Design of Non-Binary Quasi-Cyclic LDPC Codes Based on Multiplicative Groups and Euclidean Geometries

Xueqin Jiang and Moon Ho Lee

Abstract: **This paper presents an approach to the construction of non-binary quasi-cyclic (QC) low-density parity-check (LDPC) codes based on multiplicative groups over one Galois field $GF(q)$ and Euclidean geometries over another Galois field $GF(2^s)$. Codes of this class are shown to be regular with girth $6 \leq g \leq 18$ and have low densities. Finally, simulation results show that the proposed codes perform very well with the iterative decoding.**

Index Terms: **Euclieangeometry, girth, lines, multiplicative groups, non-binary quasi-cyclic (QC) low-density parity-check (LDPC) codes, pointsv.**

I. INTRODUCTION

Low-density parity-check (LDPC) codes, introduced by Gallager in 1963 [1], have drawn considerable attention since they were rediscovered in the mid of 1990's [2]–[9]. LDPC codes design over $GF(q)$ can achieve near-Shannon-limit performance for $q = 2$ (binary LDPC codes) and very long code length. On the other hand, for moderate code lengths, the error performance can be improved by increasing q (non-binary LDPC codes) [2].

A straightforward implementation of the belief propagation (BP) algorithm to decode $GF(q)$-LDPC codes has computational complexity dominated by $O(q^2)$ operations for each check sum processing [2]. However, an efficient approach using Fourier transforms over $GF(2^p)$ was presented in [10] and [11]. This approach allows reducing the computational complexity of the BP algorithm to $O(p2^p)$ and the new iterative decoding algorithm works on symbols over $GF(2^p)$. It significantly reduces the computational complexity without performance degradation. This new effective decoding algorithm for non-binary LDPC codes may motivate more research effort on the construction of non-binary LDPC codes. In the rest of this paper, whenever we mansion $GF(q)$, we will implicitly referring to the Galois field $GF(2^p)$

One parameter that is usually targeted for optimization in the process of designing LDPC codes is the girth of the underlying Tanner graph [3], [4]. For iterative sum-product decoding of quasi-cyclic (QC) LDPC codes, a part of performance loss is attributed to small values of girth. The construction of non-binary QC-LDPC codes with girth 6 and low densities based on Euclidean geometries has been presented in [5] and [6]. In this paper, we introduce a new construction of non-binary QC-LDPC codes based on multiplicative groups over the Galois field $GF(q)$ and Euclidean geometries over the Galois field $GF(2^s)$, where s is a positive integer and q is a power of two with: 1) Large girth $(6 \leq g \leq 18)$ and 2) low densities. The large girth leads to the good bit error rate (BER) performances with iterative decoding. The low density leads to the low decoding complexity.

The rest of this paper is organized as follows. Section II presents some preliminaries for the presentation. The design of the base matrix based on Euclidean geometries over $GF(2^s)$ is proposed in Section III. In Section IV, we analyze the lower and upper bound of girth of the proposed non-binary QC-LDPC codes and present a shift values assigning method for the design of the shifting matrix S. The non-binary QC-LDPC matrix H is constructed based on multiplicative groups of the Galois fields $GF(q)$ in Section V. Examples of the proposed codes and their simulation results are given in Section VI. Finally, Section VII concludes the paper.

II. PRELIMINARIES

Non-binary QC-LDPC codes are given by the null space of the matrix as follows:

$$H = \begin{pmatrix} h_{a_{(1,1)}} & h_{a_{(1,2)}} & \cdots & h_{a_{(1,N)}} \\ h_{a_{(2,1)}} & h_{a_{(2,2)}} & \cdots & h_{a_{(2,N)}} \\ \vdots & \vdots & \ddots & \vdots \\ h_{a_{(M,2)}} & h_{a_{(M,2)}} & \cdots & h_{a_{(M,N)}} \end{pmatrix}. \tag{1}$$

