Quasi-Cyclic LDPC Codes: 
Construction and Rank Analysis of Their 
Parity-Check Matrices

Keke Liu\textsuperscript{1}, Qin Huang\textsuperscript{2}, Shu Lin\textsuperscript{1} and Khaled Abdel-Ghaffar\textsuperscript{1}

\textsuperscript{1}Department of Electrical and Computer Engineering
University of California
Davis, CA 95616
(e-mail: kkeliu@ucdavis.edu, shulin@ece.ucdavis.edu, ghaffar@ece.ucdavis.edu)

\textsuperscript{2}School of Electronic and Information Engineering
Beihang University
Beijing 100083, China
(e-mail: qhuang.smash@gmail.com).

Abstract—A construction of binary and non-binary quasi-cyclic (QC)-LDPC codes based on partitions of finite fields of characteristic 2 is proposed. The construction is carried out in the Fourier transform domain. The parity-check matrices of these QC-LDPC codes are arrays of circulant permutation matrices. The ranks of these arrays are analyzed and combinatorial expressions are derived. Example codes are given and simulations show that they perform well over the AWGN channel decoded with message-passing decoding algorithms.

I. INTRODUCTION

The ever-growing needs for cheaper, faster, and more reliable communication systems have forced many researchers to seek means to attain the ultimate limits on reliable communications. Low-density parity-check (LDPC) codes are currently the most promising coding technique to achieve the Shannon capacities for a wide range of channels. These codes were first discovered by Gallager in 1962 [1] and then rediscovered in the late 1990’s [2],[3]. Ever since their rediscovery, a great deal of research effort has been expended in design, construction, structural and performance analysis, encoding, decoding, generalizations, and applications of LDPC codes. Numerous papers have been published on these subjects. Many LDPC codes have been chosen as the standard codes for various next generations of communication systems and they are appearing in recent data storage products. More applications are expected to come.

Major methods for constructing LDPC codes can be divided into two general categories: graph-theoretic-based methods and algebraic methods. Each type of constructions has its advantages and disadvantages in terms of overall error performance, encoding and decoding implementations. In general, algebraically constructed LDPC codes have lower error-floors and their decoding using iterative message-passing algorithms, such as the sum-product algorithm (SPA) and the min-sum algorithm (MSA), converges faster than the graph-theoretic-based codes constructed by computer search. Furthermore, it is much easier to construct algebraic LDPC codes with large minimum distances. Algebraic constructions of LDPC codes are mainly based on finite fields, finite geometries, and combinatorial designs. These constructions result in mostly quasi-cyclic (QC)-LDPC codes.

QC-LDPC codes have advantages over other types of LDPC codes in hardware implementation of encoding and decoding. Encoding of a QC-LDPC code can be efficiently implemented using simple shift registers with complexity linearly proportional to its number of parity-check symbols (or its length) [4]. In hardware implementation of its decoder, the quasi-cyclic structure of the code (or circular structure of its parity-check matrix) simplifies the wire routing for message passing [5] and allows partially parallel decoding [6] which offers a trade off between decoding complexity and decoding speed. Well designed or constructed QC-LDPC code can perform as well as any other types of LDPC codes. Major methods for constructing QC-LDPC codes are given in [7]–[16].

A q-ary QC-LDPC code is given by the null space of an array $H$ of sparse circulant matrices of the same size over the field $\text{GF}(q)$ where $q$ is a power of prime. If the array $H$, viewed as a matrix, has constant column weight $\gamma$ and constant row weight $\rho$, the code given by the null space of $H$ is said to be $(\gamma, \rho)$-regular, otherwise it is said to be irregular.

