

논문 2005-42TC-8-1

재킷 행렬을 이용한 저밀도 부호의 구성

(Low Density Codes Construction using Jacket Matrices)

문명룡*, 이광재**, Hou Jia***, 황기연***, 이문호***

(Myung-Ryong Moon, Hou Jia, Gi-Yean Hwang, Moon-Ho Lee, and Kwang-Jae Lee)

요약

본 논문에서는 대수 이론과 관련된 일반화된 치환 행렬로부터 저밀도 부호의 명시적 구성을 고찰하였으며, 순환공식과 치환 행렬에 관한 재킷 역 블록 행렬을 설계하였다. 설계 결과로부터 제안 기법은 저밀도 부호를 얻기 위한 간단하며, 고속화된 기법임을 알 수 있다. 또한, π -회전 LDPC(low density parity check) 부호와 같은 구조화 LDPC 부호 역시 저밀도 재킷 역 블록 행렬임을 증명하였다.

Abstract

In this paper, the explicit low density codes construction from the generalized permutation matrices related to algebra theory is investigated, and we design several Jacket inverse block matrices on the recursive formula and permutation matrices. The results show that the proposed scheme is a simple and fast way to obtain the low density codes, and we also proved that the structured low density parity check (LDPC) codes, such as the π -rotation LPDC codes are the low density Jacket inverse block matrices too.

Keywords : LDPC, Jacket matrix, Hadamard.

I. 서론

부호이론의 관점에서, 매우 우수한 성능을 도출하기 위해 저밀도 부호를 통신이론에 적용할 수 있으며^[1-6], 이러한 목적에 부합하는 LDPC(low density parity check) 부호가 최근 주목 받고 있다. LDPC 부호는 선형 오류 정정 블록 부호 계열이며, 저밀도(sparse) 검사 행렬로서 정의된다. 각 부호어는 몇 가지 선형 제약 조건을, 부호어의 각 심벌은 소수의 제약 조건을 만족해야 한다^[5,6]. 또한, 터보(turbo) 부류의 복호 알고리즘, 즉

확률적 반복 복호 알고리즘 및 관련 이론은 선형 블록 부호를 샤논 한계(Shannon limit)에 근접하도록 하는데 도움이 될 수 있다. 한편, 재킷 변환(Jacket transform)은 Hadamard 행렬에서 확장되었지만 문헌 [7]의 저자에 의해 가장 보편적인 직교변환의 형태로 일반화 되었다. 특히, 고속 알고리즘의 개발 또는 재킷 변환을 이용한 통신 시스템의 개발 및 이의 행렬 구성을 위한 재킷 변환과 간단한 반복식(recursive formula)을 제시하였다. 행렬 순환은 기본 재킷 행렬과 연속적으로 감소하는 차수를 갖는 계수 행렬간의 곱의 형태가 된다. 이 구성은 재킷 행렬의 명확한 블록 순회 저밀도 행렬 분해(block circular sparse matrices factorization)를 제공한다. 재킷 행렬의 주요 특성은 이 행렬의 원소에 대한 역행렬이 매우 용이하게 얻어지며, 특별한 구조를 갖는다는 점이다. 재킷 행렬은 Hadamard 행렬과 관련된 하중 Hadamard 변환과 몇 개의 대칭 행렬을 이용하여 유도되며, 기존 DFT 기법과는 달리 단순 이진, 혼합 기저 인덱스 그리고 임의 크기의 변환 등으로 일반화 할 수

* 정회원, 전주공업대학
(Jeonju Technical College)

** 정회원, 한려대학교
(Hanlyo University)

*** 정회원, 전북대학교
(Chonbuk National University)

※ 본 논문은 한국산업기술재단의 지역혁신인력사업 및 과학기술부의 국제화사업, 전북대학교의 지원으로 이루어 졌음.

접수일자: 2005년3월14일, 수정완료일: 2005년8월13일

있다^[7,8].

본 논문에서는 재킷 행렬과 재킷 역 블록 행렬 (Jacket inverse block matrices)의 정의 위주로 설명하며, 재킷 행렬의 새로운 특성과 저밀도 부호(low density codes)에서의 응용에 대해 기술한다.

II. 치환 행렬에 의한 저밀도 부호의 생성

본 절에서는 먼저 재킷 행을 다음과 같이 정의한다.

<정의 1> 재킷 행렬(Jacket matrices)

$m \times n$ 크기의 행렬 $[J]_{m \times n}$ 의 경우, 이의 원소는 $[J]_{m \times n} = [L_{ij}]_{m \times n}$, $i = \{0, 1, \dots, m\}$, $j = \{0, 1, \dots\}$, 이 행렬의 역 형태는 단지 각 원소 단위의 역과 전치(transpose) 즉, $([J]_{m \times n})^{-1} = ([1/L_{ij}]_{m \times n})^T$ 의 관계를 갖는다. 여기서 $(x)^T$ 는 (x) 의 전치를 나타내며, 여기서 정규화 상수는 생략하였다.

