LDPC 부호 적용을 위한 Tanner의 최소 거리 바운드의 일반화

정회원 신 민 호*, 준회원 김 준 성*, 종신회원 송 홍 엽*

Generalization of Tanner's Minimum Distance Bounds for LDPC Codes

Min-Ho Shin*, Joon-Sung Kim*, Hong-Yeop Song* *Regular Members*

요 약

LDPC 부호의 검사행렬은 비트노드와 검사노드간의 이분 그래프로 표현된다 Tanner는 그래프상의 인접 행렬(adjacency matrix) 고유값을 이용하여, 균일 LDPC 부호의 최소 거리 하한식(minimum distance bound)을 유도하였다. 본 논문에서는 Tanner의 결과를 일반화하여, 균일 및 블록 구조를 갖는 비균일 LDPC부호에 적용 가능한 두개의 최소 거리 하한식을 유도한다 첫 번째는 최소 거리 부호어에 인접한 비트노드들의 관계를 통하여 유도되는 비트노드 기반 하한식이고, 두 번째는 최소 거리 부호어와 연접한 검사노드들의 관계에서 얻어지는 검사노드 기반 하한식이다. 본 논문에서 유도한 하한식을 통하여 블록 구조를 갖는 비균일 LDPC부호의 거리 특성을 그래프의 고유값들과의 관계로 나타낼 수 있다

Key Words LDPC codes, bit-oriented bound, parity-oriented bound, Tanner graph

ABSTRACT

LDPC(Low Density Parity Check) codes are described by bipartite graphs with bit nodes and parity-check nodes. Tanner derived minimum distance bounds of the regular LDPC code in terms of the eigenvalues of the associated adjacency matrix In this paper we generalize the Tanner's results We derive minimum distance bounds applicable to both regular and blockwise-irregular LDPC codes. The first bound considers the relation between bit nodes in a minimum-weight codeword, and the second one considers the connectivity between parity nodes adjacent to a minimum-weight codeword. The derived bounds make it possible to describe the distance property of the code in terms of the eigenvalues of the associated matrix.

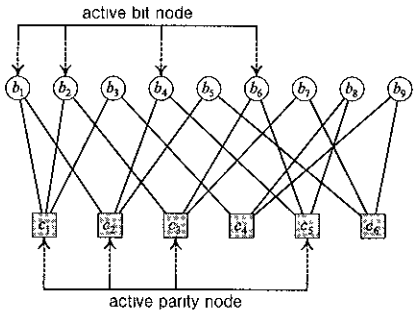
I 서 론

LDPC 부호(low density parity check codes)는 1962년 Gallager에 의해 처음 제안되었으며, 1990대 중반에 Mackay와 Neal에 의해 재발견된 이래 Shannon의 이론적 채널 용량 한계에 근접하는 성능을 가진 부호로서 많은 연구가 진행되어 오고 있다.[1][2][3][4] 1990년 중반 이후 Luby 등은 균일 LDPC 부호보다 성능이 우수한 비균일 LDPC 부호를 제안하였고, Richardson 등은 비균일 LDPC 부호의 점근적인 성능을 분석한 밀도 진화 기법(density evolution)을 소개하여 이용하여 터보 부호의 성능을 능가하는 매우 우수한 부호들이 연구되어 오고 있다[3][4] 하지만, LDPC부호의 최소 거리

* 연세대학교 전기·전자공학과 부호 및 정보이론 연구실({mh shin, js kim, hy song}@coding yonsei ac kr)
논문번호 KICS2004-07-096, 접수일자 2004년 7월 12일
※본 연구는 삼성종합기술원의 "4G wireless system의 연구 개발" 과제의 지원에 의해 이루어졌음

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

(a) LDPC 부호의 검사행렬 예제



(b) LDPC 부호의 이분 그래프 표현

그림 1 LDPC 부호의 검사행렬 예제와 이분 그래프 표현

바운드(minimum distance bound)와 거리 특성에 대해서는 많은 연구가 이루어지지 못하였다. 이에 Tanner는 그래프상에서 노드들과 최소 거리 부호어와의 관계를 이용하여, 균일 LDPC 부호의 최소 거리 하한식을 그래프의 고유값의 관계로 유도하였다.[2]