In almost all of the proposed constructions of LDPC codes (quasi-cyclic or not), the following constraint on the rows and columns of the parity-check matrix $H$ is imposed: no two rows (or two columns) can have more than one place where they both have identical non-zero components. This constraint on the rows and columns of $H$ is referred to as the row-column (RC)-constraint. This RC-constraint ensures that the Tanner graph of the LDPC code given by the null space of $H$ has a girth of at least 6 and that the minimum distance of the code, if $(\gamma, \rho)$-regular, is at least $\gamma + 1$ [7], [17]. The distance bound
is tight for regular LDPC codes whose parity-check matrices have large column weights and row redundancies, such as the algebraic LDPC codes constructed using finite fields, finite geometries, and combinatorial designs. A parity-check matrix $H$ that satisfies the RC-constraint is called an RC-constrained parity-check matrix and the code given by its null space is called an RC-constrained LDPC code.

In most of the constructions of binary QC-LDPC codes, the parity-check matrix of a code is an RC-constrained array of circulant permutation matrices (CPMs) and/or zero matrices (ZMs) over $\text{GF}(2)$. In a recent paper [18], we showed that the Fourier transform of an RC-constrained array $H$ of CPMs and/or ZMs of size $(2^r - 1) \times (2^r - 1)$ over $\text{GF}(2)$ followed by appropriate column and row permutations result in a diagonal array $H^F \pi = \text{diag}(B^{\circ 0}, B^{\circ 1}, B^{\circ 2}, \ldots, B^{\circ (2^r-2)})$ of matrices of the same size over $\text{GF}(2^r)$ which consists of a base matrix $B = B^{\circ 1}$ and its Hadamard powers, $B^{\circ 0}, B^{\circ 1}, B^{\circ 2}, \ldots, B^{\circ (2^r-2)}$, where the $t$-th Hadamard power $B^{\circ t}$ of $B$ is defined as the Hadamard product of $t$ copies of $B$ [19]. The superscript $F$ of $H$ represents the Fourier transform operation applied to $H$ and $\pi$ represents the overall column and row permutations applied to the Fourier transform $H^F$ of $H$. This is to say that in the Fourier transform domain, the array $H$ is uniquely specified by the base matrix $B$.

The base matrix $B$ satisfies the constraint that every $2 \times 2$ submatrix contains at least one zero entry or is non-singular. This constraint on the $2 \times 2$ submatrices of $B$ is referred to as the $2 \times 2$ submatrix constraint (SM-constraint). In the same paper, we also showed that if a base matrix $B$ that satisfies the $2 \times 2$ SM-constraint is given, an RC-constrained binary array $H$ of CPMs and/or ZMs can be constructed by column and row permutations followed by inverse Fourier transforms of the diagonal matrix $\text{diag}(B^{\circ 0}, B^{\circ 1}, B^{\circ 2}, \ldots, B^{\circ (2^r-2)})$. Then the null space of $H$ gives an RC-constrained binary QC-LDPC code.

Therefore, construction of RC-constrained binary parity-check matrices of QC-LDPC codes is equivalent to construction of base matrices over $\text{GF}(2^r)$ that satisfy the $2 \times 2$ SM-constraint. Since the size of a base matrix $B$ is much smaller than the size of its corresponding array $H$, construction of a $2 \times 2$ SM-constrained base matrix is much easier than direct construction of an RC-constrained array of CPMs and/or ZMs. Furthermore, it is much easier to determine the rank of an RC-constrained array $H$ in the Fourier transform domain. This is done by adding the ranks of the base matrix $B$ and its Hadamard powers. For several classes of base matrices constructed from finite fields and combinatorial designs, we were able to derive combinatorial expressions for the ranks of their corresponding RC-constrained arrays of CPMs and/or ZMs.

This paper is concerned with the construction of binary and non-binary QC-LDPC codes in Fourier transform domain. First, we present a class of $2 \times 2$ SM-constrained base matrices which are constructed based on partitions of finite fields of characteristic 2. Based on this class of base matrices, we construct a class of RC-constrained arrays of CPMs and ZMs over $\text{GF}(2)$ whose null spaces give a new class of RC-constrained binary QC-LDPC codes. Then, we analyze the ranks of the arrays in this class. Using the same base matrices, we show that RC-constrained non-binary arrays of CPMs of a special type and/or ZMs over $\text{GF}(2^r)$ can also be constructed. The null spaces of these arrays give a class of $2^r$-ary QC-LDPC codes. Examples are given to show that the codes constructed perform well over the AWGN channel decoded with either the SPA or the MSA.