재킷 행렬을 벡터 공간으로 표시하면 다음과 같다.

$$[J]_{m \times n} = \begin{bmatrix} L_0 \\ L_1 \\ M \\ L_{m-1} \end{bmatrix}, [J]_{m \times n}^{-1} = \frac{1}{C} \begin{bmatrix} 1/L_0 \\ 1/L_1 \\ M \\ 1/L_{m-1} \end{bmatrix}^T \quad (1)$$

여기서, C 는 정규화 상수, $L_i = (L_0, L_1, \dots, L_j)$, $1/L_i = (1/L_0, 1/L_1, \dots, 1/L_{n-1})$.

<보조정리 1> 대칭(symmetric) 직교 행렬의 원소가 균일한 경우, 이 대칭 직교 행렬은 재킷 행렬이다.

<증명> 대칭 직교 행렬의 근은 다음과 같이 주어진다.

$$\begin{bmatrix} a & b \\ b & -a \end{bmatrix} \begin{bmatrix} a & b \\ b & -a \end{bmatrix}^H = \begin{bmatrix} |a|^2 + |b|^2 & 0 \\ 0 & |a|^2 + |b|^2 \end{bmatrix} = (|a|^2 + |b|^2) I_2$$

$|a|^2 = |b|^2$ 이 균일한 경우, $\begin{bmatrix} a & b \\ b & -a \end{bmatrix}$ 은 다음과 같은 재킷 행렬이 된다.

$$\begin{bmatrix} a & b \\ b & -a \end{bmatrix} \begin{bmatrix} 1/a & 1/b \\ 1/b & -1/a \end{bmatrix} = \begin{bmatrix} 1+1 & \frac{a}{b} - \frac{b}{a} \\ \frac{b}{a} - \frac{a}{b} & 1+1 \end{bmatrix} = 2[I]_2$$

$$\text{여기서, } \frac{a}{b} - \frac{b}{a} = \frac{a^2 - b^2}{ab} = 0.$$

일반적으로, 대칭 직교 행렬은 이 정의를 만족할 수 있으며, 재킷 구성 법칙을 직교 설계에 적용할 수 있다^[5]. 그러나 원소 역 이론(element inverse theory)은 균일한 값을 갖는 영(零)이 아닌 원소에 대해서만 적용된다. 재킷 역 행렬에 관한 개념을 확장하기 위해서 다수의 블록 행렬로 구성되는 재킷 역 블록 행렬에 대해 고찰하며, 이 행렬 구성에서는 영(零)을 포함할 수 있다. 재킷 역 블록 행렬의 정의는 다음과 같다.

<정의 2> JIBM(Jacket inverse block matrices)

$m \times n$ 크기의 행렬 $[JB]_{m \times n}$, $i \in \{0, 1, 2, \dots, m-1\}$, $j \in \{0, 1, 2, \dots, n-1\}$ 에서 $[JB]_{m \times n} = [Lb_{ij}]_{m \times n}$ 이 성립하는 경우를 고려한다.

부 행렬 $Lb_{ij} = [lb_{gh}]_{k \times k}$ 는 $k \times k$ 정방 행렬, $g, h \in \{0, 1, \dots, k-1\}$ 이며, 원소 lb_{gh} 는 유한군 G_n 을 형성할 수 있다. $[JB]_{m \times n}$ 의 역 행렬은 블록의 역으로부터 용이하게 얻을 수 있다.

즉, $[JB]_{m \times n}^{-1} = ([Lb_{ij}]^{-1})_{m \times n}^T$ 와 같으며, 여기서 정규화 상수는 생략하였다.

예를 들어, 재킷 행렬을 다음과 같이 쓸 수 있다^[7].

$$[J]_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & i & -1 \\ 1 & i & -i & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, ([J]_4)^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -i & -1 \\ 1 & -i & i & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

여기서, 군 G_4 에 속하는 원소 $\{1, i, -1, -i\}$ 를 가지며, $i = \sqrt{-1}$ 이다. 이제 관련된 작은 재킷 행렬로서의 원소를 $g \in \{\pm 1, \pm i\}$ 로 정의하면, 앞서의 경우와 동일한 관계를 갖게 되므로 이렇게 구성된 행렬을 재킷 역 블록 행렬(JIBM)이라 부르기로 한다.

<정의 3> BJIBM(binary Jacket inverse block matrices)

원소 $lb_{gh} = GF(2)$ 인 경우 단지 $\{0, 1\}$ 만을 원소로 갖게 되며, lb_{gh} 를 원소로 하는 이러한 재킷 역 블록 행렬 $[JB]_{m \times n}$ 을 이진 재킷 역 블록 행렬(BJIBM)이라 부르기로 한다.

<정리 1> BJIBM을 $i \times i, i \times i, \dots$ 크기의 정방 행렬 $[JB]_i, [J]B, \dots$ 으로 다음과 같이 쓸 수 있으며

$$JB = [JB]_i \otimes [J]B \otimes [JB]_k \otimes \dots$$

이 또한 BJIBM이 된다. 여기서 \otimes 는 Kronecker 곱을 나타낸다.

본 논문에서는 저밀도 부호의 효율적인 설계를 위해 치환 행렬에 근거한 대칭 BJIBM을 구성하며, 이 경우 단지 정방 행렬만을 고려한다.

<정의 4> LDC(low density code)

저밀도 부호는 패리티 검사 행렬의 원소 중에서 “1”의 수가 부호 길이의 1/2 이하인 이진 부호이다. 또한, 비 이진 부호인 경우 역시 저밀도 이진 부호로 매핑될 수 있으며 저밀도 비 이진 부호로 정의된다.

