

# Quasi-Cyclic LDPC Codes on Latin Squares and the Ranks of their Parity-Check Matrices

Li Zhang, Qin Huang, Shu Lin, K. Abdel-Ghaffar  
Department of Electrical and Computer Eng.  
University of California  
Davis, CA 95616, USA  
Email: {lizhang,qinhuang,shulin,ghaffar}@ucdavis.edu

Ian F. Blake  
Department of Electrical and Computer Eng.  
University of British Columbia  
Vancouver, BC, V6T 1Z4, CANADA  
Email: ifblake@ece.ubc.ca

**Abstract**—Quasi-cyclic codes are the most promising class of structured LDPC codes due to their ease of implementation and excellent performance over noisy channels when decoded with message-passing algorithms as extensive simulation studies have shown. An approach for constructing quasi-cyclic LDPC codes based on Latin squares over finite fields is presented. By analyzing the parity-check matrices of these codes, expressions for their ranks are derived. Experimental results show that, with iterative decoding algorithms, the constructed codes perform very well over the AWGN and the binary erasure channels.

## I. INTRODUCTION

LDPC codes have attracted widespread interest because of their remarkable performance that can be achieved by efficient decoding algorithms. These codes, first discovered by Gallager in 1962 [1], laid dormant for about 35 years until their rediscovery in the late 1990's [2], [3]. Since then a great deal of research effort has been expended in design, construction, structural analysis, encoding, decoding, generalizations and applications of LDPC codes. Many LDPC codes have been chosen as the standard codes for various next generations of communication systems.

A regular binary LDPC code  $\mathcal{C}$  [1] is given by the null space of a sparse parity-check matrix  $\mathbf{H}$  over  $\text{GF}(2)$  that has constant column weight  $\gamma$  and constant row weight  $\rho$ , where  $\gamma$  and  $\rho$  are small compared to the code length. Such an LDPC code is said to be  $(\gamma, \rho)$ -regular. If the columns and/or rows of the parity-check matrix  $\mathbf{H}$  have varying weights, then the null space of  $\mathbf{H}$  gives an irregular LDPC code.

In almost all of the proposed constructions of LDPC codes, the following constraint on the rows and columns of the parity-check matrix  $\mathbf{H}$  is imposed: no two rows (or two columns) can have more than one position where they both have 1-components. This constraint on the rows and columns of  $\mathbf{H}$  is referred to as the *row-column (RC)-constraint*. The RC-constraint on  $\mathbf{H}$  ensures that the Tanner graph [4] of the LDPC code given by the null space of  $\mathbf{H}$  has a girth of at least 6 [5], [6], [7]. It also ensures that the minimum distance of a  $(\gamma, \rho)$ -regular LDPC code is at least  $\gamma + 1$ . This distance bound is tight for regular LDPC codes whose parity-check matrices have large column weights, such as finite geometry LDPC codes [5] and finite field LDPC codes constructed in [8], and this paper.

If the parity-check matrix  $\mathbf{H}$  of an LDPC code is an array (or a block) of sparse *circulants* of the same size over  $\text{GF}(2)$ , then the null space of  $\mathbf{H}$  gives a *quasi-cyclic (QC)-LDPC* code. Many of the algebraic constructions of LDPC codes result in QC-codes. Extensive simulation studies have shown that LDPC QC-codes have very good performance over noisy channels when decoded with message-passing algorithms, see [6], [7] and the references therein. Well designed algebraic QC-LDPC codes can perform close to the Shannon limit and just as well as (or even better than) their corresponding random or pseudo-random QC-LDPC codes constructed using computer-based methods over the AWGN and the binary erasure channels, as demonstrated in [8], [9]. In addition, a major advantage of QC-LDPC codes is that they can be efficiently encoded using simple shift-registers [10].

This paper is concerned with constructions of QC-LDPC codes and rank analysis of their parity-check matrices. We consider a general class of QC-LDPC codes and then a subclass constructed based on Latin squares.

The paper is organized as follows. Section II presents a general algebraic method for constructing QC-LDPC codes. A general framework to determine the rank of the parity-check matrices is developed in Section III. Although the general algebraic method for constructing QC-LDPC codes presented in Section II was proposed in [8], [9]; these papers did not provide any analysis of the ranks of the parity-check matrices of the constructed codes. In this paper, such an analysis is provided. This analysis generalizes and simplifies the rank analysis of a class of QC-LDPC codes constructed based on cyclic MDS (or RS) codes with two information symbols [11]. In Section IV, we present a large class of algebraic QC-LDPC codes constructed based on Latin squares over finite fields, called *QC-LDPC codes on Latin squares*. The construction of QC-LDPC codes on Latin squares follows the general method explained in Section II. (The construction method as well as the constructed codes significantly differ from those based on BIBD designs devised using Latin squares [12], [13], [14].) We analyze, in Section V, the ranks of the parity-check matrices of several subclasses of QC-LDPC codes on Latin squares and derive combinatorial expressions for these ranks. The paper is concluded in Section VI.

## II. A GENERAL ALGEBRAIC CONSTRUCTION OF QC-LDPC CODES

Consider the Galois field  $\text{GF}(q)$ . Let  $\alpha$  be a primitive element of  $\text{GF}(q)$ . Then, the powers of  $\alpha, \alpha^{-\infty} = 0, \alpha^0 = 1, \alpha^1, \alpha^2, \dots, \alpha^{q-2}$ , give all the  $q$  elements of  $\text{GF}(q)$  and  $\alpha^{q-1} = 1$ .