II. CONSTRUCTION OF A CLASS OF BINARY QC-LDPC CODES BASED ON FIELD PARTITIONS

In this section, we present a new algebraic method for constructing a class of QC-LDPC codes. Given a finite field, we first arbitrarily partition the elements of the field into two disjoint subsets. Based on these two disjoint subsets, we form a base matrix over the given field. Every entry of the matrix is a sum of two elements, one from the first subset and the other from the second subset. From this matrix, we can form an array of CPMs. This array, as a matrix, satisfies the RC-constraint. Then, the null space of this array gives a QC-LDPC code.

A. A Class of $2 \times 2$ SM-Constrained Base Matrices Constrained by Field Partitions

Let $\text{GF}(2^r)$ be a finite field with $2^r$ elements which is an extension field of the binary field $\text{GF}(2)$. Let $\alpha$ be a primitive element of $\text{GF}(2^r)$. Then, the powers of $\alpha$, $\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}$, give all the elements of $\text{GF}(2^r)$ and $\alpha^{2^r-1} = 1$. Let $m$ and $n$ be two positive integers such that $m + n = 2^r$. Partition the elements of $\text{GF}(2^r)$ into two disjoint subsets: $G_1 = \{\lambda_0, \lambda_1, \ldots, \lambda_{m-1}\}$ and $G_2 = \{\delta_0, \delta_1, \ldots, \delta_{n-1}\}$, i.e., $G_1 \cup G_2 = \text{GF}(2^r)$ and $G_1 \cap G_2 = \emptyset$. Form the following $m \times n$ matrix over $\text{GF}(2^r)$:

$$
B = \begin{bmatrix}
\lambda_0 + \delta_0 & \lambda_0 + \delta_1 & \cdots & \lambda_0 + \delta_{n-1} \\
\lambda_1 + \delta_0 & \lambda_1 + \delta_1 & \cdots & \lambda_1 + \delta_{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_{m-1} + \delta_0 & \lambda_{m-1} + \delta_1 & \cdots & \lambda_{m-1} + \delta_{n-1}
\end{bmatrix}
$$

We note that each row of $B$ is formed by adding an element in $G_1$ to all the $n$ elements in $G_2$ and each column of $B$ is formed by adding an element in $G_2$ to all the $m$ elements in $G_1$. Since the characteristic of the field $\text{GF}(2^r)$ is 2, every element in $\text{GF}(2^r)$ is its own additive inverse. It follows from the fact that $G_1$ and $G_2$ are disjoint and the formation of $B$ that: (1) all the entries in $B$ are nonzero; (2) all the entries in a row of $B$ are different; and (3) all the entries in a column of $B$ are different. Every entry in $B$ is a power of the primitive element $\alpha$ of $\text{GF}(2^r)$. In the following, we prove that the $m \times n$ matrix $B$ over $\text{GF}(2^r)$ given by (1) satisfies the $2 \times 2$ SM-constraint.

**Theorem 1.** The $m \times n$ matrix $B$ over $\text{GF}(2^r)$ given by (1) satisfies the $2 \times 2$ SM-constraint.
whose Tanner graph has a girth at least 6. Note that the null space of $H$ of length $2^r-2$ of (2), \( B^{2^l} \) is an RC-constrained binary array, the rank of $H$ is then given by the sum of the ranks of the base matrix $B$ and its Hadamard powers:

$$
\text{rank}(H) = \text{rank}(H^{F,\pi}) = \sum_{l=0}^{2^r-2} \text{rank}(B^{2^l}).
$$