본 논문에서는 Tanner의 결과를 확장하여, 균일 및 블록 구조를 갖는 비균일 LDPC 부호에 적용 가능한 최소 거리 하한식을 유도한다 첫 번째 하한식은 최소 거리 부호어와 인접한 비트노드들 관계를 통하여 유도되는 비트노드 기반 바운드이고, 두 번째는 최소 거리 부호어와 인접한 검사노드들의 관계에서 얻어지는 검사노드 기반 바운드이다. 본 논문에서 유도한 하한식을 통하여 균일 및 블록 구조를 갖는 비균일 LDPC부호의 거리 특성을 그래프의 고유값들과의 관계로 나타낼 수 있으며, LDPC 부호의 설계에 있어서 척도로 활용할 수 있다

II Tanner의 최소 거리 바운드

LDPC 부호는 패리티 검사 행렬 H의 원소들이 대부분 '0'인 선형 블록 부호(linear block code)이다. 검사행렬 H가 $m \times n$행렬인 LDPC 부호는 검사노드의 개수가 m이고 비트노드의 개수가 n인 이분 그래프(bipartite graph)로 생각할 수 있다.[2][6]

이분 그래프는 $B=(V_b \cup V_c, E)$로 표현되며, 여기서 V_b는 비트 노드들의 집합 $V_b=\{b_1, b_2, \cdot, b_n\}$이고, V_c는 검사 노드들의 집합 $V_c=\{c_1, c_2, \cdots, c_m\}$이다 또한 변집합(edge set) E는 행렬 H의 0이 아닌 원소 h_{ij}에 해당하는 $V_c \times V_b$상의 순서쌍 (c_i, b_j)들로 이루어진 집합이다.[6]

이분 그래프의 연결성(connectivity)은 노드 i가 j번째 노드에 해당하는 변(edge)에 연결 되어 있으면 행렬의 원소 $a_{ij}=1$ 그렇지 않으면 원소 $a_{ij}=0$인 $(m+n) \times (m+n)$ 연접 행렬(adjacency matrix) A로 나타내어진다 따라서 연접 행렬 A는 다음의 수식으로 나타낼 수 있다.

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix}$$

Tanner는 LDPC 부호의 최소 거리 부호어(minimum-weight word)와 이분 그래프상의 서브그래프(subgraph)의 특성을 분석하여 바운드를 유도하였다. 여기서 최소 거리 부호어의 1의 위치에 해당하는 노드들을 활성 비트 노드(active bit node)라 정의하며, 활성 노드에 입사되는(incident on) 변들을 활성 변(active edge)이라 정의한다 검사 노드 중에서 최소한 하나의 활성 변을 가진 노드들을 활성 검사 노드(active parity node)라고 정의한다 그림1에서는 LDPC 부호의 검사행렬 예제와 그에 따른 이분 그래프를 예시하였다. 그림1에서는 최소 무게 부호어 (110101000)에 따른 활성 비트 노드와 활성 검사 노드를 표시하였다

Tanner는 위와 같은 부호와 그래프와의 관계 분석을 통하여 다음 두개의 하한식을 유도하였다 검사행렬 H가 $m \times n$ 행렬이고, 고정 열무게(fixed column weight) γ, 고정 행무게(fixed row weight)

ρ를 갖는 균일 LDPC라 하고, μ_1, μ_2를 각각 행렬 HH^T의 최대 고유값, 두 번째로 큰 고유값이라고 하자. 그러면 비트 노드 기반 하한식은[2, Theorem 3.1]

$$d \geq \frac{n(2\gamma-\mu_2)}{\mu_1-\mu_2}$$

이 되고, 검사 노드 기반 하한식은[2, Theorem 4.1]

$$d \geq \frac{2n(2\gamma+\rho-2-\mu_2)}{\rho(\mu_1-\mu_2)}$$

이 된다. Tanner의 최소 거리 바운드는 균일 LDPC 부호에 있어서 거리 특성을 그래프의 고유값들로 표현함으로써, μ_2/μ_1이 작을수록 보다 좋은 거리 특성을 갖는다는 발견적 규칙(heuristic rule)을 세웠다.