본 논문에서는 BJIBM을 개발하기 위해서 적절한 대수 이론과 순환 함수(recursive function)로부터 일반화된 치환 저밀도 부호 구성을 유도하며, 대수 이론에 근거하여 지수부를 치환 행렬로 표시한다.

<정의 5> Group permutation matrices

곱셈 군(multiplication group) $G_p = \{0, 1, 2, \dots, p-1\}$ 와 관련된 단위 군(unit group) $\{\alpha^0, \alpha^1, \dots, \alpha^{p-1}\}$ 는 $p \times p$ 크기의 치환 행렬에 의해 나타낼 수 있으며, 여기서 p 는 소수(prime number)이다.

<정의 6> Permutation matrix representation

P -type 치환 행렬을 나타내며, 이는 $(p-1)$ -shift 치환 행렬로 $\{0, 1, 2, \dots, p-1\}$ -shift를 갖는다. 0-shift 치환 행렬은 $[I]_p$ 이며, 이는 다음과 같은 다항식으로 표시된다.

$$Y_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} a_{(i+p-j) \bmod p} x_i \right), \begin{cases} a_i = 1 & i = 0 \\ a_i = 0 & \text{others} \end{cases} \quad (2)$$

여기서, $a_i = \{0, 1\} \in GF(2)$. 그리고 $(p-1)$ -shift 치환 행렬은 다음과 같은 다항식으로 표시된다.

$$Y_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} a_{(i+p-j) \bmod p} x_i \right), \begin{cases} a_i = 1 & i = p-1 \\ a_i = 0 & \text{others} \end{cases} \quad (3)$$

본 논문에서 $p \times p$ 항등 행렬인 $\alpha^0 = [I]_p$ 과 $\alpha^1 = 1 - shift$ 치환 행렬을 고려한다.

$(\alpha^{p-k})(\alpha^k) = \alpha^p = [I]_k, k \in G_p$ 와 $(\alpha^k)^T = (\alpha^{p-k})$ 는 용이하게 검증할 수 있으며, 따라서 식 (3)은 다음과 같이 쓸 수 있다.

$$\left(Y_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} a_{(i+p-j) \bmod p} x_i \right) \right)_{\begin{cases} a_i = 1 & i = p-k \\ a_i = 0 & \text{others} \end{cases}}^T = Y_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} a_{(i+p-j) \bmod p} x_i \right)_{\begin{cases} a_i = 1 & i = k \\ a_i = 0 & \text{others} \end{cases}} \quad (4)$$

앞에서 소개한 개념에 따라 순환함수(Kronecker) 상에서의 BJIBM을 통해 저밀도 부호(LDC)를 유도한다.

<정의 7> BJIBM on permutation matrices

α^k 는 군 $\{\alpha^0, \alpha^1, \dots, \alpha^{p-1}\}$ 로부터의 $p \times p$ 치환 행렬이며, $i, j \in \{0, 1, 2, \dots, \frac{N}{p} - 1\}$ 인 정방 행렬 및 이의 역을 각각 $[JB]_N = [(a^k)_{ij}]$, $([JB]_N)^{-1} = [(\alpha^{-k})_{ij}]^T$ 이라 하면, 치환 행렬 상의 BJIBM 밀도는 $1/p$ 이며, p 가 증가함에 따라 이러한 종류의 행렬에서의 밀도는 매우 낮아지게 된다.

예 1) G_2 에서 군은 $\{\alpha^0, \alpha^1\}$, $p = 2$ 인 경우 기본 치환 행렬은 다음과 같으며,

$$\alpha^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \alpha^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \alpha^{-1} = \alpha$$

BJIBM은 다음과 같이 쓸 수 있고

$$[JB]_k = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix}, [JB]_k^{-1} = \begin{bmatrix} (\alpha^0) & (\alpha^0) \\ (\alpha^0) & (\alpha^{-1}) \end{bmatrix}^T \quad (5)$$

$$[JB]_k([JB]_k)^{-1} = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} = \begin{bmatrix} \alpha^0 + \alpha^0 & \alpha^0 + \alpha^1 \\ \alpha^0 + \alpha^1 & \alpha^0 + \alpha^0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

여기서 $\alpha^0 + \alpha^1 = 0$ 이다. 이진 행렬은 다음과 같이 표시되며, 이 행렬의 밀도는 $1/p = 1/2$ 이다.

$$[JB]_4 = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix}^{\Delta} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

이제, 정리 1을 토대로 반복 함수를 이용하여 다음과 같이 LDC를 구성할 수 있다.

$$[JB]_N = [JB]_{N/4} \otimes \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} \quad (6)$$

예 2) 크기 8의 JIBM은 다음과 같다.

$$[JB]_8 = [JB]_4 \otimes \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix}, \quad \text{단, } [JB]_4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

따라서 다음을 얻는다.

$$[JB]_8 = [JB]_4 \otimes \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix}^{\Delta} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix},$$

식 (6)에 대한 일반화된 밀도 함수는 다음과 같다.

$$\text{Density}(J_N) = \begin{cases} \frac{1}{2}, \text{if } N=2 \\ \frac{1}{2}, \text{if } N=4 \\ \frac{1}{4}, \text{if } N=4^n, n=2,3,4,\dots \\ \frac{1}{2} \times \frac{1}{(2)^{t-2}}, \text{if } N=2^t, t=3,5,7,9,\dots \end{cases} \quad (7)$$

따라서, 크기 2 및 4인 경우를 제외하면 이러한 모든 행렬은 저밀도 JIBM으로 볼 수 있다.