Suppose the matrix given by (1) is used as the base matrix $B$. Then, $B^{2^l} = [(\lambda_i + \delta_j)]_{0 \leq i < m}$, $0 \leq j < n$, for $0 \leq l < 2^r-1$. In the binomial expansion of \( \lambda_i + \delta_j \) (or the number of odd integers in the $l$-th level of Pascal triangle), let $t_1, t_2, \ldots, t_{\mu_l}$ denote the positions of these odd coefficients. We note that $t_1 = 0$ and $t_{\mu_l} = l$. Then

$$
(\lambda_i + \delta_j)^l = \lambda_i^{l-t_1} \delta_j^{t_1} + \lambda_i^{l-t_2} \delta_j^{t_2} + \lambda_i^{l-t_3} \delta_j^{t_3} + \cdots + \lambda_i^{l-t_{\mu_l} - 1} \delta_j^{t_{\mu_l} - 1} + \delta_j^l.
$$

(4) Based on the expression given by (4), the $l$-th Hadamard power $B^{2^l}$ can be expressed as a product of two matrices as follows:

$$
B^{2^l} = V_{l,L}V_{l,R}
$$

with

$$
V_{l,L} = \begin{bmatrix}
\lambda_0^l & \lambda_1^l & \lambda_2^l & \cdots & \lambda_{m-1}^l \\
\delta_0^l & \delta_1^l & \delta_2^l & \cdots & \delta_{n-1}^l \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\delta_0^{\mu_l} & \delta_1^{\mu_l} & \delta_2^{\mu_l} & \cdots & \delta_{n-1}^{\mu_l}
\end{bmatrix}
$$

(6) where $V_{l,L}$ is an $m \times \mu_l$ matrix over $GF(2^r)$ and $V_{l,R}$ is a $\mu_l \times n$ matrix over $GF(2^r)$. Let $\omega(l)$ be the number of nonzero terms in the radix-$2$ expansion (or binary representation) of $l$, called the radix-$2$ weight of $l$. It follows from Lucas theorem [20] that $\mu_l = 2^{\omega(l)}$. For $0 \leq l < 2^{r-1}$, since $\mu_l \leq l+1 < 2^r$, we must have $\omega(l) < r$ and $\mu_l \leq 2^{r-1}$.

To determine the rank of $B^{2^l}$, we will determine the ranks of $V_{l,L}$ and $V_{l,R}$. This can be done in the following case: the nonzero elements of both $G_1$ and $G_2$ form two sequences of consecutive powers of $\alpha$. The 0 element can be in either $G_1$ or $G_2$. For example, $G_1 = \{0, \alpha^0, \alpha, \ldots, \alpha^{m-2}\}$ and $G_2 = \{\alpha^{m-1}, \alpha^m, \ldots, \alpha^{2r-2}\}$. Let $n = 2^r - m$. We also assume that $m \leq 2^{r-1} \leq n$. In this case, $V_{l,L}$ and $V_{l,R}$ can be transformed into matrices with the Vandermonde structure [20],[21] by elementary column and row operations. Since $m \leq n$, then $n \geq 2^{r-1} \geq \mu_l$. As a result, \( \text{rank}(V_{l,L}) = \min(m, \mu_l) \) and \( \text{rank}(V_{l,R}) = \mu_l \). It follows from (6) that
$$\text{rank}(B^{ol}) = \text{rank}(V_{l,R} V_{l,L})$$. Since $V_{l,R}$ has full row rank, $\text{rank}(B^{ol}) = \text{rank}(V_{l,L} V_{l,R}) = \text{rank}(V_{l,L}) = \min(m, \mu_l)$ (7) for $0 \leq l < 2^r - 1$. For $l = 0$, all the entries of $B^{ol}$ are equal to 1. Hence, the rank of $B^{ol}$ is 1, i.e., $\text{rank}(B^{ol}) = 1$. Then, it follows from (3) and (7) that the rank of $H$ is:

$$\text{rank}(H) = 1 + \sum_{l=1}^{2^r-2} \text{rank}(B^{ol}).$$

(8)

