논문 2010-47TC-11-7

유클리드 기하학 기반의 넓은 둘레를 가지는 준순환 저밀도 패리티검사 코드

(Quasi-Cyclic Low-Density Parity-Check Codes with Large Girth Based on Euclidean Geometries)

이 미 성*, 지앙쉐에친**, 이 문 호***

(Mi Sung Lee, Xueqin Jiang, and Moon Ho Lee)

요 약

이 논문은 유클리드 기하학과 Circulant Permutation Matrices에서 병렬 구성을 기반으로 하는 Quasi-cyclic Low-density parity-check (QC-LDPC) 코드의 생성을 위한 하이브리드한 접근방식을 나타낸다. 이 방법으로 생성된 코드는 넓은 둘레(Large Girth)와 저밀도(Low Density)를 가진 규칙적인 코드로 나타내어진다. 시뮬레이션 결과는 이 코드들이 반복 복호(Iterative Decoding)를 통해 좋은 성능을 갖는것과 부호화되지 않은 시스템에서 좋은 코딩 이득을 달성하는 것을 보인다.

Abstract

This paper presents a hybrid approach to the construction of quasi-cyclic (QC) low-density parity-check (LDPC) codes based on parallel bundles in Euclidean geometries and circulant permutation matrices. Codes constructed by this method are shown to be regular with large girth and low density. Simulation results show that these codes perform very well with iterative decoding and achieve reasonably large coding gains over uncoded system.

Keywords: QC LDPC codes, Euclidean geometry, lines, points, circulant permutation matrices.

Ⅰ. Introduction

Recently, Euclidean geometries were successfully used to construct cyclic and quasi-cyclic LDPC codes for iterative decoding. Methods of construction are presented [1, 4~6]. LDPC codes constructed by these methods perform very well over the additive white Gaussian noise (AWGN), binary random and burst erasure channels. The construction of quasicyclic LDPC codes by combining parallel bundles and circulants of lines of finite geometries has been proposed in [1]. Let B be an $(p_1^{d_1 s_1}-1)\times(p_1^{d_1 s_1}-1)$ incidence matrix constructed from a d_1-dimensional Euclidean geometry $EG(d_1, p_1^{s_1})$. Let P_1, P_2, ... , P_τ be a set of τ $p_2^{(d_2-1)s_2}\times p_2^{d_2 s_2}$ incidence matrices of τ parallel bundles of lines from a d_2-dimensional Euclidean geometry $EG(d_2, p_2^{s_2})$. Replacing the 1-entries of B by the incidence matrices P_1, P_2, ... , P_τ, and the 0-entries by zero matrices, a QC parity check matrix H with the girth 6 and density $p_1^{s_1}/(p_1^{d_1 s_1}-1)p_2^{(d_2-1)s_2}$ is obtained. In this hybrid

* 정회원, *** 정회원 전북대학교 전기전자컴퓨터공학부 (Chonbuk National University)
** 정회원, 둥화대학교 정보통신기술대학 전자통신학과 (Donghua University)
※ 본 논문은 WCU R32-2009-000-200 14-0에 의하여 이뤄졌음
접수일자:2010년8월23일, 수정완료일: 2010년11월10일

construction, B is called the base matrix and the matrices P_j's with $1 \le j \le \tau$ are called the constituent matrices.

In this paper, we describe a new hybrid construction of QC LDPC codes with: 1) larger girth and 2) lower density by combining parallel bundles in Euclidean geometries and circulant permutation matrices constructed based on the multiplicative groups of finite fields. Because of the larger girth and the lower density properties, these codes have good bit error rate (BER) performance and lower encoding and decoding complexities. The construction of the proposed QC LDPC codes consists of three steps. First, construct a base matrix B based on parallel bundles in a d-dimension Euclidean geometry. Second, replace each 1-entry in the mth row and nth column of B with a positive integer $a_{(m,n)}$ in the range [1, q-1] and obtain a shift matrix S. Third, H is obtained by the combination of vertical and horizontal expansions of $a^{(a_{(m,n)}-1)}$'s and 0's as [5~7], where $a^{(a_{(m,n)}-1)}$ is a nonzero element of GF(q). Then each entry $a_{(m,n)}$ of S becomes a (q-1)×(q-1) circulant permutation matrix $P_{a_{(m,n)}}$ in H and each 0-entry of S becomes a (q-1)×(q-1) zero matrix in H. $P_{a_{(m,n)}}$ is also called the constituent matrix.