Let  $\mathbf{P}$  be a  $(q-1) \times (q-1)$  circulant permutation matrix (CPM) whose top row is given by the  $(q-1)$ -tuple  $(010 \dots 0)$  over  $\text{GF}(2)$  where the components are labeled from 0 to  $q-2$  and the single 1-component is located at the 1st position. Then  $\mathbf{P}$  consists of the  $(q-1)$ -tuple  $(010 \dots 0)$  and its  $(q-2)$  right cyclic shifts as rows. For  $1 \leq i < q$ , let  $\mathbf{P}^i = \mathbf{P} \times \mathbf{P} \times \dots \times \mathbf{P}$  be the product of  $\mathbf{P}$  with itself  $i$  times, called the  $i$ th power of  $\mathbf{P}$ . Then,  $\mathbf{P}^i$  is also a  $(q-1) \times (q-1)$  CPM whose top row has a single 1-component at the  $i$ th position. For  $i = q-1$ ,  $\mathbf{P}^{q-1} = \mathbf{I}_{q-1}$ , the  $(q-1) \times (q-1)$  identity matrix. Let  $\mathbf{P}^0 \triangleq \mathbf{P}^{q-1} = \mathbf{I}_{q-1}$ . Then the set  $\mathcal{P} = \{\mathbf{P}^0, \mathbf{P}, \mathbf{P}^2, \dots, \mathbf{P}^{q-2}\}$  of CPMs forms a cyclic group of order  $q-1$  under matrix multiplication over  $\text{GF}(2)$  with  $\mathbf{P}^{q-1-i}$  as the multiplicative inverse of  $\mathbf{P}^i$  and  $\mathbf{P}^0$  as the identity element.

For  $0 \leq i < q-1$ , we represent the nonzero element  $\alpha^i$  of  $\text{GF}(q)$  by the  $(q-1) \times (q-1)$  CPM  $\mathbf{P}^i$ . This matrix representation is referred to as the  $(q-1)$ -fold binary matrix dispersion (or simply binary matrix dispersion) of  $\alpha^i$ . Since there are  $q-1$  nonzero elements in  $\text{GF}(q)$  and there are exactly  $q-1$  different CPMs over  $\text{GF}(2)$  of size  $(q-1) \times (q-1)$ , there is a *one-to-one correspondence* between a nonzero element of  $\text{GF}(q)$  and a CPM of size  $(q-1) \times (q-1)$ . For a nonzero element  $\delta$  in  $\text{GF}(q)$ , we use the notation  $\mathbf{B}(\delta)$  to denote its binary matrix dispersion. If  $\delta = \alpha^i$ , then  $\mathbf{B}(\delta) = \mathbf{P}^i$ . For the 0-element of  $\text{GF}(q)$ , its binary matrix dispersion is defined as the  $(q-1) \times (q-1)$  zero matrix (ZM), denoted by  $\mathbf{P}^{-\infty}$ .

Consider a  $k \times n$  matrix over  $\text{GF}(q)$ ,

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

whose rows satisfy the following constraint: for  $0 \leq i, j < k, i \neq j$  and  $0 \leq c, l < q-1$ , the Hamming distance between the two  $q$ -ary  $n$ -tuples,  $\alpha^c \mathbf{w}_i$  and  $\alpha^l \mathbf{w}_j$ , is at least  $n-1$ , (i.e.,  $\alpha^c \mathbf{w}_i$  and  $\alpha^l \mathbf{w}_j$  differ in at least  $n-1$  places). The above constraint on the rows of matrix  $\mathbf{W}$  given in (1) is called the *row-distance (RD)-constraint* and  $\mathbf{W}$  is called an RD-constrained matrix.

For  $0 \leq i < k$  and  $0 \leq j < n$ , dispersing each nonzero entry  $w_{i,j}$  of  $\mathbf{W}$  into a  $(q-1) \times (q-1)$  CPM  $\mathbf{B}(w_{i,j}) \triangleq \mathbf{B}(i, j)$  over  $\text{GF}(2)$  and each 0-entry into a  $(q-1) \times (q-1)$  ZM, we obtain the following  $k \times n$  array of CPMs and/or ZMs over  $\text{GF}(2)$  of size  $(q-1) \times (q-1)$ :

$$\mathbf{H} = [\mathbf{B}_{i,j}]_{0 \leq i < k, 0 \leq j < n}. \quad (2)$$

$\mathbf{H}$  is called the binary  $(q-1)$ -fold array dispersion of  $\mathbf{W}$  (or simply binary array dispersion of  $\mathbf{W}$ ) and it is a  $k(q-1) \times n(q-1)$  matrix over  $\text{GF}(2)$ . The matrix  $\mathbf{W}$  is called the *base*

*matrix*. Based on the RD-constraint on the rows of  $\mathbf{W}$  and the binary matrix dispersions of the entries of  $\mathbf{W}$ , it was proved in [8], [9] that  $\mathbf{H}$ , as a  $k(q-1) \times n(q-1)$  matrix over  $\text{GF}(2)$ , satisfies the RC-constraint. Hence, its associated Tanner graph has a girth of at least 6.

The total number of 1-entries in  $\mathbf{H}$  is at most  $kn(q-1)$ , while the total number of entries of  $\mathbf{H}$  is  $kn(q-2)^2$ . Therefore, for a relatively large  $q$ ,  $\mathbf{H}$  is a sparse matrix that satisfies the RC-constraint. Hence, the null space of  $\mathbf{H}$  gives a QC-LDPC code  $\mathcal{C}_{qc}$  of length  $n(q-1)$  with rate at least  $(n-k)/n$ , whose Tanner graph has a girth of at least 6. The subscript “qc” stands for “quasi-cyclic”. If  $\mathbf{W}$  has constant column and row weights,  $\mathcal{C}_{qc}$  is a regular QC-LDPC code, otherwise it is an irregular QC-LDPC code.

The construction presented above is a simplified version of the construction given in [8], [9] where several classes of RD-constrained matrices over finite fields were given. By array dispersions of these classes of RD-constrained matrices, several classes of QC-LDPC codes were constructed. The codes given in the examples of [8], [9] decoded with iterative decoding using the sum-product algorithm (SPA) displayed excellent performance over the AWGN and binary erasure channels in terms of error-rate, error-floor and rate of decoding convergence. However, no analysis of the rank of the array  $\mathbf{H}$  given by (2) was provided in [8], [9]. In the following section, such analysis is presented for the special case in which  $q = 2^m$ .