Let $\omega_0$ be the largest integer such that $2^{\omega_0} \leq m$, then a combinatorial expression for the sum of terms given by (8) can be derived as follows:

$$\sum_{l=1}^{2^r-2} \text{rank}(B^{ol}) = \sum_{l=1}^{2^r-2} \min(m, \mu_l)
= \sum_{1 \leq \omega \leq 2^r-2} \sum_{l \leq 2^r-2} m + \mu_l
= \sum_{\omega=\omega_0+1}^{\omega_0} \sum_{l=1}^{2^r-2} \omega
= \sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) m + \sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) 2^\omega
= \sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) m + \sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) 2^\omega - \sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) 2^\omega.$$

Note that $\sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) 2^\omega = 3^r - 2^r - 1$. Consequently, we have

$$\sum_{l=1}^{2^r-2} \text{rank}(B^{ol}) = 3^r - 2^r - 1 - \sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) (2^\omega - m).$$

(9)

Combining (8) and (9), we have the following combinatorial expression for the rank of $H$ with $m \leq 2^{r-1}$:

$$\text{rank}(H) = 3^r - 2^r - \sum_{\omega=\omega_0+1}^{\omega_0} \left( \sum_{l=1}^{r} \omega \right) (2^\omega - m).$$

(10)

For $m = 2^{r-1} = n$, the base matrix given by (1) is a square matrix and its corresponding array $H_x$ is a $2^{r-1} \times 2^{r-1}$ array of $(2^r - 1) \times (2^r - 1)$ CPMs. In this case, $\omega_0 = r - 1$ and

$$\text{rank}(H_x) = 3^r - 2^r.$$

(11)

The null space of $H_x$ gives a binary QC-LDPC code with the following parameters: (1) length $n = 2^{r-1} (2^r - 1)$; (2) dimension $k = 2^{2r-1} + 2^{r-1} - 3^r$; (3) minimum distance $d_{\text{min}}$ is at least $2^{2r-1} + 1$. The null space of any sub-array of $H_x$ gives a QC-LDPC code.

The above derivation of $\text{rank}(H)$ is for the case $m \leq 2^{r-1}$. For $m > 2^{r-1}$, the derivation of $\text{rank}(H)$ is similar.

In the following, we give two examples to demonstrate the performances of two QC-LDPC codes constructed based on field partitions given in Subsection II.B. We assume BPSK transmission of the AWGN channel. Decoding is carried out either with the SPA or the MSA.

**Example 1.** Let $GF(2^k)$ be the field for construction. Let $\alpha$ be a primitive element of $GF(2^k)$. Partition $GF(2^k)$ into two subsets: $G_1 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ and $G_2 = \{\alpha^5, \alpha^6, \ldots, \alpha^{126}\}$. Using these two subsets of $GF(2^k)$, we can construct a $6 \times 58$ base matrix $B$ over $GF(2)$ of the form given in (1). Array dispersion of this base matrix results in a $6 \times 58$ array $H$ of $63 \times 63$ CPMs. $H$ is a $378 \times 3654$ RC-constrained matrix over $GF(2)$ with column and row weights 6 and 58, respectively. Since $m = 6$, we find that $\omega_0 = 2$. Using the combinatorial expression given by (10), we find that the rank of $H$ is 319. Hence, the null space of $H$ gives a $(6, 58)$-regular (3654, 3335) QC-LDPC code of rate 0.9127. The bit and block error performances of the code decoded with 5, 10 and 50 iterations of the MSA are shown in Figure 1. We see that the decoding of the code converges fast. At the BER of $10^{-6}$, the code decoded with 50 iterations of the MSA performs 1.2 dB from the Shannon limit. At the BLER (block error rate) $10^{-5}$, it performs 0.8 dB from the sphere packing bound.