This paper is organized as follows. Two classes of base matrices B_I and B_{II} constructed from parallel bundles are introduced in Section II. In Section III, we analyze the lower and upper bound of girth of the proposed QC LDPC codes and present a shift value assigning algorithm for the design of the shift matrix S. Two classes of QC LDPC matrices H_I and H_{II} associated with B_I and B_{II} are constructed in Section IV. Examples of the proposed codes and their simulation results are given in Section V. Finally, Section VI concludes the paper.

II. DESIGN OF BASE MATRIX B

In this section, we will introduce two classes of base matrices constructed from the parallel bundles of lines and μ-flats in Euclidean geometries.

1. Class-I base matrix B_I

Let EG(d, p^s) be a d-dimensional Euclidean geometry over the Galois field GF(p^s), where p is a prime and d, s are two positive integers. This geometry consists of p^{ds} points, each point is simply a d-tuple over GF(p^s). A line in EG(d, p^s) consists of p^s points. There are $p^{(d-1)s}(p^{ds}-1)/(p^s-1)$ lines in EG(d, p^s). Every line has $p^{(d-1)s}-1$ lines parallel to it. For any point in EG(d, p^s), there are $(p^{ds}-1)/(p^s-1)$ lines intersecting at this point. Let GF(p^{ds}) be the extension field of GF(p^s). GF(p^{ds}) may be regarded as EG(d, p^s). Let α be a primitive element of GF(p^{ds}). Then $\{0, \alpha^0, \alpha^1, \dots, \alpha^{p^{ds}-2}\}$ form the p^{ds} points of EG(d, p^s). Let α^j be a nonorigin point in EG(d, p^s), then the p^s points

$$\{\beta\alpha^j\} \triangleq \{\beta\alpha^j : \beta \in GF(p^s)\}$$

form a line that pass through the origin in EG(d, p^s). Let α^i and α^j be two linearly independent points in EG(d, p^s). Then the collection of the following points:

$$\{\alpha^i + \beta\alpha^j\} \triangleq \{\alpha^i + \beta\alpha^j : \beta \in GF(p^s)\}$$

form a line in EG(d, p^s) that passes through the point α^i. Given a line L and the incidence vector $v_L^T = (v_0, v_1, \dots, v_{p^{ds}-1})$ of L be a binary p^{ds}-tuple with v_i =1 if the ith point of EG(d, p^s) is a point on L, and v_i=0 otherwise. Let the base matrix B_I be a matrix whose columns are the incidence vectors v_L of all the lines in EG(d, p^s) and whose rows correspond to the p^{ds} points in EG(d, p^s). Then B_I consists of p^{ds} rows and $p^{(d-1)s}(p^{ds}-1)/(p^s-1)$ columns.

Lemma 2.1: The base matrix B_I has the following two properties [4]:

1) girth: g_b = 6;

2) density: $r = 1/p^{(d-1)s}$.

A line and the $p^{(d-1)s}-1$ lines parallel to it are said to form a parallel bundle. There are $\gamma = (p^{ds}-1)/(p^s-1)$ bundles of parallel lines, and each

parallel bundle consists of $p^{(d-1)s}$ parallel lines. Let $b_1, b_2, \ldots, b_\delta$ be a set of δ $p^{ds} \times p^{(d-1)s}$ incidence matrices of δ parallel bundles of lines with $1 \le \delta \le \gamma$. Then we obtain the following base matrix:

