)} & \mathbf{Q}_{2,2}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{Q}_{3,1}^{(i)} & \mathbf{Q}_{3,2}^{(i)} & \mathbf{Q}_{3,3}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{Q}_{4,2}^{(i)} & \mathbf{Q}_{4,3}^{(i)} & \mathbf{Q}_{4,4}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{0,3}^{(i)} & \mathbf{Q}_{0,4}^{(i)} & \mathbf{Q}_{0,0}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{1,4}^{(i)} & \mathbf{Q}_{1,0}^{(i)} & \mathbf{Q}_{1,1}^{(i)} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{2,0}^{(i)} & \mathbf{Q}_{2,1}^{(i)} & \mathbf{Q}_{2,2}^{(i)} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{3,1}^{(i)} & \mathbf{Q}_{3,2}^{(i)} & \mathbf{Q}_{3,3}^{(i)} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{Q}_{4,2}^{(i)} & \mathbf{Q}_{4,3}^{(i)} & \mathbf{Q}_{4,4}^{(i)} \end{array}\right]. \tag{9}$$

Each row (or column) consists of a sequence of 7 consecutive $(q-1) \times (q-1)$ zero matrices, including the end around case. Since $\mathbf{E}_i(10,10)$ is obtained by replacing some of the α-multiplied circulant permutation matrices of $\mathbf{G}_i(10,10)$ by zero matrices, it also satisfies the RC-constraint.

Form the following $10 \times 10k$ array of α-multiplied circulant permutation and zero matrices:

$$\mathbf{E}(10,10k) = \left[\, \mathbf{E}_0(10,10) \;\; \mathbf{E}_1(10,10) \;\; \cdots \;\; \mathbf{E}_{k-1}(10,10) \,\right]. \tag{10}$$

$\mathbf{E}(10,10k)$ is a $10(q-1) \times 10k(q-1)$ matrix over GF(q) with column and row weights 3 and $3k$, respectively. The null space of $\mathbf{E}(10,10k)$ gives a $(3,3k)$-regular QC-LDPC code $\mathcal{C}_{dis}$.

Example 4: Let GF(2^4) be the code construction field. Using the second construction method given in Section III, we constructed a 15×15 array $\mathbf{H}^{(2)}$ of 15×15 α-multiplied circulant permutation and zero matriices. Choose $k = 2$. Take a 5×10 subarray $\mathbf{H}^{(2)}(5,10)$ from $\mathbf{H}^{(2)}$ that does not contain zero matrices. Dispersing $\mathbf{H}^{(2)}$ based on (8) to (10), we obtain a 10×20 dispersed array $\mathbf{E}(10,20) = [\mathbf{E}_0(10,10) \; \mathbf{E}_0(10,10)]$ which is a 150×300 matrix with column and row weights 3 and 6, respectively. The null space of $\mathbf{E}(10,20)$ gives a 16-ary $(300,150)$ QC-LDPC code. The block error performance of this code decoded with the FFT-QSPA is shown in Figure 4. Also included in Figure 4 are the block error performances of the $(300,150,151)$ shortened RS code over GF(2^9) with the hard-decision BM and the algebraic soft-decision KV decodings. At the BLER of 10^{-5}, the 16-ary $(300,150)$ QC-LDPC code achieves a 3.6 dB coding gain over the corresponding RS code with the hard-decision BM decoding, while achieves a 2.9 dB and a 2.3 dB coding gains over the RS code using the algebraic soft-decision KV decoding with MIM λ equal to 4.99 and infinity, respectively.

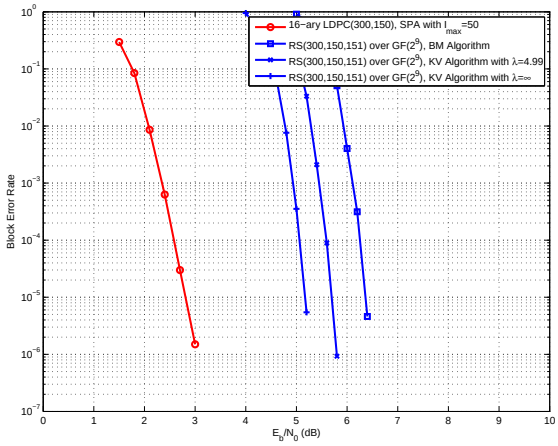

Fig. 4. Block error performances of the 16-ary $(300,150)$ QC-LDPC code and the $(300,150,151)$ shortened RS code over GF(2^9) over the AWGN channel.