**Example 2.** In this example, we construct a longer code. The field chosen for code construction is $GF(2^7)$. Let $\alpha$ be a primitive element of $GF(2^7)$. Partition the elements of the field into two disjoint subsets: $G_1 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ and $G_2 = \{\alpha^5, \alpha^6, \ldots, \alpha^{126}\}$. Based on these two disjoint subsets of $GF(2^7)$, we construct a $6 \times 122$ base matrix $B$ over $GF(2^7)$ of the form given in (1). Disperse $B$ into a $6 \times 122$ array $H$ of $127 \times 127$ CPMs. This array $H$ is a $762 \times 15494$ RC-constrained matrix over $GF(2)$ with column and row weights 6 and 122, respectively. Since $m = 6$, the largest positive integer $\omega_0$ such that $2^{\omega_0} \leq 6$ is 2. Using the combinatorial expression given by (10), we find that the rank of $H$ is 687. The null space of this array gives a binary RC-constrained $(6, 122)$-regular (15494, 14807) QC-LDPC code of rate 0.9557 whose Tanner graph has a girth of at least 6. The bit and block error rates of this code with 50 iterations of the SPA are shown in Figure 2. At the BER of $10^{-8}$, the code performs 0.92 dB from the Shannon limit.
IV. NON-BINARY QC-LDPC CODES

In this section, we show that RC-constrained arrays of non-binary CPMs of a special type can also be constructed using the base matrices constructed in Section II. The null spaces of these arrays give a class of non-binary QC-LDPC codes. Again we consider code construction based on fields of characteristic 2. Let $\alpha$ be a primitive element of $\text{GF}(2^r)$. For $0 \leq k < 2^r - 1$, let $P(\alpha^k)$ be a $(2^r - 1) \times (2^r - 1)$ matrix over $\text{GF}(2^r)$ with columns and rows labeled from 0 to $2^r - 2$ which has the following structures: (1) the top row of $P(\alpha^k)$ has a single nonzero component with value $\alpha^k$ at the $k$-th position; and (2) every row of $P(\alpha^k)$ is the cycle-shift (one place to the right) of the row above it multiplied by $\alpha$ and the first row is the cycle-shift of the last row multiplied by $\alpha$. This $(2^r - 1) \times (2^r - 1)$ matrix $P(\alpha^k)$ over $\text{GF}(2^r)$ is called an $\alpha$-multiplied CPM. There are $2^r - 1$ such $\alpha$-multiplied CPMs. For $0 \leq k < 2^r - 1$, we represent the element $\alpha^k$ of $\text{GF}(2^r)$ by the $\alpha$-multiplied CPM $P(\alpha^k)$.

This representation, which is one-to-one, is referred to as the $\alpha$-multiplied CPM dispersion (or simply dispersion) of $\alpha^k$. Next, we replace each entry of the $m \times n$ base matrix $B$ given by (1) by its corresponding $\alpha$-multiplied CPM. This results in an $m \times n$ array $H_\alpha$ of $\alpha$-multiplied CPMs of size $(2^r - 1) \times (2^r - 1)$. The array $H_\alpha$ consists of $n$ column blocks of $\alpha$-multiplied CPMs, denoted $H_{\alpha,0}, H_{\alpha,1}, \ldots, H_{\alpha,n-1}$. Each column block $H_{\alpha,j}$ of $\alpha$-multiplied CPMs with $0 \leq j < n$ is an $(m(2^r - 1) \times (2^r - 1))$ matrix over $\text{GF}(2^r)$. Due to the structure of an $\alpha$-multiplied CPM, all the nonzero elements in the $k$-th column of $H_{\alpha,j}$ are $\alpha^k$ for $0 \leq k < 2^r - 1$ and $0 \leq j < n$. We call $\alpha^k$ the value of the $k$-th column of $H_{\alpha,j}$. View the overall array $H_\alpha$ as an $m(2^r - 1) \times n(2^r - 1)$ matrix over $\text{GF}(2^r)$. If we multiply each column of $H_\alpha$ by the multiplicative inverse of its value, we obtain the binary array $H$ of CPMs constructed from the base matrix $B$ as given in Section II. Therefore, the rank of $H_\alpha$ is the same as that of $H$, i.e., $\text{rank}(H_\alpha) = \text{rank}(H)$.