The matrix H is a $M \times N$ array of α-multiplied circulant permutation matrix and/or zero matrix. Analog to the binary case, each row of the α-multiplied circulant permutation matrix 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. The shifting matrix S of H is defined by

$$S = \begin{pmatrix} a_{(1,1)} & a_{(1,2)} & \cdots & a_{(1,N)} \\ a_{(2,1)} & a_{(2,2)} & \cdots & a_{(2,N)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(M,1)} & a_{(M,2)} & \cdots & a_{(M,N)} \end{pmatrix}. \tag{2}$$

H can be obtained by replacing each entry $a_{m,n}$ of S with $h_{a_{m,n}}$. The base matrix B of H is obtained by replacing zero matrices and α-multiplied circulant permutation matrices in H with '0's and '1's, respectively. The cycles in B and S correspond to the block-cycles in H. In this paper, the term "weight" implies the number of nonzero entries in a row/column of H and the density of B or H is defined as the ratio of the total number of nonzero entries to the total number of entries of B or H. The construction of proposed non-binary LDPC codes consists of

Manuscript received April 13, 2009; approved for publication by Emanuele Viterbo, Division I Editor, December 18, 2009.

This work was supported by World Class University R32-2009-000-20014-0 and Fundamental Research 2010-0020942 NRF, Korea.

X. Jiang is with the Department of Communications and Electronic Engineering, Donghua University, China, email: xqjiang@dhu.edu.cn.

M. H. Lee (corresponding author) is with the Department of Electronics, Chonbuk National University, Korea, email: moonho@chonbuk.ac.kr.

1229-2370/10/$10.00 © 2010 KICS

three steps. First, construct a $M \times N$ base matrices B. Second, replace each '1' in B with a shift value in the range $[0, q-2]$ and replace each '0' with a "∞" and obtain a $M \times N$ shifting matrix S. Third, each entry $a_{(m,n)}$ of S is replaced with $h_{a_{(m,n)}}$ which is a $(q-1)\times(q-1)$ α-multiplied circulant permutation matrix or zero matrix. The obtained matrix is a $M(q-1) \times N(q-1)$ non-binary QC-LDPC matrix H. In the following, we will elaborate on each of these steps in detail.

III. DESIGN OF THE BASE MATRIX B

Let $EG(d, 2^s)$ be a d-dimensional Euclidean geometry over the Galois field $GF(2^s)$ where d and s are two positive integers. This geometry consists of 2^{ds} points, each point is simply a d-tuple over $GF(2^s)$. The all zero d-tuple $0 = (0, 0, \cdots, 0)$ is called the origin. A line in $EG(d, 2^s)$ consists of 2^s points. There are $2^{(d-1)s}(2^{ds}-1)/(2^s-1)$ lines in $EG(d, 2^s)$. Every line has $2^{(d-1)s}-1$ lines parallel to it. For any point in $EG(d, 2^s)$, there are $(2^{ds}-1)/(2^s-1)$ lines intersecting at this point [7].

Let $GF(2^{ds})$ be the extension field of $GF(2^s)$. $GF(2^{ds})$ may be regarded as the $EG(d, 2^s)$. Let α be a primitive element of $GF(2^{ds})$. Then, $\{0, \alpha^0, \alpha^1, \cdots, \alpha^{2^{ds}-2}\}$ form the 2^{ds} points of $EG(d, 2^s)$. Given a line L and the line vector $v_L = (v_0, v_1, \cdots, v_{2^{ds}-2})$ be a binary $(2^{ds}-1)$-tuple with $v_i = 1$ if α^i is a point on L and $v_i = 0$ otherwise. Let B be a base matrix whose columns are the vectors v_L^T which are generated from all the lines in $EG(d, 2^s)$ that do not pass through the origin and whose rows correspond to the $2^{ds}-1$ non-origin points in $EG(d, 2^s)$. The rows are arranged in the order of $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{2^{ds}-2}$. Then B consists of $2^{ds}-1$ rows and $(2^{(d-1)s}-1)(2^{ds}-1)/(2^s-1)$ columns.