The above code construction based on dispersion of a $5 \times 5k$ array of α-multiplied circulant permutation matrices can be easily generalized. Let $\mathbf{H}(l,kl)$ be an RC-constrained $l \times kl$ array of $(2^m-1)\times(2^m-1)$ α-multiplied circulant permutation

matrices over GF(2^m). Divide $\mathbf{H}(l, kl)$ into k subarrays of size $l \times l$, $\mathbf{H}_0(l, l), \mathbf{H}_1(l, l), \cdots, \mathbf{H}_{k-1}(l, l)$, each consisting l consecutive columns of α-multiplied circulant permutation matrices of $\mathbf{H}(l, kl)$. For $0 \leq i < k$, disperse $\mathbf{H}_i(l, l)$ into a $2l \times 2l$ array $\mathbf{G}_i(2l, 2l)$ of α-multiplied circulant permutation and zero matrices in the form given by (8). Then each row (or each column) of $\mathbf{G}_i(2l, 2l)$ contains a unique sequence of l consecutive zero matrices with an α-multiplied circulant permutation matrix before it and an α-multiplied circulant permutation matrix after it(including the end around case). Let e be a positive integer such that $0 \leq e \leq l - 3$. We replace the e α-multiplied circulant permutation matrices right behind the sequence of l consecutive zero matrices in each row of $\mathbf{G}_i(2l, 2l)$(including the end around case). This results in a $2l \times 2l$ array $\mathbf{E}_i(2l, 2l)$ in which each row (or column) consists of a unique $l+e$ consecutive zero matrices. Form the following $2l \times 2kl$ array of α-multiplied circulant permutation and zero matrices:

$$\mathbf{E}(2l, 2kl) = \left[\mathbf{E}_0(l, l) \ \mathbf{E}_1(l, l) \ \cdots \ \mathbf{E}_{k-1}(l, l) \right]. \qquad (11)$$

$\mathbf{E}(2l, 2kl)$ is a $2l(2^m - 1) \times 2kl(2^m - 1)$ matrix over GF(2^m) with column and row weights $l - e$ and $k(l - e)$, respectively, and it satisfies the RC-constraint. The null space over GF(2^m) of $\mathbf{E}(2l, 2kl)$ gives a 2^m-ary $(l-e, k(l-e))$-regular QC-LDPC code $\mathcal{C}_{dis}$. For $e = l - 3$, $\mathcal{C}_{dis}$ is a 2^m-ary $(3, 3k)$-regular QC-LDPC code. The above construction by array dispersion results in large class of nonbinary QC-LDPC codes.

The length of the *zero covering span* [11], [12] of $\mathbf{E}(2l, 2kl)$ is at least $(l + e)(q - 1)$. Using $\mathbf{E}(2l, 2kl)$ for decoding, the code $\mathcal{C}_{dis}$ given by the null space of $\mathbf{E}(2l, 2kl)$ is capable of correcting any burst of symbol erasures of length at least up to $(l+e)(q-1)+1$ using the iterative decoding given in [11]. The 16-ary (300,150) QC-LDPC code given in Example 4 is capable of correcting any burst of 16-ary symbol erasures of length at least up to $7 \times 15 + 1 = 106$.

V. CONCLUSION

In this paper, we have extended our previous work [1] on algebraic constructions of nonbinary QC-LDPC codes. New methods and new classes of nonbinary QC-LDPC codes have been presented. Codes given in the Examples perform very well with iterative decoding using the FFT-QSPA and they achieve significant coding gains over RS codes of the same length and rates decoded with either the algebraic hard-decision BM decoding or the algegraic soft-decision KV decoding at the expense of larger computational complexity. An interesting question is "Whether they can replace RS codes in some applications?".

REFERENCES

[1] S. Lin, S. Song, L. Lan, L. Zeng, and Y.Y. Tai, "Constructions of nonbinary quasi-cyclic LDPC codes: A finite field approach," *Inaugural Workshop for the Center of Information Theory and its Applications*, UCSD division of Calit2 and the Jacobs School of Engineering, San Diego, California, Feb. 2006.

[2] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

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

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

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

[6] L. Barnault and D. Derlercq, "Fast decoding algorithm for LDPC codes over GF(2^q)," *Proc. ITW2003*, pp. 70-73, Paris, France, Mar. 31-Apr. 4, 2003.

[7] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," to appear *IEEE Trans. Commun.*, 2007.

[8] W.J. Gross, F.R. Kschischang, R. Köetter, 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.

[9] L. Chen, I. Djurdjevic, J. Xu, S. Lin, and K. Abdel-Ghaffar, "Construction of quasi-cyclic LDPC codes based on the minimum-weight codewords of Reed-Solomon codes," *Proc. IEEE Int. Symp. Inform. Therory*, p. 239, Chicago, IL, Jun./Jul. 2004.

[10] 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.

[11] S. Song, S. Lin, and K. Abdel-Ghaffar, "Burst-correction decoding of cyclic LDPC codes," *Proc. IEEE Int. Symp. Inform. Theory*, pp. 1718-1722, Seattle, WA, Jul. 2006.

[12] Y.Y. Tai, L. Lan, L. Zeng, S. Lin, and K. 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.