III. 일반화된 최소 거리 바운드

Tanner의 바운드는 균일 LDPC 부호에만 적용된다. 이에 본 절에서는 Tanner의 결과를 확장하여 블록 구조를 갖는 비균일 LDPC 부호에 적용 가능한 하한식을 유도한다.

정리1(비트 노드 기반 하한식). 연결된 그래프 구조를 갖는 검사 행렬 H가 $H=[H_1, H_2, \cdots, H_p]$이고, 실수 행렬 H^TH의 순서적으로 나열된 고유값들이 $\mu_1 > \mu_2, > \cdots > \mu_s$라고 하자. 여기서 각 H_i는 $m \times n$행렬이고, 고정된 열무게 γ_i, 고정된 행무게 ρ_i를 각각 가지며, $\gamma_1 < \gamma_2 < \cdots < \gamma_p$라고 가정하자. 그러면 검사 행렬 H를 갖는 부호는 다음의 최소 거리 바운드를 만족한다.

$$d \geq \frac{(2\gamma_1-\mu_2)n\sum_{i=1}^{p}\gamma_i^2}{\gamma_p^2(\sum_{i=1}^{p}\rho_i\gamma_i-\mu_2)}$$

증명: 최소 무게 부호어(minimum-weight codeword)에 따른 길이 pn인 실수 벡터 c를 부호어가 0이 아닌 위치에 1의 값을, 0의 위치에 0의 값을 갖는 벡터로 정의하자. H^TH의 첫 번째 고유벡터 $e_1 = (\gamma_1, \cdots, \gamma_1, \gamma_2, \cdots, \gamma_2, \cdots, \gamma_p, \cdots, \gamma_p)^T / \sqrt{n\sum_{i=1}^{p}\gamma_i^2}$이 되고, 이에 따른 고유값은 $\mu_1 = \sum_{i=1}^{p}\rho_i\gamma_i$이 된다. 또한 연결된 그래프를 가정하였으므로 Perron-Frobenius의 정리에 따라 이 고유값은 유일하다.[5] d_i가 최소 무게 부호어 c에서 H_i에 따른 n 구간씩에서의 1의 개수라고 하자. 그리고 c_i가 c의 i번째 공간에 대한 투영(projection) 벡터라고 하자. 그러면

$$c^Tc = \|c\|^2 = d, \qquad (1)$$

$$\|c_i\|^2 = \frac{(\sum_{i=1}^{p}d_i\gamma_i)^2}{n\sum_{i=1}^{p}\gamma_i^2} \leq \frac{d^2\gamma_p^2}{n\sum_{i=1}^{p}\gamma_i^2}. \qquad (2)$$

x_i를 Hc에 의해 정의된 i번째 검사식에 따른 1의 개수라고 하자. 그러면 0이 아닌 x_i는 짝수여야 되며, 최소한 2 이상이 된다. 따라서,

$$\|Hc\|^2 = \sum_{i=1}^{m}x_i^2 \geq 2\sum_{i=1}^{m}x_i = 2\sum_{i=1}^{p}d_i\gamma_i \geq 2\gamma_1 d \qquad (3)$$

고유 공간(eigenspace) 표현을 이용하면,

$$\|Hc\|^2 = \sum_{i=1}^{s}\mu_i\|c_i\|^2 \leq (\mu_1-\mu_2)\|c_1\|^2 + \mu_2\|c\|^2 \qquad (4)$$

(1), (2), (3)을 (4)식에 넣어 정리하면 정리1의 바운드가 유도된다. ■

정리2(검사 노드 기반 하한식). 연결된 그래프 구조를 갖는 검사 행렬 H가 $H=[H_1, H_2, \cdots, H_p]$이고, 실수 행렬 HH^T의 순서적으로 나열된 고유값들이 $\mu_1 > \mu_2, > \cdots > \mu_s$라고 하자. 여기서 각 H_i는 $m \times n$행렬이고, 고정된 열무게 γ_i, 고정된 행무게 ρ_i를 각각 가지며, $\gamma_1 < \gamma_2 < \cdots < \gamma_p$라고 가정하자. 그러면 검사 행렬 H를 갖는 부호는 다음의 최소 거리 바운드를 만족한다.