Since there are at most one line between two point, any two columns of B have at most one '1' in the same row. Consequently, the girth of B is 6. Let p_0 be the origin point and p_1 be any one non-origin point in the Euclidean geometry G, there are $(2^{ds}-1)$ choices for p_1 and there is a line $L_{(0,1)}$ connecting p_0 and p_1. Let p_2 be a point in G but not on $L_{(0,1)}$, there are $(2^{ds}-2^s)$ choices for p_2 and there is a line $L_{(0,2)}$ connecting p_0 and p_2 and a line $L_{(1,2)}$ connecting p_1 and p_2. Let p_3 be a point in G but not on $L_{(0,1)}$, $L_{(0,2)}$, and $L_{(1,2)}$, then there are $(2^{ds}-3\cdot 2^s+3)$ choices for p_3 (first exclude the $3\cdot 2^s$ points on $L_{(0,1)}$, $L_{(0,2)}$, and $L_{(1,2)}$, and then plus 3 again because p_0, p_1, and p_2 have been excluded two times) and there is a line $L_{(1,3)}$ connecting p_1 and p_3 and a line $L_{(2,3)}$ connecting p_2 and p_3. The three lines $L_{(1,2)}$, $L_{(2,3)}$, and $L_{(1,3)}$ enclose a triangle with p_1, p_2, and p_3 as the vertices. Thus the number of 6-cycles passing through the non-origin points is

$$\eta_6 = (2^{ds}-1)\cdot(2^{ds}-2^s)\cdot(2^{ds}-3\cdot 2^s+3)/6. \tag{3}$$

The $(2^{(d-1)s}-1)(2^{ds}-1)/(2^s-1)$ vectors v_L of lines that do not pass through the origin can be partitioned into

$$t = (2^{(d-1)s}-1)/(2^s-1) \tag{4}$$

cyclic submatrices $b_1, b_2, \cdots, b_t$ and each submatrices contains $(2^{ds}-1)$ vectors of lines. Let $b_1, b_2, \cdots, b_\delta$ be δ submatrices with $1 \le \delta \le t$. Now, the $M \times N$ base matrix B can be represented as

$$B = [b_1, b_2, \cdots, b_\delta] \tag{5}$$

where $M = 2^{ds}-1$ and $N = \delta(2^{ds}-1)$. Each of these δ cyclic submatrices contains $(2^{ds}-1)$ columns which are obtained by cyclic-shift any column in the submatrix $(2^{ds}-1)$ times. Consequently, B has a quasi-cyclic structure [7].

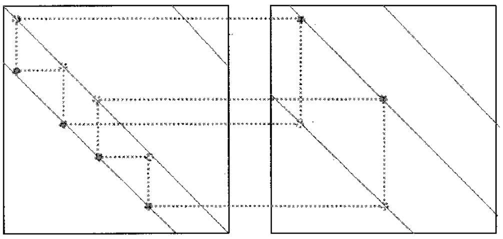

Fig. 1. Quasi-cyclic cycles in two submatices of S.

Lemma 1: If the base matrix B is constructed into the quasi-cyclic form as (5), then the cycles in the corresponding shifting matrix S are quasi-cyclic.

Proof: Since B has a quasi-cyclic structure, the row and column index pairs of '1's are quasi-cyclic. Then it is clear that the index pairs of cycles in B are also quasi-cyclic and therefore the corresponding cycles in S are quasi-cyclic. An example of quasi-cyclic cycles in two submatrices of S is shown in Fig. 1. □

The base matrix B has the following properties: 1) each column has weight $\rho = 2^s$; 2) each row has weight $\gamma = 2^s\delta$; 3) girth is 6; 4) the density of B is $2^s/(2^{ds}-1)$.

IV. DESIGN OF THE SHIFTING MATRIX S

In this section, we first analyze the girth of the proposed non-binary QC-LDPC codes and then introduce one method to optimize the shift values in S.

A. Girth of The Proposed LDPC Codes

After replacing each '1' in B with a shift value in the range $[0, q-2]$ and replacing each '0' with a "∞," a $M \times N$ shift matrix $S = [S_1, S_2, \cdots, S_\delta]$ is obtained.

