

효율적 부호를 고려한 Dual-Diagonal Quasi-cyclic LDPC(Low Density Parity Check) 복호기의 구현

변용기, 김종태
성균관대학교 정보통신공학부

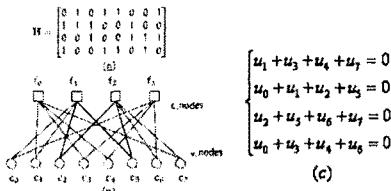
Implementation of Dual-Diagonal Quasi-cyclic LDPC(Low Density Parity Check) decoder for Efficient Encoder

Yong Ki Byun and Jong Tae Kim
School of Information and Communication Eng.. Sungkyunkwan Univ.

Abstract - 1962년 Gallager에 의해 처음 제안된 LDPC 부호는 복호를 수행하는 부호방식으로 패리티 행렬(H)의 대부분이 0으로 구성되어 복호시에 적은 연산량을 요구하며, shannon의 한계에 도달하는 복호 능력으로, 차세대 통신의 주된 부호 방식으로 고려되고 있다. 하지만, LDPC는 부호화에 있어서 여타 다른 부호방식에 비해 복잡한 특성을 가지고 있으므로, 이를 개선하기 위한 부호방식의 적용이 필요하다. 본 논문에서는 효율적인 부호화를 위하여 Dual-diagonal H 행렬을 구성하고, 쉽게 부호 길이를 확장 할 수 있는 Quasi-Cyclic 방식을 적용한 복호기를 구현하였다.

1. 서 론

$l \times k$ 길이의 정보(s)로부터 부호화된 부호코드 u 는 $l \times n$ 차원의 행렬이 된다. LDPC 부호는 $m \times n$ 차원의 패리티 행렬 H 가 있을 때, 두 행렬 연산이 $u \cdot H' = 0$ 이 되는 특성을 가진다. 이를 <그림 1>의 H 행렬(a)에 적용하면 <그림 1>의 (c)와 같은 식을 만들어 낸다.



<그림 1> H 행렬(a)과 Tanner 그래프(b) 및 패리티 식(c)

위 식을 모두 만족하는 u 값을 찾는다면 신호의 복호화가 끝나게 된다. $u = s \cdot G$ 로 만든다면, $s \cdot G \cdot H'$ 는 0 행렬이 될 것이다. 임의의 s 에 대하여, $G \cdot H'$ 역시 0 행렬이 되어야 한다. 부호를 조직적으로 구성하기 위하여, 코드워드 u 중 정보 비트를 앞 쪽에 배치하면, 생성행렬 G 는 식(1)과 같이 구성된다.

$$G = [I_{n-k} | P_{k \times n-k}] \quad (1)$$

H 행렬을 다시 $H = [H_1 | H_2]$ 와 같이 표현하면, 식(1)에 의해

$$I \cdot H_1 + P \cdot H_2 = 0 \Rightarrow P = H_2^{-1} \quad (2)$$

와 같이 되며, 최종 코드 u 는 식(3)과 같이 표현된다.

$$u = s \cdot G = [s | sP] = [s | sH_1' H_2^{-1}] \quad (3)$$

LDPC 부호의 몇 가지 제한 사항을 들면, 식(3)에서 부호화를 위해선 s 와 H_1' 및 H_2^{-1} 의 매우 복잡한 행렬 곱 연산이 필요하다는 것이다. 또한, LDPC의 일반적 특성은 부호길이(n)이 길수록, I 의 개수 및 위치가 매우 랜덤하여 짧은 주기(short cycle)를 만들지 않을 수록 좋은 성능을 가지는 것인데, 랜덤한 특성을 가지는 H 행렬은 크기가 커질 수록 구현에 있어서 복잡성이 커지는 문제가 있다.

본론 및 결론에서는 H 행렬의 구조를 통하여 이러한 문제들을 해결 하여 개선된 LDPC 구조를 소개하고, 상위수준에서 설계한 LDPC 복호기를 통하여, 성능을 확인 한다.