<정리 2> 크기 $m \times n$ 의 JIBM은 $n \times n$ JIBM에서 몇 개의 독립 부분블록을 삭제하여 얻을 수 있다.

<증명> $n \times n$ JIBM이 다음과 같이 주어진 경우,

$$[JB]_{n \times n} = \begin{bmatrix} Lb_{0,0} & Lb_{0,1} & \dots & Lb_{0,\frac{n}{p}-1} \\ Lb_{1,0} & Lb_{1,1} & \dots & Lb_{1,\frac{n}{p}-1} \\ \text{M} & \text{M} & & \text{M} \\ Lb_{\frac{n}{p}-1,0} & Lb_{\frac{n}{p}-1,1} & \dots & Lb_{\frac{n}{p}-1,\frac{n}{p}-1} \end{bmatrix}$$

이의 역은

$$[JB]_{n \times n}^{-1} = \frac{1}{C} \begin{bmatrix} 1/Lb_{0,0} & 1/Lb_{0,1} & \dots & 1/Lb_{0,\frac{n}{p}-1} \\ 1/Lb_{1,0} & 1/Lb_{1,1} & \dots & 1/Lb_{1,\frac{n}{p}-1} \\ \text{M} & \text{M} & & \text{M} \\ 1/Lb_{\frac{n}{p}-1,0} & 1/Lb_{\frac{n}{p}-1,1} & \dots & 1/Lb_{\frac{n}{p}-1,\frac{n}{p}-1} \end{bmatrix}^T$$

$$= \frac{1}{C} \begin{bmatrix} 1/Lb_{0,0} & 1/Lb_{1,0} & \dots & 1/Lb_{\frac{n}{p}-1,0} \\ 1/Lb_{0,1} & 1/Lb_{1,1} & \dots & 1/Lb_{\frac{n}{p}-1,1} \\ \text{M} & \text{M} & & \text{M} \\ 1/Lb_{0,\frac{n}{p}-1} & 1/Lb_{1,\frac{n}{p}-1} & \dots & 1/Lb_{\frac{n}{p}-1,\frac{n}{p}-1} \end{bmatrix}$$

따라서 다음의 관계를 얻을 수 있다.

$$\sum_{i=0}^{\frac{n-1}{p}-1} \sum_{j=0}^{\frac{n-1}{p}-1} (Lb_{i,j})(1/Lb_{i,j}) = \begin{cases} n & \text{if } l=i \\ 0 & \text{if } l \neq i \end{cases}$$

여기서 $C = n$, $l \in \{0, 1, \dots, \frac{n}{p} - 1\}$, 그리고 부분 블록 행렬 $Lb_{i,j}$ 의 크기는 $p \times p$ 이다.

이 $n \times n$ JIBM에서 독립 부분블록 k 의 한 줄을 삭제하기로 한다. 여기서 $k \in \{0, 1, \dots, n-1\}$ 이다. 결국, 다음과 같이 쓸 수 있으며,

$$[JB]_{(n-p) \times n} = \begin{bmatrix} Lb_{0,0} & Lb_{0,1} & \dots & \dots & \dots & Lb_{0,\frac{n}{p}-1} \\ Lb_{1,0} & Lb_{1,1} & \dots & \dots & \dots & Lb_{1,\frac{n}{p}-1} \\ \text{M} & \text{M} & & & & \text{M} \\ Lb_{k+1,0} & Lb_{k+1,1} & \dots & \dots & \dots & Lb_{k+1,\frac{n}{p}-1} \\ \text{M} & \text{M} & \dots & \dots & \dots & \text{M} \\ Lb_{\frac{n}{p}-1,0} & Lb_{\frac{n}{p}-1,1} & \dots & \dots & \dots & Lb_{\frac{n}{p}-1,\frac{n}{p}-1} \end{bmatrix}$$

이의 역은 다음과 같다.

$$[JB]_{(n-p) \times n}^{-1} = \frac{1}{C} \begin{bmatrix} 1/Lb_{0,0} & 1/Lb_{1,0} & \dots & 1/Lb_{k+1,0} & \dots & 1/Lb_{\frac{n}{p}-1,0} \\ 1/Lb_{0,1} & 1/Lb_{1,1} & \dots & 1/Lb_{k+1,1} & \dots & 1/Lb_{\frac{n}{p}-1,1} \\ \text{M} & \text{M} & \dots & \dots & \dots & \text{M} \\ \text{M} & \text{M} & \dots & \dots & \dots & \text{M} \\ \text{M} & \text{M} & \dots & \dots & \dots & \text{M} \\ 1/Lb_{0,\frac{n}{p}-1} & 1/Lb_{1,\frac{n}{p}-1} & \dots & 1/Lb_{k+1,\frac{n}{p}-1} & \dots & 1/Lb_{\frac{n}{p}-1,\frac{n}{p}-1} \end{bmatrix}$$

이의 조건은 다음과 같다.