It is stated in [8] that the necessary and sufficient condition for the existence of the cycle of length $2i$ represented is

$$\sum_{k=0}^{i-1}(a_{(m_k,n_k)} - a_{(m_{k+1},n_k)}) \equiv 0 \mod (q-1) \tag{6}$$

where $m_i = m_0$, $m_k \neq m_{k+1}$, $n_k \neq n_{k+1}$, $a_{(m_k,n_k)}$ and $a_{(m_{k+1},n_k)}$ are entries of S.

Theorem 1: If there are u overlaps between a block-cycle of length $2l$ and a block-cycle of length $2k$ in a QC-LDPC code, then there exists a cycle of length $2(2l+2k-u)$ which is twice the number of the distinct blocks in these block-cycles. Furthermore, the girth of the QC-LDPC code is at most $2(2l+2k-u)$.

Theorem 2: If the base matrix B is constructed based on the non-origin points and the lines passing through non-origin points in the Euclidean geometries over the Galois field $GF(2^s)$, the girth of the proposed non-binary QC-LDPC codes are lower bounded by 6 and upper bounded by 18.

Proof: Letting g_b denote the girth of B and g denotes the girth of H. It is obvious that the girth of H is at least the same as the girth of B, which means g is lower bounded by g_b. Then we get $6 \leq g$. Let u be the length of the overlaps between a cycle c_{2l} of length $2l$ and a cycle c_{2k} of length $2k$. It is clear that the length of the block-cycle in H which corresponds to the non-overlapped part between c_{2l} and c_{2k} is also at least g_b, which means

$$\begin{aligned}(2l-u)+(2k-u) &\geq g_b\\ l+k-g_b/2 &\geq u.\end{aligned} \tag{7}$$

According to Theorem 1 and (7), we have

$$\begin{aligned}2(2l+2k-u) &\geq 2(2l+2k-l-k+g_b/2)\\ &= 2l+2k+g_b,\end{aligned} \tag{8}$$

which means g is upper bounded by $2l+2k+g_b$. Since $2l \geq g_b$, $2k \geq g_b$, and $g_b = 6$, we get $g \leq 18$. The proof is completed. □

B. Shift Values Optimization

The shift values assigning method in the following guarantees the girth $g = 2i$ for the proposed non-binary QC-LDPC codes.

Step 1: Initially, each '1' in B becomes an undetermined shift value in S and each '0' in B becomes a "∞" in S.

Step 2: We assign the shift values in the range $[0, q-2]$, column by column, from 1 to N. For the n-th column, we consider the cycles on its left only. We denote the shift values in the n-th column from top to bottom as $a_{(m_k,n)}$, $k = 1, 2, \cdots, \rho$. If the assigned shift value $a_{(m_k,n)}$ forms cycles of length shorter than $2i$ with already existing shift values, we need to check whether the shift values on these cycles violate the condition (6). If condition (6) is met, we have to choose another nonnegative integer in the range $[0, q-2]$ for $a_{(m_k,n)}$. This process is repeated until condition (6) is not met for all the shift values in this column. For a column of ρ shift values, there are $(q-1)^\rho$ possible assignments.

According to Lemma III.1, cycles in S are quasi-cyclic. This property reduces the complexity of the cycle searching in S. For a given q, it is usually difficult to find shift values which guarantee the largest girth. However, if q is sufficiently large, it is always possible to prevent $2i-2$-cycles for $6 \leq 2i < 18$ by assigning the shift values such that all the sums of $i-1$ shift values are different from any other modulo $q-1$.