2. 본 론

2.1 개선된 H 행렬 구조를 갖는 LDPC 부호

서론에서와 같이 수식 (3)에 의해 부호어를 얻기 위해 가우시안 소거법으로 H 행렬을 변환 한다면, 1이 적은 H 행렬의 특성을 잃게 되므로, 복호시 연산을 복잡하게 만드는 결과를 가져온다. 그러므로 초기 H 행렬 생성시부터 이를 고려한 형태로 H_2 행렬을 구성 할 필요가 있다. 또한 차세대 이동통신에서는 채널 상태에 따라 다양한 부호율 및 부호 길이를 지원 할 필요가 있다. 본론에서는 이를 고려한 구조인 Quasi-Cyclic 구조 및 dual-diagonal 구조를 소개하고, 복호기를 구현하여, AWGN 채널 상에서 시뮬레이션 결과를 보인다.

2.1.1 Quasi-Cyclic LDPC 구조

서론에서와 같이 긴 부호 길이를 갖는 랜덤한 LDPC 행렬은 구현이 복잡하며, 부호 길이가 수백, 수천 비트 이상으로 길어지면, 실질적인 구현은 힘들다. Marc P. C.는 확장 인수를 도입, 순환 행렬로 H 를 구성하여, 규칙성을 가지면서, 부호 길이를 조절 할 수 있는 Quasi-Cyclic(QC) LDPC 구조를 제안하였다. QC-LDPC는 확장 인수 L 값을 가지며, H 행렬 내부의 원소가 $L \times L$ 차원의 크기를 갖는 단위행렬 I 를 오른쪽으로 임의 수 만큼 순환 시킨 행렬로 이루어진다. 임의의 순환값을 결정하는 것은 QC-LDPC에서 매우 중요한 요소이다. 단위행렬의 순환으로 이루어진 내부 행렬의 특성상 무수히 많은 경로(short cycle)를 유발 할 수 있기 때문이다. Tanner[6]는 이를 고려하여 <그림 2>와 같은 방식으로 순환값을 결정하였다. L 값을 소수로 선택하고, $L-1$ 의 약수 중 $GF(L)$ 상의 원시원소 a, b 를 선택하여 a 와 b 사이의 곱 및 승 연산으로 순환 값은 결정하였다. <그림 2>에서 P 는 I 행렬의 순환값을 나타내며, H 행렬은 이러한 방식으로 만들어진 H 행렬의 예를 보여준다.

$$P = \begin{bmatrix} 1 & a & a^2 & \cdots & a^{L-1} \\ b & ab & a^2b & \cdots & a^{L-1}b \\ b^2 & ab^{L-1} & a^2b^{L-1} & \cdots & a^{L-1}b^{L-1} \end{bmatrix} \quad H = \begin{bmatrix} I^1 I^2 I^4 I^8 I^{16} \\ I^3 I^{10} I^{20} I^9 I^6 \\ I^{25} I^{19} I^7 I^{14} I^{20} \end{bmatrix}$$

<그림 2> 순환 행렬 P 와 $a=2, b=5, L=31$ 에서의 예.

$m \times n$ 크기의 H 행렬은 L 확장 인수를 적용하여, 실제 $(m \times L) \times (n \times L)$ 의 크기를 갖는 행렬이 된다. 즉 L 값을 변화 시키면 설계구조에 커다란 변화 없이 부호 길이를 변화 시킬 수 있는 구조이다. 랜덤한 H 행렬이 좋은 성능을 갖는 것은 사실이지만, 수천에서 수만 비트의 중간 정도 길이 부호에 있어서는 QC-LDPC 역시 매우 좋은 성능을 가지므로, 중간길이(수천에서 수만 비트)의 부호에서는 매우 효율적인 구조이다.