If the base matrix $B$ is constructed based on two disjoint subsets, $G_1$ and $G_2$, of consecutive powers of $\alpha$, then the combinatorial expression given by (10) also gives the rank of $H_\alpha$. Furthermore, the $2 \times 2$ SM-constraint on $B$ also ensures that $H_\alpha$ satisfies the RC-constraint. The null space of $H_\alpha$ gives a $2^r$-ary QC-LDPC code whose Tanner graph has a girth of at least 6. The above construction gives a class of regular $2^r$-ary QC-LDPC codes.

Example 3. Let $\text{GF}(2^5)$ be the field for code construction and $\alpha$ be a primitive element of the field. Partition the elements of $\text{GF}(2^5)$ into two disjoint subsets: $G_1 = \{0, 1, \alpha, \alpha^2\}$ and $G_2 = \{\alpha^3, \alpha^4, \ldots, \alpha^{30}\}$. Based on these two subsets of $\text{GF}(2^5)$, we form a $4 \times 28$ base matrix $B$ over $\text{GF}(2^5)$ of the form given by (1). Replacing each entry in $B$ by its corresponding $\alpha$-multiplied CPM of size $31 \times 31$, we obtain a $4 \times 28$ array $H_\alpha$ of $\alpha$-multiplied CPMs of size $31 \times 31$. $H_\alpha$ is a $124 \times 868$ RC-constrained matrix over $\text{GF}(2^5)$ with column and row weights 4 and 28, respectively. Since $m = 4$, the parameter $\omega_0$ is 2. Using the combinatorial expression given by (10), we find that the rank of $H_\alpha$ is 111. The null space of $H_\alpha$ gives a $(4,28)$-regular $32$-ary $(868,757)$ QC-LDPC code of rate 0.8721. The bit, symbol, and block error performances of this code decoded with 50 iterations of Fast Fourier Transform q-ary SPA (FFT-QSPA) are shown in Figure 3. At the BLER of $10^{-4}$, the code performs 1.8 dB from the sphere packing bound.

V. MASKING

Let $B = [b_{i,j}]$, $0 \leq i < m$ and $0 \leq j < n$, denote the base matrix over $\text{GF}(2^r)$ given by (1) where $b_{i,j} = \lambda_i + \delta_j$. Let $Z(m, n) = [z_{i,j}]$, $0 \leq i < m$ and $0 \leq j < n$, be an $m \times n$ matrix over $\text{GF}(2)$ with both 0 and 1 entries. Take the Hadamard product of $Z(m, n)$ and $B$, $B_{\text{mask}} = Z(m, n) \odot B = [z_{i,j}b_{i,j}]$, $0 \leq i < m, 0 \leq j < n$, where $z_{i,j}b_{i,j} = b_{i,j}$ if $z_{i,j} = 1$ and $z_{i,j}b_{i,j} = 0$ if $z_{i,j} = 0$. This product simply replaces a set of nonzero entries of $B$ by a set of zeros. This operation is called masking. $Z(m, n)$ and $B_{\text{mask}}$ are called the masking matrix and the masked base matrix, respectively. The masked base matrix also satisfies the $2 \times 2$ SM-constraint. Let
Let $H_{\text{mask}}$ and $H_{\alpha, \text{mask}}$ be the binary and $\alpha$-multiplied array dispersions of $B_{\text{mask}}$. Then the null spaces of $H_{\text{mask}}$ and $H_{\alpha, \text{mask}}$ give a binary and a 2$^\alpha$-ary QC-LDPC codes. Masking reduces the density of CPMs (or $\alpha$-multiplied CPMs) in $H$ (or in $H_{\alpha}$). This may reduce the number of short cycles in the Tanner graph of the code given by the null space of $H_{\text{mask}}$ (or $H_{\alpha, \text{mask}}$) or even increase the girth of the Tanner graph of the code. As a result, the performance of the code may be improved. As shown in [11], masking is very effective in constructing irregular QC-LDPC code. This is illustrated by the following example.