V. CONSTRUCTION OF THE NON-BINARY MATRIX H

Consider a Galois field $GF(q)$, where q is a power of two. Let α be a primitive element of $GF(q)$. Then, the powers of α, $\alpha^\infty = 0, \alpha^0, \alpha, \cdots, \alpha^{q-2}$, give all the elements of $GF(q)$ and $\alpha^{q-1} = 1$. The $q-1$ nonzero elements of $GF(q)$ form the multiplicative groups of $GF(q)$. For each nonzero element α^i with $0 \leq i \leq q-2$, we form a $(q-1)$-tuple over $GF(q)$, $z(\alpha^i) = (z_0, z_1, \cdots, z_{q-2})$, whose components correspond to the $q-1$ nonzero elements of $GF(q)$, where the ith component $z_i = \alpha^i$ and all the other $q-2$ components are equal to 0. The 0 element of $GF(q)$ is defined as the all-zero $(q-1)$-tuple, $(0, 0, \cdots, 0)$. This $(q-1)$-tuple is referred as the q-ary *location vector* of the field element α^i. For each entry $a_{(m,n)}$ of the $M \times N$ shifting matrix S, we expand it vertically into a $(q-1) \times 1$ vector $A_{(m,n)}$ by multiplying $\alpha^{a_{(m,n)}}$ with $\alpha^0, \alpha^1, \cdots, \alpha^{q-2}$ as follows:

$$A_{(m,n)} = \begin{pmatrix} \alpha^{a_{(m,n)}} \\ \alpha^{a_{(m,n)}}\alpha \\ \vdots \\ \alpha^{a_{(m,n)}}\alpha^{(q-2)} \end{pmatrix} \tag{9}$$

where α^∞ is defined as 0. Replacing each entry of $A_{(m,n)}$ by its q-ary *location vector*, we obtain a $(q-1) \times (q-1)$ matrix $h_{a_{(m,n)}}$ over $GF(q)$. Finally, we obtain the non-binary QC-LDPC matrix H as shown in (1). The null space over $GF(q)$ of H gives a non-binary QC-LDPC code C over $GF(q)$. Replace the nonzero entries of H with the nonzero elements of another Galois field $GF(q^*)$, then the matrix H^* over $GF(q^*)$ is obtained and the null space of H^* gives another non-binary LDPC code C^* over $GF(q^*)$. Replace the nonzero entries of H with the nonzero elements of another Galois field $GF(q^*)$, then the matrix H^* over $GF(q^*)$ is obtained and the null space of H^* gives another non-binary LDPC code C^* over $GF(q^*)$.

The non-binary matrix H and H^* have the following properties: 1) each column has weight $\rho = 2^s$; 2) each row has weight $\gamma = \delta 2^s$; 3) the girth is lower bounded by 6 and upper bounded by 18. 4) The code rate is at least $(\delta-1)/\delta$; 5) the non-binary minimum distance is at least $\rho + 1 = 2^s + 1$; 6) the density is $r = 2^s/(2^{ds}-1)(q-1)$.

VI. SIMULATION RESULTS

In the following, we use two examples to illustrate the construction of the proposed codes. A method to construct non-binary QC LDPC code based on points and parallel μ-flats in Euclidean geometry was presented in [5]. For comparison, we first construct a QC LDPC codes C_1 based on the methods introduced in [5]. Then, with our proposed approach, we construct two non-binary LDPC codes C_2 and C_2^* which have the rate and code length close to those of C_1. A binary code C_3 which has the same degree distributions and binary code length as C_2^* and designed by progressive edge-growth (PEG) algorithm is also given. For comparison, we have also consider the Shannon limit, uncoded BPSK and the sphere-packing bound [12]. The sphere-packing bound is for binary code length and code rate the same as C_2^*.

Example 1: Consider the 3-flats in the Euclidean geometry $EG(5,2)$ over $GF(2)$. Based on the method introduced in [5], we construct a 124×248 matrix H_1 over $GF(32)$. The null space of H_1 gives a 32-ary QC LDPC code C_1 with rate 0.528 and code length 248. To construct a code with rate and code length close to those of C_1, we consider the Euclidean geometry $EG(3,2)$ and choose the following parameters: $\delta = 4$, $q = 16$. With our proposed approach, we obtain a 105×210 matrix H_2 over $GF(16)$. The null space of H_2 gives a 16-ary QC LDPC code C_2 with rate 0.505 and code length 210. By replacing each