$$B_I = [b_1, b_2, \ldots, b_\delta]. \quad (1)$$

2. Class-II base matrix B_{II}

Now, we extend the concept of lines to planes in EG(d, p^s)[4]. Let $g_0, g_1, \ldots, g_\mu$ be $\mu+1$ linearly independent points in EG(d, p^s), where $1 < \mu < d$. The p^{us} points of the form

$$g_0 + \beta_1 g_1 + \ldots \beta_\mu g_\mu$$

with $\beta_i \in GF(p^s)$ for $1 < i < \mu$, constitute a μ-flat that passes through the point g_0. The μ-flat that consists of the p^{us} points

$$\beta_1 g_1 + \ldots \beta_\mu g_\mu$$

passes through the origin. For any μ-flat passing through the origin, there are $p^{(d-\mu)s} - 1$ μ-flats in EG (d, p^s) parallel to it. The number of μ-flats in EG (d, p^s) is

$$p^{(d-\mu)s} \prod_{i=1}^{\mu} \frac{p^{(d-i+1)s} - 1}{p^{(\mu-i+1)s} - 1}.$$

Given a μ-flat F and the incidence vector $v_F^T = (v_0, v_1, \ldots, v_{p^{ds}-1})$ of F be a binary p^{ds}-tuple with v_i = 1 if the ith point of EG(d, p^s) is in F, and v_i = 0 otherwise. Let the base matrix B_{II} be a matrix whose columns are the incidence vectors v_F of all the μ -flats in EG(d, p^s) and whose rows correspond to the p^{ds} points in EG(d, p^s). Then B_{II} consists of p^{ds} rows and $p^{(d-\mu)s} \Pi_{i=1}^{\mu} (p^{(d-i+1)s} - 1)/(p^{(\mu-i+1)s} - 1)$ columns.

If g_μ is not in the $(\mu-1)$-flat $\{g_0 + \beta_1 g_1 + \ldots \beta_{\mu-1} g_{\mu-1}\}$, then the μ-flat $\{g_0 + \beta_1 g_1 + \ldots \beta_\mu g_\mu\}$ contains the $(\mu-1)$-flat $\{g_0 + \beta_1 g_1 + \ldots \beta_{\mu-1} g_{\mu-1}\}$. Let b_μ be a point not in $\{g_0 + \beta_1 g_1 + \ldots \beta_\mu g_\mu\}$. Then, the two μ-flats $\{g_0 + \beta_1 g_1 + \ldots \beta_\mu g_\mu\}$ and $\{g_0 + \beta_1 g_1 + \ldots \beta_\mu b_\mu\}$ intersect on $(\mu-1)$-flat $\{g_0 + \beta_1 g_1 + \ldots \beta_{\mu-1} g_{\mu-1}\}$ which means they have the $p^{(\mu-1)s}$ points in $\{g_0 + \beta_1 \alpha_1 + \ldots \beta_{\mu-1} g_{\mu-1}\}$ as their common points. Since $1 < \mu < d$, s is a positive integer and p is a prime, then $p^{(\mu-1)s} \ge p \ge 2$. Hence, $\{g_0 + \beta_1 g_1 + \ldots \beta_\mu g_\mu\}$ and $\{g_0 + \beta_1 g_1 + \ldots \beta_\mu b_\mu\}$ have at least two points in common and therefore the girth g_b of B_{II} is 4;

Lemma 2.2: The base matrix B_{II} has the following two properties:

1) girth: g_b = 4;

2) density: r = $1/(p^{(d-\mu)s})$.

There are $\gamma = \Pi_{i=1}^{\mu} (p^{(d-i+1)s} - 1)/(p^{(\mu-i+1)s} - 1)$ bundles of parallel μ-flats and each parallel bundle consists of $p^{(d-\mu)s}$ parallel μ-flats. Let $b_1, b_2, \ldots, b_\delta$ be a set of δ $p^{ds} \times p^{(d-\mu)s}$ incidence matrices of δ parallel bundles of μ-flats with $1 \le \delta \le \gamma$. Then we obtain the following base matrix:

$$B_{II} = [b_1, b_2, \ldots, b_\delta]. \quad (2)$$

Lemma 2.3: In each submatrix b_j of $B \in \{B_I, B_{II}\}$, where $1 \le j \le \delta$ all the column are incidence vectors of parallel bundles of lines and μ-flats, there are no two '1's in the same row. Therefore there is no cycle in b_j.