$$d \geq \frac{2m(2\gamma_1+\sum_{i=1}^{p}\rho_i-2-\mu_2)}{\gamma_p(\sum_{i=1}^{p}\rho_i\gamma_i-\mu_2)}$$

증명 활성 검사 노드(active parity node)의 위치에

1의 값을 그렇지 않으면 0의 값을 갖는 길이 m인 실수 벡터 $\boldsymbol{p}$를 정의하자. 그리고 $\boldsymbol{p}$를 행렬 HH^T의 i번째 고유 공간(eigenspace)에 투영한 벡터를 $\boldsymbol{p}_i$라 하자 행렬 HH^T의 첫 번째 고유벡터는 $\boldsymbol{e}_1=(1,1,..,1)^T/\sqrt{m}$이 되고, 이에 따른 고유값은 $\mu_1=\Sigma_{i=1}^{p}\gamma_i^2$이 되며 연결된 그래프이므로 이 값은 유일하다[5] 벡터 $\boldsymbol{p}$에서의 1의 개수를 η라 하면, $\boldsymbol{p}^T\boldsymbol{p}=\|\boldsymbol{p}\|^2=\eta$가 되며, $\|\boldsymbol{p}_1\|^2=\eta^2/m$이 된다. $H^T\boldsymbol{p}$는 H의 비트 노드들에 대한 무게 분포를 할당하는 벡터가 된다. y_i를 i번째 비트에 대한 무게라고 하면

$$\|H^T\boldsymbol{p}\|^2=\sum_{i=1}^{np}y_i^2 \qquad (5)$$

각각의 활성 검사 노드들은 짝수개의 0이 아닌 비트 노드들과 연결되어 있다 i번째 활성 검사 노드에 대한 $H^T\boldsymbol{p}$에서의 무게가 l인 연결 노드들의 개수를 $u_i(l)$이라고 하자 그러면 i번째 활성 검사 노드에서 계산한 제곱 무게는

$$\sum_{i=1}^{\gamma_p}(1/l)u_i(l)l^2\geq 2\gamma_1+\sum_{i=1}^{p}\rho_i-2 \qquad (6)$$

활성 검사 노드의 개수는 η개이므로,

$$\sum_{i=1}^{np}y_i^2\geq\eta(2\gamma_1+\sum_{i=1}^{p}\rho_i-2). \qquad (7)$$

고유 공간 표현을 이용하면,

$$\|H^T\boldsymbol{p}\|^2=\sum_{i=1}^{n}\mu_i\|\boldsymbol{p}_i\|^2\leq(\mu_1-\mu_2)\|\boldsymbol{p}_1\|^2+\mu_2\|\boldsymbol{p}\|^2$$

위의 식들을 서로 대입하면

$$\eta\geq m(2\gamma_1+\sum_{i=1}^{p}\rho_i-2-\mu_2)/(\mu_1-\mu_2),$$

그리고 $d\gamma_p\geq 2\eta$를 이용하면 정리2의 바운드가 유도된다 ■

계1 Tanner의 바운드는 정리 1, 2에서 $p=1$인 경우이거나 $\gamma_1=\gamma_2=\cdots=\gamma_p$, $\rho_1=\rho_2=\cdots=\rho_p$인 경우이다

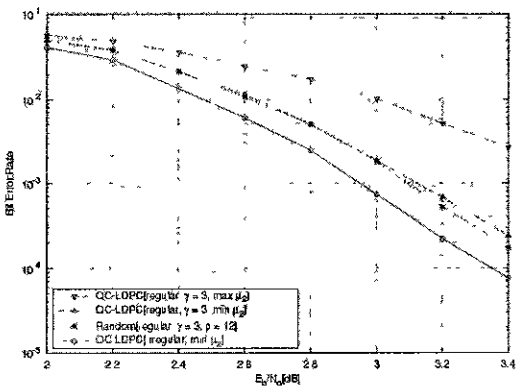
IV. 예제 및 모의 실험

일반화된 바운드의 유용성을 예시하기 위하여 그림1에 제시된 부호와 의사 순환 부호(quasi-cyclic code)로 이루어진 예제들의 바운드를 구하여 본다 의사 순환 부호는 검사 행렬 H가 $m\times m$순환 행렬들로(circulant matrix) 구성된 블록 행렬이다. 여기서 m을 순환 행렬의 차수라 하며, 각각의 순환 행렬은 행렬의 첫 행으로부터 그와 동등한 다항식으로 표현할 수 있다. 즉 순환 행렬 H의 i,j번째 원소가 H_{ij}일때, 다음의 수식으로 표현할 수 있다[6]