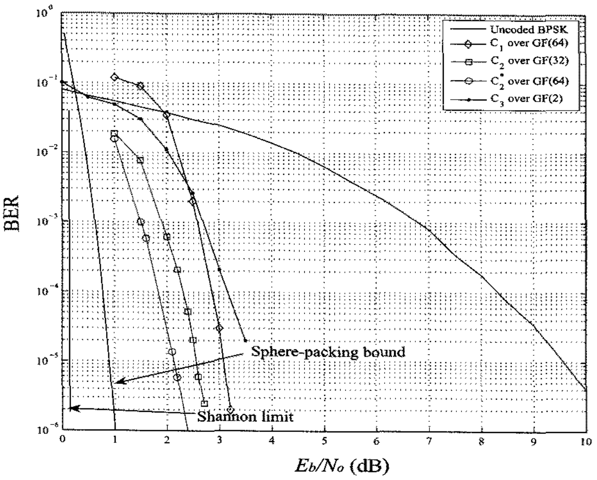

Fig. 2. Simulation results of example 1.

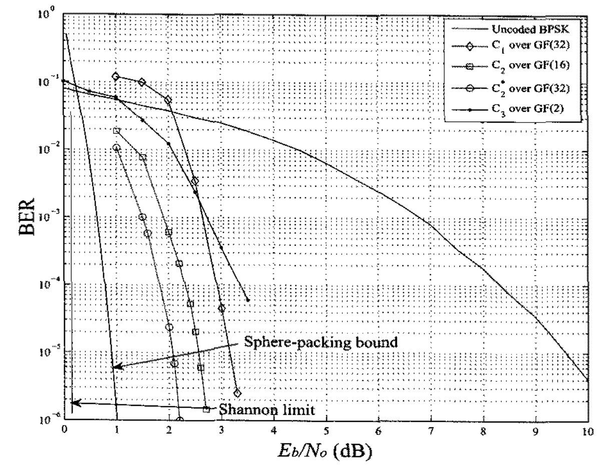

Fig. 3. Simulation results of example 2.

Table 1. A list of parameters of codes in example 1.

Code	Matrix size	Binary length	Density	$GF(q)$
C_1	124×248	1240	0.0313	$GF(32)$
C_2	105×210	840	0.0190	$GF(16)$
C_2^*	105×210	1050	0.0190	$GF(32)$
C_3	105×210	1050	0.0190	$GF(2)$

Table 2. A list of parameters of codes in example 2.

Code	Matrix size	Binary length	Density	$GF(q)$
C_1	124×248	1488	0.0313	$GF(64)$
C_2	105×210	1050	0.0190	$GF(32)$
C_2^*	105×210	1260	0.0190	$GF(64)$
C_3	105×210	1260	0.0190	$GF(2)$

nonzero entry of H_2 with a nonzero element of $GF(32)$, we obtain a matrix H_2^* over $GF(32)$. The null space of H_2^* gives a 32-ary LDPC code C_2^* with rate 0.5 and code length 210. From Fig. 2, we can see that the coding gains of 0.6dB and 1.0dB are achieved by C_2 and C_2^* over C_1, respectively, for a BER $= 10^{-5}$.

Example 2: Consider the 3-flats in the Euclidean geometry $EG(6,2)$ over $GF(2)$. Based on the method introduced in [5], we construct a 504 × 504 matrix H over $GF(64)$. Let H_1 be a 252 × 504 submatrix of H. The null space of H_1 gives a 64-ary QC LDPC code C_1 with rate 0.528 and code length 504. We consider the Euclidean geometry $EG(3,2)$ and choose the following parameters: $\delta = 4$, $q = 32$. With our proposed approach, we obtain a 217 × 434 matrix H_2 over $GF(32)$. The null space of H_2 gives a 32-ary QC LDPC code C_2 with rate $R = 0.502$ and code length 434. By replacing each nonzero entry of H_2 with a nonzero element of $GF(64)$, we obtain a matrix H_2^* over $GF(64)$. The null space of H_2^* gives a 64-ary LDPC code C_2^* with rate 0.5 and code length 434. From Fig. 3, we can see that the coding gains of 0.7 dB and 1.2 dB are achieved by C_2 and C_2^* over C_1, respectively, for a BER $= 10^{-5}$.