Ⅲ. DESIGN OF SHIFT MATRIX S

In this section, we first analyze the girth of the proposed QC LDPC codes and then introduce one simple shift value assigning algorithm.

1. Girth of The Proposed QC LDPC codes

After replacing each 1-entry in $B \in \{B_I, B_{II}\}$ with a shift value $a_{(m,n)}$, the shift matrix $S = [S_1, S_2, \ldots, S_\delta]$ is obtained, where $a_{(m,n)}$ means cyclic shift to the right by $(a_{(m,n)} - 1)$ positions. It is stated in [2] that in a QC LDPC code, the necessary and sufficient condition for the existence of the cycle of length 2i is

$$\sum_{k=0}^{i-1} ((a_{(m_k, n_k)} - 1) - (a_{(m_{k+1}, n_k)} - 1)) \equiv 0 \mod(q-1) \quad (3)$$

where $m_i = m_0$, $m_k \ne m_{k+1}$, $n_k \ne n_{k+1}$ and $a_{(m_k, n_k)}$ is

표 1. Girth와 Density 비교
Table 1. Girth and Density Comparisons.

	$EG(d_1, p_1^{s1})$	$EG(d_2, p_2^{s2})$	$EG(d, p^s)$	δ	q	Codeword length	Maximum achievable girth	Density
Codes in Example 8 [1]	$EG(2,5)$	$EG(3,2^3)$				12288	6	0.003255
Codes from H_I			$EG(6,2^1)$	16	25	12288	8	0.00130
Codes from H_I			$EG(5,2^1)$	16	49	12288	10	0.00130
Codes from $H_{II}(\mu=2)$			$EG(6,2^1)$	32	25	12288	6	0.00260

표 2. EG(3, 2)에서 Points와 Lines
Table 2. Points and Lines in EG(3, 2).

(a) Points in EG(3,2)

$0=(000)$, $\alpha_0=(001)$, $\alpha_1=(010)$, $\alpha_2=(011)$, $\alpha_3=(100)$, $\alpha_4=(101)$, $\alpha_5=(110)$, $\alpha_6=(111)$.

(b) Lines in EG(3,2)

$\{0,\alpha_0\}$	$\{\alpha_0,\alpha_1\}$	$\{\alpha_1,\alpha_3\}$	$\{\alpha_2,\alpha_6\}$
$\{0,\alpha_1\}$	$\{\alpha_0,\alpha_2\}$	$\{\alpha_1,\alpha_4\}$	$\{\alpha_3,\alpha_4\}$
$\{0,\alpha_2\}$	$\{\alpha_0,\alpha_3\}$	$\{\alpha_1,\alpha_5\}$	$\{\alpha_3,\alpha_5\}$
$\{0,\alpha_3\}$	$\{\alpha_0,\alpha_4\}$	$\{\alpha_1,\alpha_6\}$	$\{\alpha_3,\alpha_6\}$
$\{0,\alpha_4\}$	$\{\alpha_0,\alpha_5\}$	$\{\alpha_2,\alpha_3\}$	$\{\alpha_4,\alpha_5\}$
$\{0,\alpha_5\}$	$\{\alpha_0,\alpha_6\}$	$\{\alpha_2,\alpha_4\}$	$\{\alpha_4,\alpha_6\}$
$\{0,\alpha_6\}$	$\{\alpha_1,\alpha_2\}$	$\{\alpha_2,\alpha_5\}$	$\{\alpha_5,\alpha_6\}$

표 3. EG(3, 2)에서 Points와 2-FLATS
Table 3. Points and 2-FLATS in EG(3, 2).

(a) Points in EG(3,2)

$0=(000)$, $\alpha_0=(001)$, $\alpha_1=(010)$, $\alpha_2=(011)$, $\alpha_3=(100)$, $\alpha_4=(101)$, $\alpha_5=(110)$, $\alpha_6=(111)$.