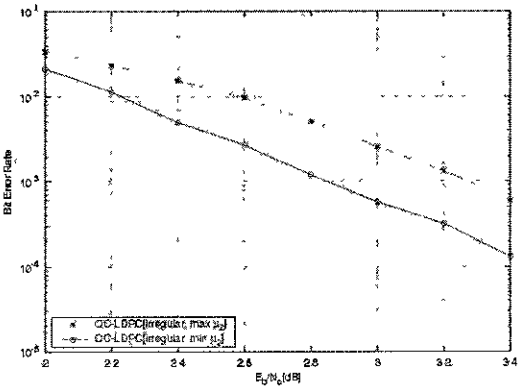
$$h(x)=\sum_{j=0}^{m-1}H_{0j}x^j$$

예제1 그림1에 제시한 부호는 부호율이 4/9인 [9,2,3]균일 LDPC부호로서, HH^T의 고유값으로 $\mu_1=6$, $\mu_2=3$을 갖는다 H^TH의 0이 아닌 고유값과 HH^T의 0이 아닌 고유값들은 서로 같다. 따라서 비트 노드 기반 하한식은 $d\geq 3$, 검사 노드 기반 하한식은 $d\geq 4$가 된다 전영역 탐색에 따른 검사 행렬H를 갖는 블록 부호의 최소 거리는 4로서 검사 노드 기반 바운드가 실제 최소 거리를 하한값으로 갖는 예제이다. 이 예제의 경우 두 번째로 큰 고유값들의 값이 모두 같아서 고유 공간 방법에 따른 근사화에 손실을 주지 않으므로 유도한 바운드가 실제 최소 거리에 매우 근접함을 알 수 있다

예제2. 검사 행렬 H가 3개의 순환행렬로 구성된 의사 순환 부호 $H=[H_1,H_2,H_3]$라 하자 각 순환 행렬 H_i는 차수가 25인 행렬이며, 동등한 다항식이 $h_1(x)=1+x^4+x^{14}$, $h_2(x)=1+x^5+x^{12}$, $h_3(x)=1+x+x^3+x^9$로 이루어져 있다 그러면 $\mu_1=34$, $\mu_2=9$가 된다 이 예제의 경우 $\mu_2>2\gamma_1$이 되므로 정리1의 하한식은 의미 없는 결과가 나온다 반면에 정리2는 $d\geq 2.5$가 된다. 탐색 결과 실제 최소 거리는 6이다



(a) 부호율 3/4, 길이 868인 LDPC 부호의 성능 실험 결과



(b) 부호율 2/3, 길이 501인 비균일 LDPC 부호의 모의 성능 실험 결과

그림2 의사 순환 LDPC 부호의 AWGN 채널에서의 BER 성능 모의 실험 결과 복호 방법은 합곱 알고리즘을 이용하였으며, 최대 반복 복호 회수는 80번임

예제3 검사 행렬 H가 3개의 순환행렬로 구성된 의사 순환 부호 $H=[H_1, H_2, H_3]$이고, 각 순환 행렬 H_i는 차수가 71이며, 행렬의 다항식 표현은 $h_1(x)=1+x^2+x^{21}+x^{39}+x^{49}$, $h_2(x)=1+x^6+x^{13}+x^{36}+x^{44}$, $h_3(x)=1+x+x^4+x^{46}+x^{55}+x^{60}$이라고 하자 이 경우 검사 노드 기반 하한식은 $d\geq 3$이 된다.