The complexities of the LDPC codes are not only dominated by the order of the $GF(q)$ but also by the densities of the parity-check matrices. Table I and Table II show sizes of parity-check matrices, binary code length, densities and the corresponding Galois field of all the simulated codes in examples 1 and 2, respectively.

VII. CONCLUSION

In this paper, an approach to the construction of non-binary QC-LDPC with large girth and low densities has been presented. First, we designed the base matrix B based on Euclidean geometries over $GF(2^s)$. Second, we analyzed the lower and upper bound of our proposed codes and introduce one method to optimize the shifting matrix S. Third, we construct the non-binary QC matrix H based on the shifting matrix S and multiplicative group of $GF(q)$. The proposed codes have girth $6 \leq g \leq 18$ and low densities $2^s/(2^{ds}-1)(q-1)$. Because of the low density, our codes have low decoding complexity. The simulation results show that substantial performance gains result from large girth. As girth increase, the BER of our proposed codes decrease.

REFERENCES

[1] R. G. Gallager, "Low density parity check codes," *IRE Trans. Inf. Theory*, IT-8, pp. 21–88, Jan. 1962.

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

[3] M. E. O'Sullivan, J. Brevik, and R. Wolski, "The performance of LDPC codes with large girth," in *Proc. 43rd Ann. Allerton Conf. Commun., Control, and Computing*, Monticello, IL, Sept. 2005.

[4] M. E. O'Sullivan "Algebraic construction of sparse matrices with large girth," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp, 718–727, Feb. 2006.

[5] B. Zhou, J. Kang, Y. Y. Tai, Q. Huang, and S. Lin, "High performance nonbinary quasi-cyclic LDPC codes on Euclidean geometries," in *Proc. IEEE MILCOM*, Orlando, Florida, Oct. 29–31, 2007, pp. 1–8.

[6] X. Jiang, C. Huang, Y. Guo, and M. Lee, "Non-binary LDPC codes design based on Euclidean geometries," in *Proc. IEEE ICITA*, pp. 452–456, Queensland, Australia, June 23–26, 2008.

[7] S. Lin and D. J. Costello, Jr., *Error Control coding: Fundamentals and Applications*, 2nd ed. Englewood Cliffs, NJ: USA, Prentice-Hall, 2004.

[8] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.

[9] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2894–2901, Aug. 2005.

[10] L. Barnault and D. Declercq, "Fast decoding algorithm for LDPC over $GF(2^q)$," in *Proc. ITW*, Paris, France, Mar. 31–Apr. 4, 2003, pp. 70–73.

[11] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over $GF(q)$," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 633–643, Apr. 2007.

[12] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels," *Inf. Contr.*, pt. I, vol. 10, no. 1, pp. 65–103, Feb. 1967.

Xueqin Jiang received the B.S. degree Nanjing Institute of Technology, Nanjing, Jiangsu, P. R. China, in computer science. He received the M.S. degree from Chonbuk National University, Jeonju, Korea, in communication engineering. He is currently working toward the Ph.D. degree in the Chonbuk National University. His research interests include LDPC codes and coding theory.

Moon Ho Lee received his B.S and M.S degree in Electrical Engineering from Chonbuk National University, Korea, in 1967 and 1976, respectively, and first Ph.D. degree in Electrical Engineering from Chonnam National University in 1984. Also he received his second Ph.D. degree in Information Engineering from the University of Tokyo in 1990. During August 1985 through August 1986, he studied at the University of Minnesota as a Post Doctor. Also Professional Engineer Licensed at 1981, Korea. From 1970-1980 he was a chief engineer at the Namyang Moonhwa Broadcasting company. Currently, he is a Professor of Division of Electronic and Information Engineering in Chonbuk National University.

His research interests is image processing, mobile communication, high speed communication networks, and information and algebra coding theory.