2.1.2 Dual-Diagonal LDPC 구조

패리티 검사 행렬에서 패리티에 해당하는 부분이 dual-diagonal의 형태가 되면 간단한 부호화 기법을 통하여 AND와 XOR 연산만으로 부호화를 할 수 있다. 패리티 검사 행렬을 정보비트에 해당하는 행렬 H_1 과 패리티 비트에 해당하는 행렬 H_2 로 나누어 보면 $H = [H_1 | H_2]$ 와 같다. H_2 는 I 이 적은 $(n-k) \times k$ 행렬로 구성되고, H_2 는 <그림 3>과 같은 DUAL-DIAGONAL 형태의 $(n-k) \times (n-k)$ 행렬로 이루어진다.

$$H_2 = \begin{bmatrix} 1 & & & & \\ 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{bmatrix} \quad H_2^{-1} = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & 1 \\ & \ddots & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{bmatrix}$$

<그림 3> Dual-Diagonal H_2 행렬 및 H_2^{-1} 행렬

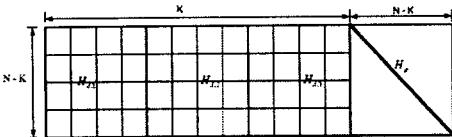
위와 같은 경우 첫 번째 패리티 비트는 정보 비트에 의해 결정되고, 두 번째 패리티 비트는 첫 번째 패리티 비트에 의해 결정되며, 그 이후 패리티 비트는 앞단의 패리티 비트에 의해 결정되는 구조를 갖는다. 즉, 이 방법은 복잡한 행렬연산을 AND와 XOR 회로로 구성 할 수 있게 만든다. 식(1)과 (3)에 의해 생성행렬은 $G = [I | H_1 | H_2^{-1}]$ 와 같다. 이것은 변환 함수가 $1/1 \oplus D$ 인 차동 부호화기에 대응되는 변환 행렬과 같고, 입력 w_1, \dots, w_n 에 대하여, 출력은 다음과 같다.

$$\begin{aligned} c_1 &= w_1 \\ c_2 &= w_1 + w_2 \\ &\vdots \\ c_r &= w_1 + \dots + w_r \end{aligned}$$

<그림 4> H_2^{-1} 행렬에 대한 입출력

H_1 행렬 역시 1이 적은 행렬이므로 두 행렬의 곱은 비교적 간단히 계산될 수 있다. dual-diagonal 구조는 효율적인 부호화를 가능하게 하지만, 페리티 H 행렬의 무게는 낮은 열에 의해 결정되기 때문에 성능에 있어 열화가 생긴다. 하지만 부호율 1/2 이상의 부호에서는 대부분의 큰 성능 열화 없이 사용 가능하기 때문에 최근 LDPC 부호에서는 많이 채택되고 있는 구조이다.

dual-diagonal 방식은 부호율까지도 복호기의 구조에 큰 변화 없이 구현할 수 있는 장점을 있다. 페리티 행렬의 H_2 부분이 dual-diagonal 성질을 유지해야 하므로, 부호율 조정은 <그림 5>와 같이 쇼트닝[2] 방식으로 할 수 있다.



<그림 5> duo-diagonal 가변 부호율 구조[2]

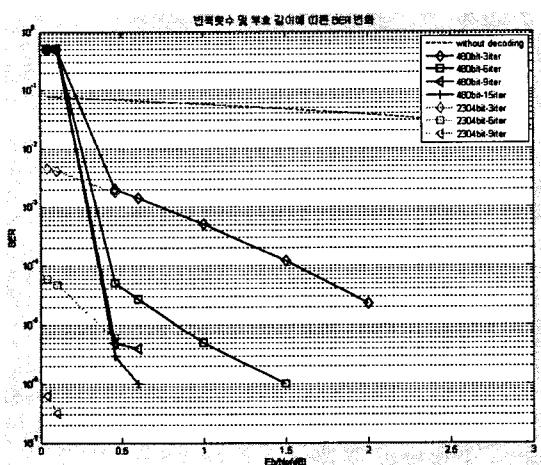
<그림 5>와 같은 구조는 최초 부호율 3/4인 QC-LDPC를 나타내며, H 행렬의 H_{dL} 을 제거함으로 해서 부호율 2/3인 QC-LDPC를 구현할 수 있으며, H_{dL} , H_{dR} 를 제거하면 부호율 1/2인 QC-LDPC를 구현할 수 있다.