(b) μ-flats in EG(3,2)

$\{0,\alpha_0,\alpha_1,\alpha_2\}$	$\{\alpha_3,\alpha_4,\alpha_5,\alpha_6\}$
$\{0,\alpha_1,\alpha_3,\alpha_5\}$	$\{\alpha_0,\alpha_2,\alpha_4,\alpha_6\}$
$\{0,\alpha_1,\alpha_4,\alpha_6\}$	$\{\alpha_0,\alpha_2,\alpha_3,\alpha_5\}$
$\{0,\alpha_2,\alpha_4,\alpha_5\}$	$\{\alpha_0,\alpha_1,\alpha_3,\alpha_6\}$
$\{0,\alpha_0,\alpha_3,\alpha_4\}$	$\{\alpha_2,\alpha_3,\alpha_4,\alpha_5\}$
$\{0,\alpha_0,\alpha_5,\alpha_6\}$	$\{\alpha_1,\alpha_4,\alpha_5,\alpha_6\}$
$\{0,\alpha_1,\alpha_2,\alpha_6\}$	$\{\alpha_2,\alpha_3,\alpha_6,\alpha_7\}$

an entry of S.

Theorem 3.1: [3] If there are u overlaps between a blockcycle of length $2l$ and a block-cycle of length $2k$ in a QC LDPC code, then there exists a cycle of length $2(2l+2k-u)$. Furthermore, the girth of the QC LDPC code is at most $2(2l+2k-u)$.

Theorem 3.2: Using the 6-girth matrix B_I as the base matrix, the girth of the QC LDPC code is lower bounded by 6 and upper bounded by 18. Otherwise, if using B_{II} as the base matrix, the girth of these codes are lower bounded by 4 and upper bounded by 12.

Proof: Letting g_b denote the girth of the base matrix B and g denotes the girth of the QC binary image of H. It is obvious that the girth of the QC binary image is at least the same as the girth of the base matrix B, which means g is lower bounded by g_b. Let $2l$ and $2k$ be length of two cycles in B, where $2l \geq g_b$, $2k \geq g_b$. Let u be the length of the overlaps between them. It is clear that the length of block-cycle corresponding to the non-overlapped part of the two cycles in B is also at least g_b, which means

$$(2l-u)+(2k-u) \geq g_b$$
$$l+k-g_b/2 \geq u. \quad (4)$$

According to Theorem 3.1 and equation (3), we have

$$2(2l+2k-u) \geq 2(2l+2k-l-k+g_b/2)$$
$$= 2l+2k+g_b, \quad (5)$$

which means g is upper bounded by $2l+2k+g_b$. Since $2l \geq g_b$, $2k \geq g_b$ and

$$g_b = \begin{cases} 6, & B=B_I; \\ 4, & B=B_{II}, \end{cases}$$

we have

$$g = \begin{cases} 6 \leq g \leq 18, & B=B_I; \\ 4 \leq g \leq 12, & B=B_{II}. \end{cases} \quad (6)$$

The proof is completed.

2. Shift Value Assigning Algorithm

The shift value assigning algorithm in the following guarantees the girth $g=2i$ for the proposed QC LDPC codes.

Step 1: Initially, all the shift values (positions of 1-entries in B) in the shift matrix S are undetermined.

Step 2: We can randomly assign positive integers in the range [1, q-1] for shift values in S_1.

Step 3: Go to the next undetermined column.

Assign the positive integer in the range [1, q-1] for each of the shift values one by one in this column. If the assigned shift value $a_{(m,n)}$ forms block-cycles of length shorter than $2i$ with already existing shift values, we need to check whether the positive integers of the shift values on these block-cycles violate the condition (3). If condition (3) is met, we have to assign another positive integer for that shift value $a_{(m,n)}$. This process is repeated until condition (3) is not met for all the shift values in this column. Go to the step 4.