## III. RANK ANALYSIS

Let  $\alpha$  be a primitive element of  $\text{GF}(2^m)$ . Let  $\mathbf{F}$  and  $\mathbf{F}^{-1}$  be the  $(2^m-1) \times (2^m-1)$  Fourier Transform (FT) matrix over  $\text{GF}(2^m)$  and its inverse which are defined as follows [15]:

$$\mathbf{F} = [\alpha^{ij}]_{0 \leq i < 2^m-1, 0 \leq j < 2^m-1},$$

$$\mathbf{F}^{-1} = [\alpha^{-ij}]_{0 \leq i < 2^m-1, 0 \leq j < 2^m-1}.$$

Then  $\mathbf{F}\mathbf{F}^{-1} = \mathbf{F}^{-1}\mathbf{F} = \mathbf{I}_{2^m-1}$ , a  $(2^m-1) \times (2^m-1)$  identity matrix.

For  $0 \leq i < 2^m-1$ , applying  $\mathbf{F}$  and  $\mathbf{F}^{-1}$  to the  $(2^m-1) \times (2^m-1)$  CPM  $\mathbf{P}^i$  over  $\text{GF}(2)$ , we obtain the following  $(2^m-1) \times (2^m-1)$  matrix over  $\text{GF}(2^m)$ :

$$\mathbf{F}\mathbf{P}^i\mathbf{F}^{-1} = \mathbf{F}\mathbf{P}\mathbf{F}^{-1}\mathbf{F}\mathbf{P}\mathbf{F}^{-1} \dots \mathbf{F}\mathbf{P}\mathbf{F}^{-1} = (\mathbf{F}\mathbf{P}\mathbf{F}^{-1})^i. \quad (3)$$

Let  $\Lambda^i = (\mathbf{F}\mathbf{P}\mathbf{F}^{-1})^i$ . Expanding  $(\mathbf{F}\mathbf{P}\mathbf{F}^{-1})^i$  based on (3), we find that  $\Lambda^i$  is a *diagonal matrix* over  $\text{GF}(2^m)$  with  $1^i, \alpha^{(2^m-2)i}, \dots, \alpha^{2i}, \alpha^i$  as entries on its main diagonal and zeros elsewhere. For simplicity, we express the above diagonal matrix as follows:  $\Lambda^i = \text{diag}(1^i, \alpha^{(2^m-2)i}, \dots, \alpha^{2i}, \alpha^i)$ . Recall that in the last section, we represent the field element  $\alpha^i$  by the CPM  $\mathbf{P}^i$ . With the above transforming process, we map  $\alpha^i$  into a diagonal matrix  $\Lambda^i$  in frequency domain. The mapping is one-to-one.  $\Lambda^i$  may be viewed as the matrix dispersion of  $\alpha^i$  in frequency domain.

Define two matrices over  $\text{GF}(2^m)$ :

$$\mathcal{F}_k = \text{diag}\{\underbrace{\mathbf{F}, \mathbf{F}, \dots, \mathbf{F}}_k\},$$

$$\mathcal{F}_n^{-1} = \text{diag}\{\underbrace{\mathbf{F}^{-1}, \mathbf{F}^{-1}, \dots, \mathbf{F}^{-1}}_n\}.$$

$\mathcal{F}_k$  is a  $k \times k$  diagonal array with  $\mathbf{F}$ 's on its main diagonal and  $\mathcal{F}_n^{-1}$  is an  $n \times n$  diagonal array with  $\mathbf{F}^{-1}$ 's on its main diagonal. Applying  $\mathcal{F}_k$  and  $\mathcal{F}_n^{-1}$  to the array  $\mathbf{H} = [\mathbf{B}_{i,j}]_{0 \leq i < k, 0 \leq j < n}$  of CPMs and/or ZMs given by (2), we obtain the following  $k \times n$  array of  $(2^m - 1) \times (2^m - 1)$  square submatrices over  $\text{GF}(2^m)$ :

$$\mathbf{H}_{freq} = \mathcal{F}_k \mathbf{H} \mathcal{F}_n^{-1} = [\mathbf{F} \mathbf{B}_{i,j} \mathbf{F}^{-1}]_{0 \leq i < k, 0 \leq j < n}. \quad (4)$$

If  $\mathbf{B}_{i,j} = \mathbf{P}^l$  with  $0 \leq l < 2^m - 1$ , then  $\mathbf{F} \mathbf{B}_{i,j} \mathbf{F}^{-1} = \Lambda^l = \text{diag}(1^l, \alpha^{(2^m-2)l}, \dots, \alpha^{2l}, \alpha^l)$ . If  $\mathbf{B}_{i,j}$  is a ZM, then  $\mathbf{F} \mathbf{B}_{i,j} \mathbf{F}^{-1}$  is also a zero matrix.  $\mathbf{H}_{freq}$  can be viewed as the frequency domain representation (or the FT) of  $\mathbf{H}$  (or as the array dispersion of  $\mathbf{W}$  in frequency domain).

Define the following index sets:

$$\begin{aligned} \mathcal{I}_{row}^0 &= [0, 2^m - 1, 2(2^m - 1), \dots, (k - 1)(2^m - 1)], \\ \mathcal{I}_{row} &= [\mathcal{I}_{row}^0, 1 + \mathcal{I}_{row}^0, \dots, (2^m - 2) + \mathcal{I}_{row}^0], \\ \mathcal{I}_{col}^0 &= [0, 2^m - 1, 2(2^m - 1), \dots, (n - 1)(2^m - 1)], \\ \mathcal{I}_{col} &= [\mathcal{I}_{col}^0, 1 + \mathcal{I}_{col}^0, \dots, (2^m - 2) + \mathcal{I}_{col}^0]. \end{aligned}$$