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (Lb_{i,j})(1/Lb_{i,j}) = \begin{cases} n & \text{if } l=i \\ 0 & \text{if } l \neq i \end{cases}$$

여기서, $l \in \{0, 1, \dots, k-1\} \cup \{k+1, k+2, \dots, \frac{n}{p}-1\}$.

도출된 행렬 역시 JIBM임이 명확하며, 정리 2는 완벽하게 증명된다.

예 3) 다음과 같은 JIBM의 일반식에 대해 고찰한다.

$$[JB]_N = \begin{bmatrix} a & b & b & a \\ b & -c & c & -b \\ b & c & -c & -b \\ a & -b & -b & a \end{bmatrix}, [JB]_N^{-1} = \begin{bmatrix} 1/a & 1/b & 1/b & 1/a \\ 1/b & -1/c & 1/c & -1/b \\ 1/b & 1/c & -1/c & -1/b \\ 1/a & -1/b & -1/b & 1/a \end{bmatrix}$$

단, $N=4p$, a, b, c 는 크기 p 인 재킷 역 부분행렬이다. 행렬 $[JB]_N$ 에서 하나의 행을 삭제하면, 재킷 블록의 역은 다음과 같이 구해진다.

$$[JB]_{(N-p) \times N} = \begin{bmatrix} a & b & b & a \\ b & -c & c & -b \\ a & -b & -b & a \end{bmatrix}, [J]_{(N-p) \times N}^{-1} = \begin{bmatrix} 1/a & 1/b & & 1/a \\ 1/b & -1/c & & -1/b \\ 1/b & 1/c & & -1/b \\ 1/a & -1/b & & 1/a \end{bmatrix}$$

$n \times n$ JIBM의 크기 p 인 부분행렬에서 k 개의 독립된 열을 삭제하면, $(n - kp) \times n$ JIBM이 되며, 이의 조건은 다음과 같다(단, $0 < k < \frac{n}{p} - 2$).

$$\sum_{i=0}^{\frac{n}{p}-1} \sum_{j=0}^{\frac{n}{p}-1} (L_{b_{i,j}})(1/L_{b_{i,j}}) = \begin{cases} n & \text{if } l=i \\ 0 & \text{if } l \neq i \end{cases}$$

여기서, $l \in \{0, 1, \dots, \frac{n}{p}-1\}$ 부분행렬의 k 개의 독립 열은 제외한다.

일반적으로, 이 정리에 따라 어떤 크기의 재킷 블록의 경우라도 용이하게 구할 수 있다.

<보조정리 2> 치환 행렬 상의 동일한 부분행렬 크기 p 를 갖는 여러 가지 BJIBM $[JB]_{M_1}, [JB]_{M_2}, \dots$ 을 고려하자. 다음 조건을 만족하면, 행렬 $[JB]$ 는 밀도 $1/p$ 을 갖는 치환 행렬 상의 BJIBM이다.

$$JB = [JB]_{M_1} \otimes [JB]_{M_2} \otimes \dots \doteq [(a^k)_{ij}] \otimes [(a^k)_{mn}] \otimes \dots \tag{8}$$

단, $i, j \in \{0, 1, 2, \dots, \frac{N_1}{p}-1\}, m, n \in \{0, 1, 2, \dots, \frac{N_2}{p}-1\}$.

예 4) $[JB]_4 = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix}$ 은 치환 행렬 상의 BJIBM이고, $p=2$ 이며,

$$[JB]_8 = [JB]_4 \otimes [JB]_4 = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} \otimes \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 & \alpha^0 & \alpha^1 \\ \alpha^0 & \alpha^0 & \alpha^1 & \alpha^1 \\ \alpha^0 & \alpha^1 & \alpha^1 & \alpha^0 \end{bmatrix}$$

그리고 이의 역은 $[JB]_8^{-1} = [JB]_8$, 밀도는 $1/p = 1/2$ 이 된다.

2.1. Girth

식 (6) 및 식 (8)로 부터 얻어진 저밀도 BJIBM은 작은 girth를 갖는다. 반면에 군 G_p 상의 기본 BJIBM은 큰 girth의 저밀도 행렬이다.

예 5) G_3 상의 대략 $p=3$ 인 BJIBM을 고려하면, 기본 치환 행렬은 다음과 같이 주어진다.

$$\alpha^0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \alpha^1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \alpha^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

여기서,

$$\alpha^0 \times \alpha = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \alpha,$$

$$\alpha \times \alpha = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \alpha^2,$$

$$\alpha^2 \times \alpha = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \alpha^3 = 1.$$

이의 다항식 표현은 다음과 같으며

$$\alpha^2 + \alpha + 1 = 0 \tag{9}$$

이는 치환 행렬에 의해 다음과 같이 나타낼 수 있다.

$$\alpha^2 + \alpha + 1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \stackrel{\Delta}{=} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \stackrel{\Delta}{=} 0 \quad (10)$$

또한, 재킷 행렬은 다음과 같이 쓸 수 있으며

$$[JB]_b = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix}, \quad [JB]_b^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{bmatrix} \quad (11)$$

식 (11)로부터 다음 식을 얻을 수 있다.

$$[JB]_b \times [JB]_b^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} \quad (12)$$

따라서 BJIBM은 다음과 같이 구성된다.

$$[JB]_b = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} \stackrel{\Delta}{=} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (13)$$

크기 N의 치환 행렬 상의 정방 BJIBM의 최대 거리는 다음과 같이 주어지며,

$$d_{\max} = 2 \times \frac{N}{p}, \quad d_{\min} = 2 \times \frac{N}{p} - 2 \quad (14)$$

치환 행렬 상에서 기본 BJIBM이 이용된다면, girth는 증가되며, girth=4와 같은 작은 girth를 피할 수 있다.