Step 4: Stop if all the shift values in S are assigned, otherwise go to step 3.

According to lemma 2.3, there is no cycles in each b_j of B, where $1 \le j \le \delta$. Then it is clear that there is no block-cycle in each S_j of S, which lower the complexity of the block-cycle searching in S. In general, for a small q, it is not easy to check whether the existence of positive integers for shift values which guarantee the QC LDPC codes to have a large girth. Moreover, finding positive integers for shift values seems even more difficult. But, certainly such positive integers exist if we allow a sufficient large q.

Ⅳ. CONSTRUCTION OF QC-LDPC CODES

Consider a Galois field GF(q), where q is a power of a prime. Let α be a primitive element of GF(q). For each nonzero element α^i with $0 \le i \le q-2$, we form a (q-1)-tuple over GF(2), $z(\alpha^i)=(z_0, z_1, \cdots, z_{q-2})$, whose components correspond to the q-1 nonzero elements of GF(q), where the ith component $z_i = 1$ 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 location vector of the field element α^i. For each entry $a_{(m,n)}$ of a M×N shift matrix S, we expand it vertically into a (q-1)×1 matrix $A_{(m,n)}$ over GF(q) by multiplying $\alpha^{(a_{(m,n)}-1)}$ with α^0, α^1, … , α^{q-2} as follows:

$$A_{(m,n)} = \begin{pmatrix} \alpha^{(a_{(m,n)}-1)} \\ \alpha^{(a_{(m,n)}-1)}\alpha \\ \vdots \\ \alpha^{(a_{(m,n)}-1)}\alpha^{(q-2)} \end{pmatrix}, \quad (7)$$

where $\alpha^{(a_{(m,n)}-1)}$ is a nonzero element of GF(q). For each 0-entry in the m-th row and n-th column of the M×N shift matrix S, we expand it into a (q-1)×1 zero matrix $A_{(m,n)}$. This vertical expansion of a row into (q-1) rows is referred to as the multiplicative (q-1)-fold vertical expansion. Replacing each entry of $A_{(m,n)}$ by its location vector. We obtain a (q-1)×(q-1) matrix $h_{(m,n)}$ over GF(2). The replacement is referred to as the multiplicative (q-1)-fold horizontal expansion. Then we obtain the following M×N array of (q-1)×(q-1) circulant permutation and/or zero matrix:

$$H = \begin{pmatrix} h_{(1,1)} & h_{(1,2)} & \cdots & h_{(1,N)} \\ h_{(2,1)} & h_{(2,2)} & & \\ \vdots & \vdots & \cdots & h_{(2,N)} \\ h_{(M,1)} & h_{(M,2)} & \cdots & h_{(M,N)} \end{pmatrix}. \quad (8)$$

If the entry in the m-th row and n-th column of S is a nonzero entry $a_{(m,n)}$, $h_{(m,n)}$ is a (q-1)×(q-1) circulant permutation matrices. However, If the entry in the m-th row and n-th column of S is a 0-entry, $h_{(m,n)}$ is a (q-1)×(q-1) zero matrix. The null space over GF(2) of H gives a QC LDPC code C over GF(2). Associated with B_I and B_{II}, the QC LDPC matrices H also have two classes, H_I and H_{II}.

Lemma 4.1: The QC LDPC matrix H_I has the following two properties:

1) girth: $6 \le g \le 18$;

2) density: $r = 1/(p^{(d-1)s}q)$.

Lemma 4.2: The QC LDPC matrix H_{II} has the following two properties:

1) girth: $4 \le g \le 12$;

2) density: $r = 1/(p^{(d-\mu)s}q)$.

Note that if we allow a sufficient large q, then the short girth (i.e. 4,6) can be easily prevented and also when q is large, the densities of H_I and H_{II} are lower than the density of the hybrid constructed codes in [1].