We permute the rows and columns of  $\mathbf{H}_{freq}$  based on the index sets  $\mathcal{I}_{row}$  and  $\mathcal{I}_{col}$ , respectively. Thus, the  $i$ th row after permutation is given by the row in  $\mathbf{H}_{freq}$  whose index is the  $i$ th element in  $\mathcal{I}_{row}$  and, similarly, the  $j$ th column after permutation is given by the column in  $\mathbf{H}_{freq}$  whose index is the  $j$ th element in  $\mathcal{I}_{col}$ . The permutations result in a  $(2^m - 1) \times (2^m - 1)$  diagonal array  $\mathbf{H}_{freq}^*$  with  $2^m - 1$  matrices,  $\mathbf{W}^{\circ(2^m-1)}, \mathbf{W}^{\circ(2^m-2)}, \dots, \mathbf{W}^{\circ 2}, \mathbf{W}^{\circ 1}$ , each of size  $k \times n$ , on its main diagonal, where  $\mathbf{W}^{\circ l}$  denotes the Hadamard product [16] of  $\mathbf{W}$  with itself  $l - 1$  times,  $1 \leq l < 2^m$ . The Hadamard product of two matrices  $\mathbf{A} = [a_{i,j}]$  and  $\mathbf{B} = [b_{i,j}]$  of the same size is defined as their element-wise product  $\mathbf{A} \circ \mathbf{B} = [a_{i,j} b_{i,j}]$ . The superscript “ $\circ$ ” of  $\mathbf{W}^{\circ l}$  stands for “Hadamard product”. Therefore,

$$\mathbf{H}_{freq}^* = \text{diag}\{\mathbf{W}^{\circ(2^m-1)}, \dots, \mathbf{W}^{\circ 2}, \mathbf{W}^{\circ 1}\}. \quad (5)$$

Hereafter, we refer to  $\mathbf{W}^{\circ l}$  as the Hadamard product of  $\mathbf{W}$  to the  $l$ th power.

Let  $\text{rank}(\mathbf{M})$  denote the rank of a matrix  $\mathbf{M}$  over a field. Since  $\mathbf{H}_{freq}$  is the frequency domain representation of  $\mathbf{H}$  and  $\mathbf{H}_{freq}^*$  is obtained by permuting the rows and columns of  $\mathbf{H}_{freq}$ , we must have

$$\text{rank}(\mathbf{H}) = \text{rank}(\mathbf{H}_{freq}) = \text{rank}(\mathbf{H}_{freq}^*). \quad (6)$$

It follows from (5) and (6) that we have the following theorem on the rank of  $\mathbf{H}$ .

*Theorem 1:* The rank of the  $k \times n$  array  $\mathbf{H}$  of CPMs and/or ZMs over  $\text{GF}(2)$  given by (2) is equal to

$$\text{rank}(\mathbf{H}) = \sum_{l=1}^{2^m-1} \text{rank}(\mathbf{W}^{\circ l}).$$

## IV. QC-LDPC CODES ON LATIN SQUARES

We present a new class of RD-constrained matrices whose constructions are based on Latin squares over finite fields. By array dispersions of this class of RD-constrained matrices, a large class of QC-LDPC codes is constructed.

### A. A Class of RD-constrained Latin Squares over Finite Fields

*Definition 1:* An array is called a Latin square of order  $n$  if each row and each column contains every element of a set of  $n$  objects exactly once.

Latin squares form a special type of combinatorial designs [17]. There are numerous constructions of Latin squares using finite fields [17], [18]. In the following, a large class of Latin squares is constructed based on finite fields using a very simple method. Latin squares in this class satisfy the RD-constraint.

Consider the field  $\text{GF}(q)$ . Let  $\alpha$  be a primitive element of  $\text{GF}(q)$ . Define the index set  $\mathcal{A} = \{0, 1, \dots, q - 2, -\infty\}$ . The indices in  $\mathcal{A}$  represent the powers of  $\alpha$ ,  $\alpha^0 = 1, \alpha^1, \dots, \alpha^{q-2}, \alpha^{-\infty}$ . Let  $\eta$  be a nonzero element of  $\text{GF}(q)$ . For any  $i \in \mathcal{A}$ , the  $q$  elements,  $\alpha^i \eta - \alpha^0, \alpha^i \eta - \alpha, \dots, \alpha^i \eta - \alpha^{q-2}, \alpha^i \eta - \alpha^{-\infty}$ , are all distinct and they form all the  $q$  elements of  $\text{GF}(q)$  with  $\alpha^{-\infty} = 0$  and  $\alpha^0 = 1$ . Form the following  $q \times q$  matrix over  $\text{GF}(q)$ :

$$\begin{aligned} \mathbf{W} &= \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{q-2} \\ \mathbf{w}_{-\infty} \end{bmatrix} \\ &= \begin{bmatrix} \alpha^0 \eta - \alpha^0 & \alpha^0 \eta - \alpha & \cdots & \alpha^0 \eta - \alpha^{-\infty} \\ \alpha \eta - \alpha^0 & \alpha \eta - \alpha & \cdots & \alpha \eta - \alpha^{-\infty} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q-2} \eta - \alpha^0 & \alpha^{q-2} \eta - \alpha & \cdots & \alpha^{q-2} \eta - \alpha^{-\infty} \\ \alpha^{-\infty} \eta - \alpha^0 & \alpha^{-\infty} \eta - \alpha & \cdots & \alpha^{-\infty} \eta - \alpha^{-\infty} \end{bmatrix}. \end{aligned} \quad (7)$$

Label the rows and columns of  $\mathbf{W}$  with  $0, 1, \dots, q - 2, -\infty$ . From the structure of  $\mathbf{W}$  displayed by (7), we can readily see that  $\mathbf{W}$  has the following structural properties: 1) the  $q$  entries of each row are all different and they form the  $q$  elements of  $\text{GF}(q)$ ; 2) the  $q$  entries of each column are all different and they form the  $q$  elements of  $\text{GF}(q)$ ; 3) any two rows differ in every position; 4) any two columns differ in every position; and 5) there are exactly  $q$  zero entries located at different rows and different columns.

It follows from properties 1) and 2) that  $\mathbf{W}$  is a Latin square of order  $q$ . For  $\eta = \alpha^0, \alpha, \alpha^2, \dots, \alpha^{q-2}$ , we can construct  $q - 1$  Latin squares from (7).

*Theorem 2:* For any nonzero element  $\eta \in \text{GF}(q)$ ,  $\mathbf{W}$  satisfies the RD-constraint.