식 (6)과 유사하게, 순환 구성을 위한 일반식은 다음과 같으며, 여기서 6×6은 포함되지 않는다.

$$[JB]_N = [JB]_{N/9} \otimes \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} \quad (15)$$

<보조정리 3> 6×6 BJIBM 구성은 G_3 와 G_2 재킷 블록의 조합으로 다음과 같이 나타낼 수 있다.

$$J_6 = J_2 \otimes J_3 \quad \text{또는} \quad J_6 = J_3 \otimes J_2 \quad (16)$$

따라서 이 행렬들을 다음과 같이 쓸 수 있다.

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} \otimes \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right\} \quad (17)$$

예 6) 18×18 저밀도 BJIBM은 다음과 같이 쓸 수 있다.

$$J_{18} = J_2 \otimes \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} \\ = \begin{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} & 0 \\ 0 & \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} \end{bmatrix}$$

III. JIBM에 의한 회전 치환 행렬의 구성

최근, 회전 치환 행렬 상의 LDPC 부호가 문헌 [9, 10]에서 제안되었으며, 본 논문에서 이러한 LDPC 부호가 BJIBM에 포함됨을 보인다.

<정의 8> π -회전 행렬

π -회전 행렬(π -rotation matrix)은 크기 p의 치환 행렬 R_π 이며, 뒤집힌(reverse) 항등 행렬이므로 π -회전 행렬의 다항식은 다음과 같이 주어진다.

$$Y_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} a_{(i+j) \bmod p} x_i \right), \quad \begin{cases} a_i = 1 & i = p-1 \\ a_i = 0 & \text{others} \end{cases} \quad (18)$$

역 행렬은 $(R_\pi)^{-1} = R_\pi$ 이다.

예 7) $p=3$ 인 π -회전 행렬은 다음과 같이 정의되며,

$$R_\pi = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad (19)$$

π -회전 부행렬 A, B, C, D 의 구성은 다음과 같다.

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$B = A \times R_\pi = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$C = R_\pi \times B = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$D = C \times R_\pi = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$R_\pi \times D = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = A$$

따라서 π -회전 LDPC 부호의 구성은 다음의 식에 근거하게 된다.

$$H = \begin{bmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{bmatrix}, \quad H^{-1} = \begin{bmatrix} A^{-1} & B^{-1} & C^{-1} & D^{-1} \\ B^{-1} & A^{-1} & D^{-1} & C^{-1} \\ C^{-1} & D^{-1} & A^{-1} & B^{-1} \\ D^{-1} & C^{-1} & B^{-1} & A^{-1} \end{bmatrix} \quad (20)$$

식 (20)은 다음의 관계를 이용하여 간단하게 검증할 수 있다.

$$\begin{aligned} HH^{-1} &= \begin{bmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{bmatrix} \begin{bmatrix} A^{-1} & B^{-1} & C^{-1} & D^{-1} \\ B^{-1} & A^{-1} & D^{-1} & C^{-1} \\ C^{-1} & D^{-1} & A^{-1} & B^{-1} \\ D^{-1} & C^{-1} & B^{-1} & A^{-1} \end{bmatrix} \\ &= \begin{bmatrix} N & Co_1 & Co_2 & Co_3 \\ Co_1 & N & Co_3 & Co_2 \\ Co_2 & Co_3 & N & Co_1 \\ Co_3 & Co_2 & Co_1 & N \end{bmatrix} = N[I] \end{aligned} \quad (21)$$

여기서 $N = AA^{-1} + BB^{-1} + CC^{-1} + DD^{-1}$ 은 정규화 상수이며, 상관 값은 다음과 같이 주어진다.

$$\begin{aligned} Co_1 &= AB^{-1} + BD^{-1} + CD^{-1} + DC^{-1}, \\ Co_2 &= AC^{-1} + BC^{-1} + CA^{-1} + DB^{-1} \\ Co_3 &= AD^{-1} + BC^{-1} + CB^{-1} + DA^{-1} \end{aligned} \quad (22)$$

<증명> $AB^{-1} + BA^{-1} = 0$ 이므로, 다음 관계는 명확하다.

$$Co_1 = AB^{-1} + BA^{-1} + CD^{-1} + DC^{-1} = 0$$

따라서 다음과 같이 쓸 수 있다.

$$Co_2 = AC^{-1} + BD^{-1} + CA^{-1} + DB^{-1} = 0$$

여기서,

$$AC^{-1} = A(R_\pi A R_\pi)^{-1} = A R_\pi^{-1} A^{-1} R_\pi^{-1} = (A R_\pi)(R_\pi A)^{-1} = B D^{-1}$$

유사한 방법으로 $CA^{-1} = D B^{-1}$ 를 얻을 수 있으며, $AD^{-1} = A(R_\pi A)^{-1} = A A^{-1} R_\pi = R_\pi$ 의 관계를 이용하면 다음 식을 얻을 수 있다.

$$Co_3 = AD^{-1} + BC^{-1} + CB^{-1} + DA^{-1} = 0$$

유사한 방법으로 다음의 관계를 얻을 수 있다.

$$AD^{-1} = BC^{-1} = CB^{-1} = DA^{-1} = R_\pi.$$

따라서 π -회전 행렬은 BJIBM의 일종이다.