본 논문에서 유도한 바운드의 약점은 유도 과정에서 사용한 몇 가지 수식의 근사화 때문이다. 첫 번째는 최소 거리 부호어에 대한 각각의 검사 수식(parity-check equation)에서 이를 만족 시키는 0이 아닌 비트의 개수가 4개 또는 그 이상이면 (2)번 수식은 근접한 값으로 근사화 되지 못한다. 두 번째

표 1 최적화 된 LDPC 부호의 탐색 결과

Code description		Eigen-value ratio	Number of 6-cycles
Random	[868,3,12]Random LDPC	0 5926	1,792
Rate 3/4 regular QC-LDPC	$h_1(x)=x^{78}+x^{121}+x^{137}$ $h_2(x)=1+x^8+x^{107}$ $h_3(x)=1+x^{11}+x^{86}$ $h_4(x)=x^{29}+x^{64}+x^{198}$	0.9543 (max)	6,727
	$h_1(x)=1+x^{121}+x^{137}$ $h_2(x)=x^8+x^{79}+x^{85}$ $h_3(x)=1+x^{11}+x^{144}$ $h_4(x)=x^{29}+x^{165}+x^{207}$	0 5469 (min)	1,085
Rate 3/4 irregular QC-LDPC	$h_1(x)=x^{67}+x^{88}$ $h_2(x)=x^{18}+x^{78}+x^{121}$ $h_3(x)=1+x^{11}+x^{144}$ $h_4(x)=1+x^{29}+x^{64}+$ $x^{165}+x^{198}+x^{205}+x^{207}$	0 5764 (max)	28,220
	$h_1(x)=x+x^{149}$ $h_2(x)=1+x^{18}+x^{137}$ $h_3(x)=1+x^{144}+x^{190}$ $h_4(x)=1+x^{29}+x^{64}+$ $x^{165}+x^{198}+x^{205}+x^{207}$	0 3880 (min)	23,002
Rate 2/3 irregular QC-LDPC	$h_1(x)=1+x^{34}$ $h_2(x)=1+x^{10}+x^{36}$ $h_3(x)=1+x+x^3+x^9+$ $x^{54}+x^{76}$	0.9305 (max)	25,050
	$h_1(x)=1+x^{12}$ $h_2(x)=1+x^5+x^{14}$ $h_3(x)=1+x+x^4+x^{11}+$ $x^{17}+x^{19}$	0 3995 (min)	5,344

μ_2보다 작은 모든 고유값들을 μ_2로 근사화 한 점이다 세 번째로 비균일 LDPC의 열무게 분포에서 최소 무게와 최대 무게의 비가 커지면 유도한 바운드는 근접한 값을 갖지 못한다. 이는 일반적으로 비균일 그래프에 있어서 바운드 유도시 갖는 단점이다.

다양한 예제 부호들을 생성하여 확인한 결과 정리1의 비트 노드 기반 하한식은 블록 행렬의 개수 p가 증가함에 따라 $\mu_2>2\gamma_1$가 되는 경향이 있어 하한식이 무의미해진다는 것을 알 수 있었다. 이러한 문제점은 Tanner의 균일 LDPC에서 얻어진 바운드나 블록 구조를 갖는 비균일 LDPC에서 얻어진 바운드 모두에 해당한다 하지만 정리 2의 검사 노드 기반 하한식은 열무게 γ_i의 값들이 커지면서 의미 있는 값들이 나온다는 것을 확인할 수 있었다.

본 논문에서 유도한 하한식이 경우에 따라 실제 최소 거리에 아주 근접하지 못한 약점은 있지만, 균일 LDPC 부호의 경우 Tanner에 의해 최소 거리와 고유값들의 관계를 통한 발견적 규칙(heuristic rule) 제안된 것처럼, 블록 구조를 갖는 비균일 LDPC 부

호에 대해서도 고유값들의 비인 μ_2/μ_1값이 작을수록 거리 특성이 좋아진다는 규칙을 세울 수 있다.

표1은 발견적 규칙을 적용하여 μ_2/μ_1이 최소인 부호와 최대인 부호를 탐색을 통해 찾은 것이다 부호율 3/4인 경우에는 (217,7,1)순환 차집합들(cyclic difference family)로부터 부호를 구성하였으며[7], 부호율 2/3인 경우에는 전영역 탐색을 통하여 예제 부호를 찾았다 그림2는 표1에 제시된 부호에 대한 모의 실험한 결과이다 실험 결과 균일 LDPC 부호인 경우 고유값들의 비 μ_2/μ_1이 최적인 부호가 최악인 부호에 비해 비트오류율(BER) 10^{-3}에서 약 0.4dB 이득이 있었으며, 블록 구조르 갖는 비균일 부호인 경우에도 비슷한 이득이 있음을 알 수 있다 또한 고유값 비 μ_2/μ_1가 작을수록 작은 싸이클이 줄어듦을 확인할 수 있었다. 이는 μ_2/μ_1가 작아짐으로써 그래프 상에서 비트 노드와 검사 노드간 확산효과가 더 커지기 때문이다.[8]