*Proof:* Let  $\mathbf{w}_i$  and  $\mathbf{w}_j$  be two different rows in  $\mathbf{W}$ . Then  $i \neq j$ . For any two integers  $c$  and  $l$  with  $0 \leq c, l < q - 1$ , consider the two  $q$ -tuples over  $\text{GF}(q)$ ,  $\alpha^c \mathbf{w}_i$  and  $\alpha^l \mathbf{w}_j$ . We need to prove that  $\alpha^c \mathbf{w}_i$  and  $\alpha^l \mathbf{w}_j$  cannot have more than one position where they have identical components.

Suppose that  $\alpha^c \mathbf{w}_i$  and  $\alpha^l \mathbf{w}_j$  have identical components at two different positions  $s$  and  $t$  ( $s \neq t$ ). Then, we have the following two equalities:  $\alpha^c (\alpha^i \eta - \alpha^s) = \alpha^l (\alpha^j \eta - \alpha^s)$  and  $\alpha^c (\alpha^i \eta - \alpha^t) = \alpha^l (\alpha^j \eta - \alpha^t)$ . From these two equalities, we obtain the equality  $(\alpha^j - \alpha^i)(\alpha^t - \alpha^s) = 0$ . This equality implies either  $i = j$  or  $s = t$  which contradicts the facts that  $i \neq j$  and  $s \neq t$ . Therefore,  $\alpha^c \mathbf{w}_i$  and  $\alpha^l \mathbf{w}_j$  cannot have more than one position where they have identical components. This proves that  $\mathbf{W}$  satisfies the RD-constraint. ■

For  $\eta = \alpha^0 = 1$ ,  $\mathbf{W}$  has the simplest form,

$$\mathbf{W} = \begin{bmatrix} 1-1 & 1-\alpha & \cdots & 1-\alpha^{q-2} & 1-0 \\ \alpha-1 & \alpha-\alpha & \cdots & \alpha-\alpha^{q-2} & \alpha-0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^{q-2}-1 & \alpha^{q-2}-\alpha & \cdots & \alpha^{q-2}-\alpha^{q-2} & \alpha^{q-2}-0 \\ 0-1 & 0-\alpha & \cdots & 0-\alpha^{q-2} & 0-0 \end{bmatrix}. \quad (8)$$

The entries on the main diagonal of  $\mathbf{W}$  are the 0-element of  $\text{GF}(q)$ .

### B. QC-LDPC Codes on Latin Squares

By array dispersion of the Latin square  $\mathbf{W}$  given by (7), we obtain the following  $q \times q$  array of  $(q-1) \times (q-1)$  CPMs and ZMs over  $\text{GF}(2)$ :

$$\mathbf{H} = \begin{bmatrix} \mathbf{B}_{0,0} & \mathbf{B}_{0,1} & \cdots & \mathbf{B}_{0,q-2} & \mathbf{B}_{0,-\infty} \\ \mathbf{B}_{1,0} & \mathbf{B}_{1,1} & \cdots & \mathbf{B}_{1,q-2} & \mathbf{B}_{1,-\infty} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{B}_{q-2,0} & \mathbf{B}_{q-2,1} & \cdots & \mathbf{B}_{q-2,q-2} & \mathbf{B}_{q-2,-\infty} \\ \mathbf{B}_{-\infty,0} & \mathbf{B}_{-\infty,1} & \cdots & \mathbf{B}_{-\infty,q-2} & \mathbf{B}_{-\infty,-\infty} \end{bmatrix}, \quad (9)$$

where  $\mathbf{B}_{i,j} = \mathbf{B}(\alpha^i \eta - \alpha^j)$  is the matrix dispersion of the entry  $\alpha^i \eta - \alpha^j$  in  $\mathbf{W}$  with  $i$  and  $j$  in the index set  $\mathcal{A}$ .  $\mathbf{H}$  has  $q$  ZMs of size  $(q-1) \times (q-1)$ . If we set  $\eta = 1$ ,  $\mathbf{W}$  has the form given by (8). Then, the zero matrices of  $\mathbf{H}$  are on the main diagonal of  $\mathbf{H}$ .  $\mathbf{H}$  is a  $q(q-1) \times q(q-1)$  matrix over  $\text{GF}(2)$  with both column and row weights equal to  $q-1$ . Since  $\mathbf{W}$  satisfies the RD-constraint,  $\mathbf{H}$  satisfies the RC-constraint. Furthermore, since all the nonzero entries in a row (or a column) of the Latin square  $\mathbf{W}$  given by (7) are different, all the CPMs in a row (or a column) of  $\mathbf{H}$  are distinct.

For any pair  $(\gamma, \rho)$  of integers  $\gamma$  and  $\rho$  with  $1 \leq \gamma, \rho \leq q$ , 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  $\text{GF}(2)$  which also satisfies the RC-constraint. The null space of  $\mathbf{H}(\gamma, \rho)$  gives a binary QC-LDPC code  $\mathcal{C}_{qc}$  of length  $\rho(q-1)$  with rate at least  $(\rho-\gamma)/\rho$ , whose Tanner graph has a girth of at least 6. For a given finite field  $\text{GF}(q)$ , the above construction gives a family of binary QC-LDPC codes on Latin squares.

In the following, we use two examples to illustrate the construction of QC-LDPC codes given above. To compute the error performances of the constructed codes over the binary-input AWGN channel in these two examples, we assume BPSK signaling and use the SPA (or min-sum algorithm (MSA)) for decoding. The maximum number of decoding iterations is set to 50. The codes given in these two examples are constructed specifically to show that they can perform

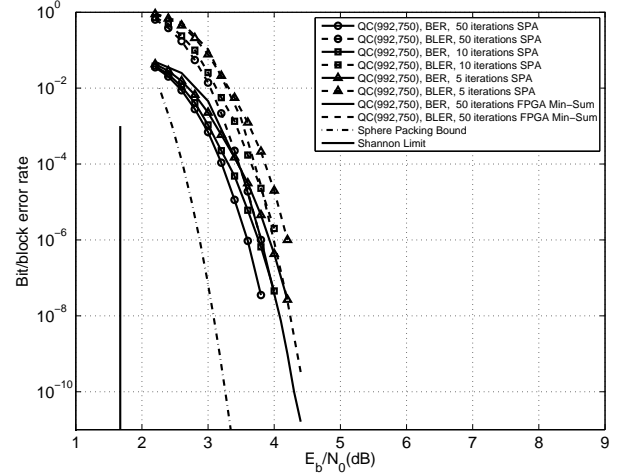


Fig. 1.(a) The error performance of the (992, 750) QC-LDPC code given in Example 1 over the AWGN channel.

down to a very low error rate without error-floor. Low error-floor is a specific feature of algebraic LDPC codes.