<정리 3> A, B, C, D가 BJIBM이면, π -회전 행렬 H 또한 이진 재킷 역 블록 행렬(BJIBM)이다.

3.1. 구조화 LDPC

π -회전 등의 구조화 LDPC 부호 계열은 두 부분으로 구성되며, 하나는 H^m , 다른 하나는 H^p 이다. H^p 는 저밀도 재킷 역 블록 부호이며, H^m 은 다음과 같은 패턴을 갖는 $m \times m$ 행렬이다.

$$H^m = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

예 8) 구조화 LDPC 부호에 근거한 BJIBM은 다음 같이 구성될 수 있다.

$$H^p = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^2 & \alpha^1 \\ \alpha^0 & \alpha^1 & \alpha^2 \end{bmatrix}$$

단, $p = 3$ 이며, 도출된 LDPC 부호 행렬은 다음과 같다.

$$H = [H^a | H^p]$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

예 9) 문헌 [10]에 제시된 패턴에 따른 π -회전 LDPC 구성에서의 기본 행렬은 다음과 같이 쓸 수 있다.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & A & B & C & D \\ 1 & 1 & 0 & 0 & B & A & D & C \\ 0 & 1 & 1 & 0 & C & D & A & B \\ 0 & 0 & 1 & 1 & D & C & B & A \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

여기서, $p=3$ 이며 초기 행렬은 다음과 같다.

$$A = \mathbf{Y}_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} a_{(i+p-j) \bmod p} x_i \right), \begin{cases} a_i = 1 & i=1 \\ a_i = 0 & \text{others} \end{cases}$$

이는 치환 행렬 상의 특별한 BJIBM으로 볼 수 있다.

IV. BJIBM 상에서 재킷 LDPC 부호의 구성

$GF(p)$ 에 대한 기본 행렬로서 치환 행렬 상의 정방형 BJIBM이 다음과 같이 주어진 것으로 한다.

$$[JB]_p = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix} \quad (23)$$

정리 2를 이용하면, 큰 girth를 갖는 비정방형 저밀도 행렬을 용이하게 얻을 수 있다.

예 10) 식 (23)에 근거하여 변형된 LDPC 부호의 한 가지

경우를 다음과 같이 쓸 수 있다.

$$[MJ]_{6 \times 9} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \end{bmatrix} \quad (24)$$

여기서 $p=3$ 이며, 이의 역은 다음과 같이 쓸 수 있다.

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & \alpha \\ 1 & \alpha^2 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$$

LDPC 부호는 다음과 같이 정의 된다.

$$[MJ]_{6 \times 9} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (25)$$

이 행렬의 girth는 8이며, 거리는 다음과 같다.

$$d_{\max} = 2 \times \frac{N}{p} = 2 \times \frac{9}{3} = 6, \quad d_{\min} = 2 \times \frac{N}{p} - 2 = 4 \quad (26)$$

예 11) 15×20 LDPC 부호를 설계하기 위해서는 $p=5$ 로 하면 된다. 25×25 치환 행렬 상의 기본 BJIBM은 다음과 같이 쓸 수 있다.

$$[JB]_{25 \times 25} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha & \alpha^3 \\ 1 & \alpha^3 & \alpha & \alpha^4 & \alpha^2 \\ 1 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix} \quad (27)$$

위의 예와 유사하게 15×20 LDPC 부호를 얻기 위해 몇 개의 열을 삭제할 수 있다. 이 경우에는 첫째 열과 마지막 열, 그리고 마지막 행을 삭제한다. 따라서 변형 재킷 블록 행렬을 다음과 같이 쓸 수 있으며,

$$[MJ]_{15 \times 20} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha \\ 1 & \alpha^3 & \alpha & \alpha^4 \end{bmatrix} \quad (28)$$

제안 재킷 LDPC 부호의 구성은 다음과 같으며, 일반적인 LDPC 부호와의 차이점을 표 1에 나타내었다.

표 1. 제안 재킷 LDPC 부호
Table 1. Proposed Jacket LDPC Codes.