V 결 론

본 논문에서는 Tanner의 결과를 일반화하여, 균일 및 블록 구조를 갖는 비균일 LDPC부호에 적용 가능한 두개의 최소 거리 하한식을 유도하였다. 첫 번째는 비트노드와 최소 거리 부호어간의 관계를 통하여 유도되는 비트노드 기반 하한식이고, 두 번째는 검사노드와 최소 거리 부호어간의 관계에서 얻어지는 검사노드 기반 하한식이다 본 논문에서 유도한 하한식을 통하여 비균일 LDPC부호의 거리 특성을 그래프의 고유값들과의 관계로 나타낼 수 있었다. 모의 실험 결과 본 논문에서 유도한 발견적 규칙은 블록 구조를 갖는 비균일 LDPC 부호를 생성함에 있어 디자인 척도로 쓰일 수 있음을 확인하였다.

참 고 문 헌

[1] E D J C MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans Inform. Theory*, vol 45, no. 2, pp. 533-547, Mar 1999.

[2] R M Tanner, "Minimum distance bounds by graph analysis," *IEEE Trans. Inform. Theory*, vol 47, no. 2, pp 808-821, Feb 2001.

[3] M Luby, M. Mitzenmacher, A Shokrollahi, and D Spielman, "Improved Low-Density Parity-Check Codes using Irregular Graphs and Belief Propagation," Proc. 1998 *IEEE Int Symp Inform. Theory*, Cambridge, MA, p 117, Aug. 1998

[4] T. J. Richardson, M A Shokrollahi, and R L. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp 619-637, Feb. 2001.

[5] F R Gantmacher, *The Theory of Matrices*, Chelsea, 1959

[6] Henk van Tilborg, "On Quasi-Cyclic Codes with Rate 1/m," *IEEE Trans. Inform. Theory*, vol 24, no. 5, pp. 628-630, Sept 1978.

[7] C J Colbourn and J. H Dinitz *The CRC handbook of combinatorial designs*, CRC Press, Inc , 1996

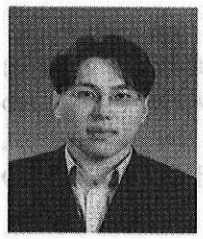
[8] M. Sipser and D Spielman, "Expander Codes," *IEEE Trans Inform. Theory*, vol. 42, no 6, pp 1710-1722, Nov 1996

신 민 호 (Min-Ho Shin) 정회원

1996년 2월 : 연세대학교 전자공학과 졸업
2000년 2월 : 연세대학교 전기전자공학과 석사
2000년 3월~현재 : 연세대학교 전기전자공학과 박사과정

<관심분야> Error Correcting Codes, PN Sequences, LDPC Codes

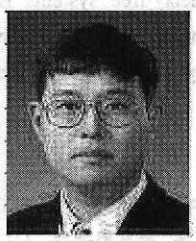
김 준 성 (Joon-Sung Kim) 준회원



2001년 2월 : 연세대학교 전파공학과 졸업
2003년 2월 : 연세대학교 전기전자공학과 석사
2003년 3월~현재 : 연세대학교 전기전자공학과 박사과정

<관심분야> Error Correcting Codes, PN Sequences, LDPC Codes

송 홍 엽 (Hong-Yeop Song) 종신회원



1984년 2월 : 연세대학교 전자공학과 졸업
1986년 5월 : USC 대학원 전자공학과 석사
1991년 12월 : USC 대학원 전자공학과 박사
1992년~1993년 : Post Doc., USC 전자공학과
1994년~1995년 : Qualcomm Inc., 선임연구원
1995년 9월~현재 : 연세대학교 전기전자공학과 교수

<관심분야> PN. sequences, Error Correcting Codes, Spread Spectrum Communication Systems, Stream Cipher Systems