*Example 1:* Let  $\text{GF}(2^5)$  be the field for code construction. Let  $\alpha$  be a primitive element of  $\text{GF}(2^5)$ . First, we construct a  $32 \times 32$  Latin square  $\mathbf{W}$  over  $\text{GF}(2^5)$  of the form given by (8). Dispersing each nonzero entry of  $\mathbf{W}$  into a  $31 \times 31$  CPM and each 0-entry on the main diagonal of  $\mathbf{W}$  into a  $31 \times 31$  zero matrix, we obtain a  $32 \times 32$  array  $\mathbf{H}$  of CPMs and ZMs of size  $31 \times 31$ .  $\mathbf{H}$  is a  $992 \times 992$  matrix over  $\text{GF}(2)$  with both column and row weights 31. The null space of  $\mathbf{H}$  gives a  $(31, 31)$ -regular (992, 750) QC-LDPC code of rate 0.756. The error performances of this code decoded with 5, 10 and 50 iterations of the SPA are shown in Figure 1(a). We see that the decoding of this code converges very fast. At the BLER (block error rate) of  $10^{-6}$ , the code decoded with 50 iterations of SPA performs only 0.95dB from the sphere packing bound. Also included in Figure 1(a) is the error performance of the code computed by an FPGA min-sum decoder. We see that the code performs down to the BER of  $10^{-11}$  without error-floor.

In Figure 1(b) we show the unresolved erasure bit rate (UEBR) and the unresolved erasure block rate (UEBLR) of the code with iterative decoding over the binary-erasure channel (BEC). As the rate of the code is  $R = 0.756$ , the Shannon limit for the BEC is  $1 - R = 0.244$  bits per channel usage. From Figure 1(b), we see that at the UEBR of  $10^{-6}$ , the code performs 0.118 from the Shannon limit. For such a short code, it performs very well over both the AWGN channel and the BEC.  $\triangle\triangle$

*Example 2:* In this example, we construct a long high-rate code. The field for code construction is the prime field  $\text{GF}(181)$ . Based on this field, we can construct a  $181 \times 181$  Latin square  $\mathbf{W}$  over  $\text{GF}(181)$  of the form given by (8). Dispersing this Latin square, we obtain a  $181 \times 181$  array  $\mathbf{H}$  of CPMs and ZMs of size  $180 \times 180$ . Take a  $6 \times 90$  subarray  $\mathbf{H}(6, 90)$  from  $\mathbf{H}$ , avoiding the ZMs on the main diagonal

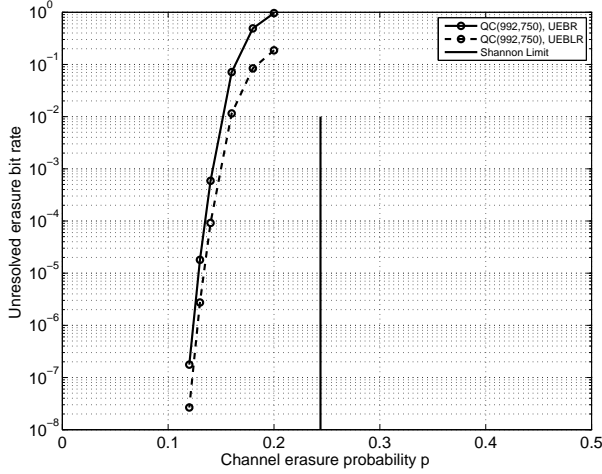


Fig. 1.(b) The error performance of the (992, 750) QC-LDPC code given in Example 1 over the BEC.

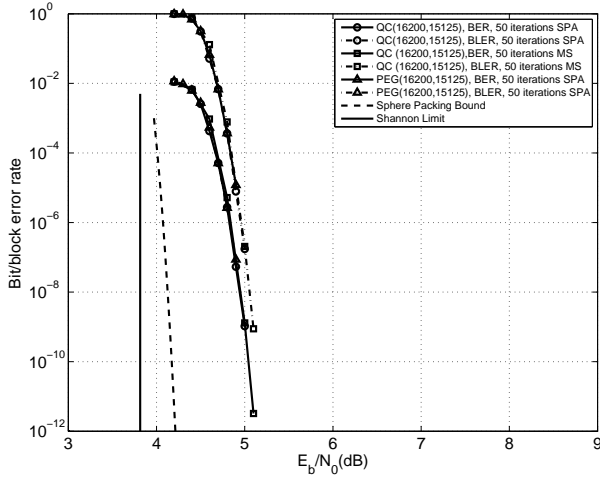


Fig. 2. The error performance of the (16200, 15125) QC-LDPC code given in Example 2 over the AWGN channel.

of  $\mathbf{H}$ . Then  $\mathbf{H}(6, 90)$  is a  $1080 \times 16200$  matrix over  $\text{GF}(2)$  with column and row weights 6 and 90, respectively. The null space of this matrix gives a  $(6, 90)$ -regular  $(16200, 15125)$  QC-LDPC code of rate 0.9336. The error performances of this code decoded using the SPA and an FPGA min-sum decoder with 50 iterations are shown in Figure 2. We see that the performance curves computed with the SPA and the FPGA min-sum decoder overlap with each other. The code performs down to a BER of almost  $10^{-12}$  without error-floor. At the BER of  $10^{-12}$ , it performs 1.3dB from the Shannon limit. Also included in Figure 2 is the error performance of a pseudo-random  $(16200, 15152)$  QC-LDPC code constructed with the PEG-algorithm [19] using lifting with circulant permutation (equivalent to a protograph-based code). We see that the performance curves of the algebraic and the pseudo-random codes overlap with each other down to the BER of  $10^{-7}$ .  $\triangle\triangle$

## V. RANK ANALYSIS OF QC-LDPC CODES ON LATIN SQUARES

In this section, we analyze the ranks of the parity-check matrices of the QC-LDPC codes that are constructed based on the Latin squares of the form given by (7) for the special case with  $q = 2^m$  (i.e., Latin squares over  $\text{GF}(2^m)$ ) with  $m \geq 2$ . Since the characteristic of  $\text{GF}(2^m)$  is 2, the subtraction “-” in (7) can be replaced by modulo-2 addition. For simplicity, we use the Latin square  $\mathbf{W}$  given by (8) for analysis. This results in no loss of generality.