	LDPC	Jacket LDPC
Type of applications	Parity Check COdes for Error Correcting	Algebra Codes for Error Correcting or Orthogonal Transform
Matrix	Non-square	Square and Non-square
Encoding	Higher Complexity	Simple and Fast
Construction	Random	Recursive

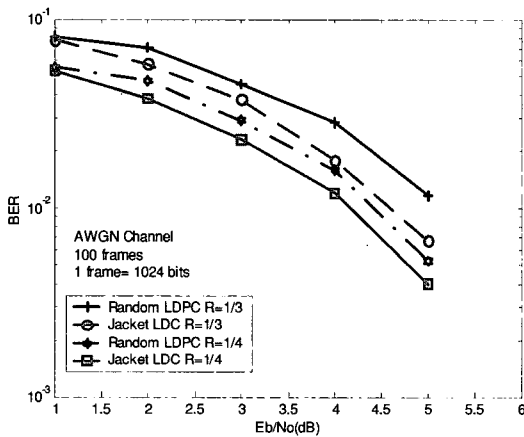


그림 1. 재킷 LDPC 부호의 성능
Fig. 1. Performance of Jacket LDPC codes.

$$[M]_{15 \times 20} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

이의 girth는 8이며, 거리는 다음과 같다.

$$d_{\max} = 2 \times \frac{N}{p} = 2 \times \frac{20}{5} = 8, \quad d_{\min} = d_{\max} - 2 = 6$$

IV. 결 론

본 논문에서는 재킷 행렬을 이용한 저밀도 부호의 구성 방법을 제시하였다. 제안 기법에 의해 우수한 저밀

도 부호를 효율적으로 제공할 수 있음을 확인하였으며, 대부분의 구조화 LDPC 부호들 또한 이러한 집합에 속하는 것을 명확하게 알 수 있다. 제시된 방법으로 보다 큰 girth를 갖는 LDPC 부호를 발굴 또는 생성할 수 있을 것으로 기대된다.

참 고 문 헌

- [1] R. G. Gallager, "Low density parity check codes," PhD thesis, MIT, Cambridge, Mass., September, 1960.
- [2] R. G. Gallager, "Low density parity check codes," Number 21 in research monograph series. MIT Press, Cambridge, Mass., 1963.
- [3] M. C. Davey and D.J.C. Mackay, "Low density parity check codes over GF(q)," IEEE Communication Letters, vol.2, no.8, pp.165-167, June 1998.
- [4] M. C. Davey and D.J.C. Mackay, "Low density parity check codes over GF(q)," In Proc. of the 1998 IEEE Information Theory Workshop, pp.70-71, IEEE, June, 1998.
- [5] S. Hui, J. Bond, and H. Schmidt, "Constructing low density parity check codes with circulant matrices," In Proc. of the 1999 IEEE Information Theory Workshop, pp.50, 1999. Greece, June 17-July 1, 1999.
- [6] D.J.C Mackay, "Good error correcting codes based on very sparse matrices," IEEE Trans. on Information Theory, vol.45, no.2, pp.399-431, 1999.
- [7] Moon Ho Lee, B. Sunder Rajan and J. Y. Park, "A generalized reverse jacket transform," IEEE Trans. Circuits Syst. II, vol. 48, no.7, 2001, pp. 684-690.
- [8] Moon Ho Lee, "A New Reverse Jacket Transform and Its Fast Algorithms," IEEE Trans. on CAS-2 Vol.47. No.1 Jan. 2000.
- [9] Li Ping, W.K. Leung, and Nam. Phemdo, "Low density parity check codes with semi-random parity check matrix," Electronics Letters, vol.35, no.1, pp. 38-39, Jan. 1999.
- [10] Rich Echard, and S.C. Chang, "Deterministic π -rotation low density parity check codes," Electronics Letters, vol.38, no.10, pp.464-465, 2002.
- [11] Dariush Divsalar, Hui Jin, and Robert J. McEliece, Coding theorems for turbo-like codes, Proceedings of the 36th Allerton Conference on Communication, Control and Computing (1998), 201-210.
- [12] D. J. C. Mackay, "Good Error-Correcting Codes Based on Very Sparse Matrices," IEEE Trans.

Information. Theory, vol. 45, pp. 399-431, Mar. 1999.

저 자 소 개



문 명 룡(정회원)
1982년 조선대학교 전기공학과
학사
1984년 조선대학교 전기공학과
석사
2005년 전북대학교 영상정보과
박사

1990년~현재 전주공업대학 디지털전기정보과
교수
<주관심분야 : 전파 측정, 무선 네트워크, 부호
이론>



이 광 재(정회원)
1986년 전북대학교 전자공학과
학사
1990년 전북대학교 전자공학과
석사
1995년 전북대학교 전기공학과
박사수료

1995년 3월~현재: 한려대학교 멀티미디어
정보통신공학과 전임강사
<주관심분야 : 이동통신, 오류정정부호, UWB>



Jia Hou(정회원)
1992년 중국우한대학교
통신공학과 학사
2002년 전북대학교 정보통신
공학과 석사
2005년 전북대학교 정보통신
공학과 박사

2005년~현재 전북대학교 정보통신공학과
포스트닥터
2005년 2월~현재: 중국 수조대학 부교수
<주관심분야 : 이동통신, 정보이론, UWB>



황 기 연(정회원)
1998년 서남대학교 전자공학과
학사
2001년 서남대학교 컴퓨터정보통
신학과 석사
2002년~현재 : 전북대학교 정보
통신공학과 박사과정

<주관심분야 : 이동통신, LDPC, 채널코딩>



이 문 호(정회원)
1967년 전북대학교 전자공학과
학사
1984년 전남대학교 전기공학과
박사 (통신기술사)
1990년 동경대학교 정보통신공학
과 박사

1984년~1985년 미국 미네소타대 전기과
포스트닥터
1980년 10월~현재 전북대학교 전자정보공학부
교수
<주관심분야 : 이동통신, 정보이론, UWB>