**Example 4.** Again, let $GF(2^7)$ be the field for code construction and $\alpha$ be a primitive element of the field. Partition the elements into two subsets: $G_1 = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{30}\}$ and $G_2 = \{\alpha^{31}, \alpha^{32}, \ldots, \alpha^{120}\}$. Based on these two subsets, we form a $32 \times 96$ base matrix $B$ over $GF(2^7)$ of the form given by (1). Take the first 64 columns of $B$ to form a $32 \times 64$ subarray $B(32, 64)$. We use the sub-array $B(32, 64)$ as the base matrix for masking to construct an irregular QC-LDPC code. Design a $32 \times 64$ masking matrix $Z(32, 64) = [z_{ij}], 0 \leq i < 32, 0 \leq j < 64$, over $GF(2)$ with column and row weight distributions close to the following variable node and check-node degree distributions (node perspective) of a Tanner graph which is designed for an irregular code of rate 0.5 [11]:

$$v(X) = 0.4554X + 0.3433X^2 + 0.1603X^7 + 0.0409X^{29},$$

$$c(X) = 0.1003X^7 + 0.8997X^8,$$

where the coefficient of $X^i$ represents the percentage of nodes with degree $i + 1$. The masking matrix $Z(32, 64)$ has 32 columns of degree 2, 20 columns of degree 3, 9 columns of degree 8, 3 columns of degree 30, 2 rows of degree 8, and 30 rows of degree 9. Masking the base matrix $B(32, 64)$ with $Z(32, 64)$ yields the masked matrix $B_{\text{mask}}(32, 64) = Z(32, 64) \circ B(32, 64)$. Next we use $B_{\text{mask}}(32, 64)$ as the base matrix and construct a $32 \times 64$ binary array $H_{\text{mask}}(32, 64)$ of CPMs and ZMs of size $127 \times 127$. $H_{\text{mask}}(32, 64)$ is a 4064 by 8128 matrix over $GF(2)$ with column and row weight distributions close to the degree distributions given above. The null space of $H_{\text{mask}}(32, 64)$ gives an irregular (8128,4064) QC-LDPC code of rate 0.5. The error performance of this irregular QC-LDPC code over the AWGN channel with 50 iterations of the SPA is shown in Figure 4. At the BER of $10^{-6}$, the code performs 1 dB from the Shannon limit and at the BLER of $10^{-5}$, it performs 0.6 dB from the sphere packing bound.

**VI. CONCLUSION**

In this paper, constructions of both binary and non-binary QC-LDPC codes were presented. The constructions were carried out in Fourier transform domain. First, we presented a class of $2 \times 2$ SM-constrained base matrices which are constructed based on partitions of finite fields of characteristic 2. Dispersing the base matrices in this class, we obtained a class of RC-constrained binary arrays of CPMs and a class of RC-constrained non-binary arrays of $\alpha$-multiplied CPMs. Array dispersion of a base matrix is equivalent to column and row permutations of the base matrix and its Hadamard powers followed by inverse Fourier transform. The null spaces of two classes of arrays give two classes of RC-constrained QC-LDPC codes, one binary and the other non-binary. Fourier transform approach to code construction allowed us to analyze the ranks of the arrays in both classes. Combinatorial expressions for the ranks of constructed arrays were derived. Examples were given to show that the codes constructed perform well over the AWGN channel decoded with either the SPA or the MSA.

**ACKNOWLEDGMENT**

This work was supported by the National Science Foundation (NSF) under the grant CCF-1015548.

**REFERENCES**