Consider the array  $\mathbf{H}$  of CPMs and ZMs over  $\text{GF}(2)$  given by (9) obtained by array dispersion of the Latin square  $\mathbf{W}$  over  $\text{GF}(2^m)$  given by (8). The CPMs and ZMs in  $\mathbf{H}$  are of size  $(2^m - 1) \times (2^m - 1)$ . For  $1 \leq \gamma, \rho \leq 2^m$ , let  $\mathbf{H}(\gamma, \rho)$  be a  $\gamma \times \rho$  subarray taken from the upper left corner of  $\mathbf{H}$ , i.e. the first  $\gamma$  rows and the first  $\rho$  columns of  $\mathbf{H}$ . Taking a subarray from  $\mathbf{H}$  this way is just for the simplicity of notation and expressions with no loss of generality. Let  $\mathbf{W}(\gamma, \rho)$  be the  $\gamma \times \rho$  submatrix taken from the upper left corner of the Latin square  $\mathbf{W}$ , i.e., the first  $\gamma$  rows and the first  $\rho$  columns of  $\mathbf{W}$ . It is clear that the  $\gamma \times \rho$  subarray  $\mathbf{H}(\gamma, \rho)$  of  $\mathbf{H}$  is the array dispersion of  $\mathbf{W}(\gamma, \rho)$ .  $\mathbf{W}(\gamma, \rho)$  can be expressed as follows:

$$\mathbf{W}(\gamma, \rho) = \begin{bmatrix} \alpha^0 & 1 \\ \alpha^1 & 1 \\ \vdots & \vdots \\ \alpha^{\gamma-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha^0 & \alpha^1 & \dots & \alpha^{\rho-1} \end{bmatrix}.$$

It follows from Theorem 1 that the rank of  $\mathbf{H}(\gamma, \rho)$  is given by

$$\text{rank}(\mathbf{H}(\gamma, \rho)) = \sum_{l=1}^{2^m-1} \text{rank}(\mathbf{W}^{ol}(\gamma, \rho)). \quad (10)$$

Therefore, to determine the rank of  $\mathbf{H}(\gamma, \rho)$ , we need to determine the rank of the Hadamard product  $\mathbf{W}^{ol}(\gamma, \rho)$  of  $\mathbf{W}(\gamma, \rho)$  to the  $l$ th power for  $1 \leq l < 2^m$ . Note that,  $\mathbf{W}^{o1}(\gamma, \rho) = \mathbf{W}(\gamma, \rho)$ . The following theorem gives an expression for  $\text{rank}(\mathbf{W}^{ol}(\gamma, \rho))$ . Its lengthy proof is omitted. In the theorem, we use  $\lambda_l$  to denote the number of odd integers in the  $l$ th row of the Pascal’s triangle [20].

*Theorem 3:* For  $1 \leq l < 2^m$ , the rank of  $\mathbf{W}^{ol}(\gamma, \rho)$  is upper bounded as follows:

$$\text{rank}(\mathbf{W}^{ol}(\gamma, \rho)) \leq \min(\gamma, \rho, \lambda_l).$$

For  $\rho = 2^m$ , we have

$$\text{rank}(\mathbf{W}^{ol}(\gamma, 2^m)) = \min(\gamma, \lambda_l).$$

The following result on the rank of  $\mathbf{H}(\gamma, \rho)$  follows from (10) and Theorem 3.

*Theorem 4:* For  $1 \leq \gamma, \rho \leq 2^m$ , the rank of the  $\gamma \times \rho$  subarray  $\mathbf{H}(\gamma, \rho)$  of the array  $\mathbf{H}$  of CPMs and ZMs obtained by the array dispersion of the RD-constrained Latin square  $\mathbf{W}$  given by (8) is upper bounded as follows:

$$\text{rank}(\mathbf{H}(\gamma, \rho)) \leq \sum_{l=1}^{2^m-1} \min(\gamma, \rho, \lambda_l).$$

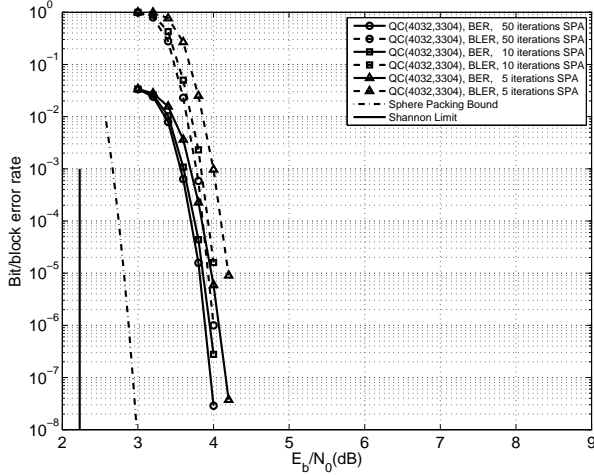


Fig. 3.(a) The error performance of the (4032, 3304) QC-LDPC code given in Example 3 over the AWGN channel.