Let EG($d_1, p_1^{s_1}$) and EG($d_2, p_2^{s_2}$) denote the Euclidean geometries from which the base matrices and the constituent matrices in Example 8[1] are constructed, respectively. To construct the QC LDPC codes which have the same code word length and code rate as the codes constructed in Example 8[1], we carefully choose the parameters q, δ and the Euclidean geometries EG (d, p^s) from which B_I and B_{II} are constructed. With the proposed hybrid approach, three QC LDPC codes are constructed. The maximum achievable girth and the density of these three codes and the codes in Example 8[1] are compared in Table I. From this table we can see that our codes have larger or equal girth and lower density.

V. SIMULATION RESULTS

In the following, we give two examples of the proposed QC LDPC codes. In computing the error performance, in terms of the BER, with iterative decoding using SPA, we assume binary phase-shift keying (BPSK) transmission over an additive white Gaussian noise (AWGN) channel.

Example 1: Consider the Euclidean geometry EG(3, 2) over GF(2), the points and the lines are given in Table II[4]. Based on the points and lines, we construct a 8 × 28 base matrix $B_I(\delta=7)$. With the shift values assigning algorithm and the parameter q = 128, shift value matrices S's for girth 6, 8, 10, 12 are constructed, respectively. H_I is obtained by vertical and horizontal expansions of the entries of B_I. Fig.1 shows the BER performance of their corresponding QC LDPC codes. For a $BER = 10^{-6}$ a coding gain of more than 5.5dB is achieved over uncoded BPSK system when the girth of the codes is 12.

Example 2: Consider the geometry EG(3, 2) over GF(2). There are fourteen 2-flats given in Table III[4]. Based on the points and 2-flats, we construct a 8 × 14 base matrix $B_{II}(\delta=7)$. With the shift values assigning algorithm and the parameter q = 256, shift value matrices S's for girth 6, 8 are constructed, respectively. B_{II} is obtained by vertical and horizontal expansions of the entries of B_{II}. Fig.2 shows the BER performance of their corresponding QC LDPC codes. For a $BER = 10^{-6}$, a coding gain of more than 7.5dB is achieved over uncoded BPSK system when the girth of the codes is 8.

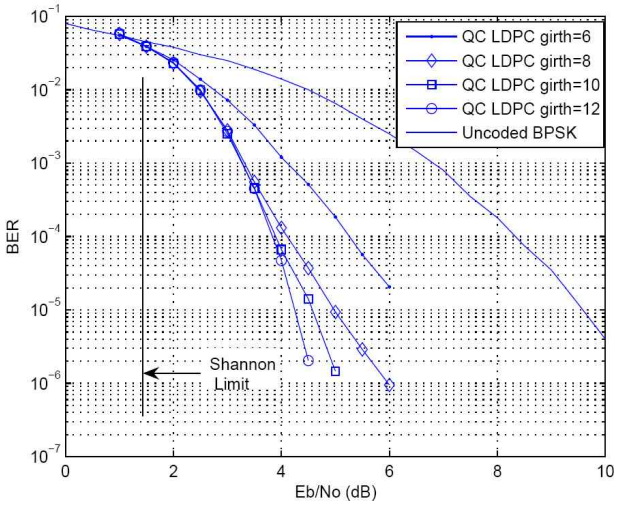


그림 1. 예제 1에서 QC LDPC의 성능
Fig. 1. Performance of QC LDPC codes in Example 1.

F(2), the points and the lines are given in Table II[4]. Based on the points and lines, we construct a 8 £ 28 base matrix B_I (± = 7). With the shift values assigning algorithm and the parameter q = 128, shift value matrices S's for girth 6, 8, 10, 12 are constructed, respectively. H_I is obtained by vertical and horizontal expansions of the entries of B_I . Fig.1 shows the BER performance of their corresponding QC LDPC codes. For a BER = 10 6 a coding gain of more than 5.5dB is achieved over uncoded BPSK system when the girth of the codes is 12.