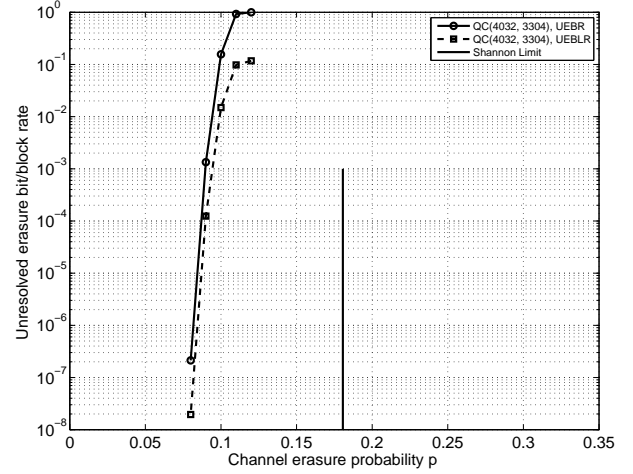


Fig. 3.(b) The error performance of the (4032, 3304) QC-LDPC code given in Example 3 over the BEC.

For  $\rho = 2^m$ ,

$$\text{rank}(\mathbf{H}(\gamma, \rho)) = \sum_{l=1}^{2^m-1} \min(\gamma, \lambda_l).$$

In case  $\rho = 2^m$ , a combinatorial expression for the rank of the  $\gamma \times 2^m$  subarray  $\mathbf{H}(\gamma, 2^m)$  of the array  $\mathbf{H}$  given by (9) can be derived as stated below. The technical proof of this result is omitted.

*Theorem 5:* For  $q = 2^m$ ,  $1 \leq \gamma \leq 2^m$ , let  $t_\gamma$  be the integer satisfying  $2^{t_\gamma} \leq \gamma < 2^{t_\gamma+1}$ . Then

$$\text{rank}(\mathbf{H}(\gamma, 2^m)) = \gamma(2^m - 1) - \sum_{t=1}^{t_\gamma} \binom{m}{t} (\gamma - 2^t).$$

In case  $\gamma = 2^m$ , we have

$$\text{rank}(\mathbf{H}(2^m, 2^m)) = 3^m - 1.$$

*Example 3:* Let  $\text{GF}(2^6)$  be the code construction field. Based on this field, we construct a  $64 \times 64$  Latin square  $\mathbf{W}$  of the form given by (8). Dispersing  $\mathbf{W}$ , we obtain a  $64 \times 64$  array  $\mathbf{H}$  of CPMs and ZMs of size of  $63 \times 63$ . It is a  $4032 \times 4032$  matrix over  $\text{GF}(2)$  with both column and row weights 63. It follows from Theorem 5 that the rank of  $\mathbf{H}$  is  $3^6 - 1 = 728$ . The null space of  $\mathbf{H}$  gives a  $(63, 63)$ -regular (4032, 3304) QC-LDPC code of rate 0.8194. The error performances of this code decoded using the SPA with 5, 10 and 50 iterations are shown in Figure 3(a). We see that the SPA decoding of this code converges very fast. At the BLER of  $10^{-6}$ , the code performs 1dB from the sphere packing bound. Its performance over the BEC is shown in Figure 3(b).  $\triangle\triangle$

## VI. CONCLUSION

In this paper, we studied the rank of parity-check matrices of QC-LDPC codes constructed based on the array dispersion of RD-constrained matrices over finite fields. Then, we presented a class of RD-constrained Latin squares over finite fields.

Based on these Latin squares, we constructed a large class of QC-LDPC codes, called QC-LDPC codes on Latin squares. We presented combinatorial expressions for the ranks of the parity check matrices of QC-LDPC codes on Latin squares.

## ACKNOWLEDGMENT

This research was supported by NASA under the Grant NNX09AI21G, NSF under the Grant CCF-0727478, and gift grants from Intel and Northrop Grumman Space Technology.

## 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, no. 18, 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, no. 2, pp.399–432, Mar. 1999.
- [4] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, no. 5, pp. 533–547, Sept. 1981.
- [5] Y. Kou, S. Lin and M. P. C. Fossorier, "Low density parity check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.
- [6] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, 2nd edition. Prentice Hall, Upper Saddle River, NJ., 2004.
- [7] W. E. Ryan and S. Lin, *Channel Codes: Classical and Modern*. New York, NY: Cambridge University Press, 2009.
- [8] L. Lan, L. Zeng, Y. Tai, L. Chen, S. Lin, and K. Abdel-Ghaffar, "Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach," *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2429–2458, Jul. 2007.
- [9] S. Song, B. Zhou, S. Lin, and K. Abdel-Ghaffar, "A unified approach to the construction of binary and nonbinary Quasi-cyclic LDPC codes based on finite fields," *IEEE Trans. Commun.*, vol. 57, no.1, pp. 84–93, Jan. 2009.
- [10] Z. Li, L. Chen, L. Zeng, S. Lin and W. H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," *IEEE Trans. Commun.*, vol. 54, no.1, pp. 71–81, Jul. 2006.
- [11] N. Kamiya and E. Sasaki, "Efficient encoding of QC-LDPC codes related to cyclic MDS codes," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 6, pp. 846–854, Aug. 2009.

- [12] B. Vasic, E. M. Kurtas, and A. V. Kuznetsov, "LDPC codes based on mutually orthogonal Latin rectangles and their application in perpendicular magnetic recording," *IEEE Trans. Magn.*, vol. 38, no. 5, pp. 2346–2348, Sept. 2002.
- [13] B. Vasic and O. Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," *IEEE Trans. Inform. Theory*, vol. 50, no. 6, pp. 1156–1176, Jun. 2004.
- [14] S. Laendner and O. Milenkovic, "LDPC codes based on Latin squares: cycle structure, stopping set, and trapping set analysis," *IEEE Trans. Commun.*, vol. 55, no. 2, p. 303–312, Feb. 2007.
- [15] R. M. Roth, *Introduction to Coding Theory*. Cambridge, UK: Cambridge University Press, 2006.
- [16] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, UK: Cambridge University Press, 2006.
- [17] M. Hall Jr., *Combinatorial Theory*, 2nd Edition. New York, NY: Wiley, 1986.
- [18] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, revised Edition. Cambridge, UK: Cambridge University Press, 1994.
- [19] X. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graph," *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.
- [20] J. H. Silverman, *A Friendly Introduction to Number Theory*, 3rd Edition. Upper Saddle River, NJ: Pearson, 2006.