Example 2: Consider the geometry EG(3; 2) over GF(2). There are fourteen 2-flats given in Table III[4]. Based on the points and 2-flats, we construct a 8 £ 14 base matrix B_{II} (± = 7). With the shift values assigning algorithm and the parameter q = 256, shift value matrices S's for girth 6, 8 are constructed, respectively. H_{II} is obtained by vertical and horizontal expansions of the entries of B_{II} . Fig.2 shows the BER performance of their corresponding QC LDPC

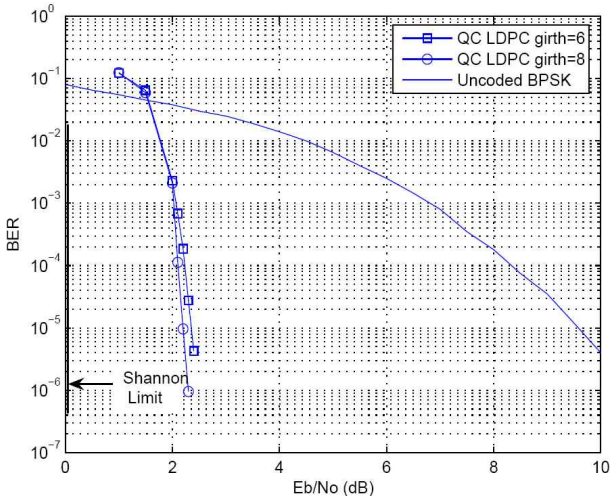


그림 2. 예제 2에서 QC LDPC의 성능
Fig. 2. Performance of QC LDPC codes in Example 2.

codes. For a BER = 10 6, a coding gain of more than 7.5dB is achieved over uncoded BPSK system when the girth of the codes is 8.

VI. CONCLUSION

Based on the parallel bundle of lines and μ-flats in EG(d, p^s), we construct the base matrices B's with girth 6 and 4, respectively. And based on the multiplicative groups of finite fields, we constructed the circulant permutation matrices. With these base matrices and the circulant permutation matrices, a hybrid approach to the construction of the QC LDPC codes has been presented. Codes of this class have larger girth and lower density than the hybrid constructed codes in [1], which means that our codes have good performance and lower coding complexity.

REFERENCES

[1] H. Tang, J. Xu, Y. Kou, S. Lin and K. Abdel-Ghaffar, "On Algebraic Construction of Gallager and Circulant Low-Density Parity-Check Codes," IEEE Trans. Inf. Theory, vol. 50. no. 6, pp, 1269-1279, June. 2004.

[2] 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.

[3] 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.

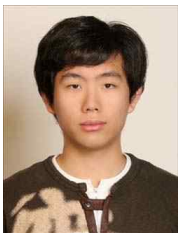
[4] S. Lin and D. J. Costello, Jr., Error Control coding: Fundamentals and Applications, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 2004.

[5] L. lan, L. Zeng, Y. 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. Inf. Theory, vol. 53. no. 7, pp, 2429-2458, July.2007.

[6] H. Tang, J. Xu, S. Lin and K. Abdel-Ghaffar, "Codes on Finite Geometries," IEEE Trans. Inf. Theory, vol. 51. no. 2, pp, 572-596, Feb.2005.

[7] S. Lin, S. Song, Y. Y. Tai, L. Lan and L. Zeng "Algebraic Constructions of Nonbinary Quasi-Cyclic LDPC Codes," Communications, Circuits and Systems Proceedings, vol. 2, pp,1303-1308, 25-28 June 2006.

저 자 소 개



이 미 성(정회원)
2009년 전북대학교 전자공학 학사
2009년 전북대학교 전자정보 공학부 석사 과정
<주관심분야 : 무선이동통신>

지앙쉐에친(정회원)
2006년 전북대학교 전자공학과 석사
2010년 전북대학교 전자공학과 박사
2010년~현재 둥화대학교 정보통신기술대학 전자통신학과 조교수
<주관심분야 : 무선이동통신>

이 문 호(정회원)
1967년 전북대학교 전자공학과 학사
1984년 전남대학교 전기공학과 박사
1990년 동경대학교 정보통신공학과 박사
1980년 10월~현재 전북대학교 전기전자컴퓨터 공학부 교수
<주관심분야 : 무선이동통신>