2.1.3 QC-LDPC와 Dual-diagonal LDPC 구조의 동시 적용

앞절에서는 QC-LDPC의 구조와 Dual-diagonal 구조를 설명하고, 이를 통해서 규칙성을 가진 구조에서 쉽게 긴 길이의 부호를 효율적으로 구현할 수 있음을 보였다. 두 가지 LDPC의 구조를 동시에 적용한다면, 두 구조의 장점을 동시에 취하는 구조를 얻을 수 있다. 즉, dual-diagonal 구조의 행렬 원소를 각각 $L \times L$ 의 차원을 갖는 순환 행렬로 구성한다면, 원하는 길이의 효율적인 LDPC 부호 구조를 얻을 수 있다.

2.2 실험 결과

본 논문에서는 Richardson 구조를 기본으로 삼성전자가 WiBro 표준에 제안한 Optional B-LDPC 구조[4]를 기본으로 복호기를 상위수준에서 복호기를 구현하고 실험을 실시하였다. 삼성의 Optional B-LDPC 구조는 변형된 Dual-Diagonal 형태의 H 행렬 구조를 가진다. 설계된 복호기의 H 행렬은 부호율이 1/2이 되도록 페리티 행렬을 설계 하였으며, 복호시 사용된 각 노드 계산은 LLR(log likelihood ratio)을 적용한 Belief Propagation 방식으로 수행하였다. 각 노드에 정보 전달시 실제 하드웨어 구현 시에는 4비트에서 5비트 정보 단위로 구현되며, 본 실험에서는 floating point 값을 적용하였다. 이는 실제 구현과 차이가 있을 수 있으며, 실제 구현시 차이는 반복횟수를 늘려줌으로써 보상 할 수 있다. 실험 진행은 L 값을 조정하여 서로 다른 부호 길이에 대하여 반복된 복호결과의 BER을 측정 하였으며, 각 실험에 대한 결과를 <그림 6>에 나타내었다. 실험에 사용된 H 행렬의 순환값은 모든 L 값에 대해서 동일한 값이 사용되었다. 이는 QC-LDPC의 특성에 따라 L 값의 변화만으로 부호 길이를 조절 할 수 있기 때문이다.



<그림 6> 반복횟수 및 부호길이에 따른 BER 변화

<그림 6>에서 볼 수 있듯이 L 값을 20에서 96으로 늘려 부호 길이가 480에서 2304 비트로 늘어남에 따라 BER 성능이 좋아지는 것을 확인할 수 있다. <그림 7>은 E_b/N_0 가 0.5dB인 AWGN 채널하에서, 부호율 1/2, 부호길이 480비트 LDPC를 통하여 복호하였을 때 결과를 예 나타내었다.

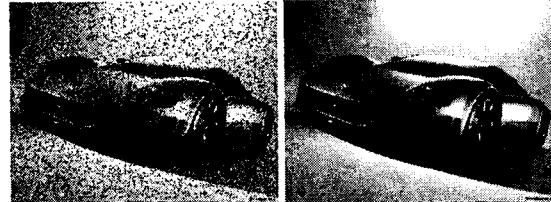
3. 결론

LDPC 부호는 Shannon의 한계에 이르는 성능으로 차세대 통신의 가장 주

목 받는 부호 방식 중의 하나이다. 부호화가 복잡하다는 단점이 있었지만, 계속적인 연구로 많은 제약들이 개선되었다.

본 논문에서는 기존 LDPC 부호의 H 행렬을 개선하여 가변적인 부호 길이 특성을 가진 QC-LDPC 부호를 소개하였다. 부호와 복호 연산을 효율적으로 수행하기 위하여, QC-LDPC에 Dual-Diagonal 구조를 적용하였으며, 이는 가변 부호율 특성까지 가지게 된다. 본 논문에서는 소개된 구조의 LDPC 부호를 구현하고 그 우수성을 확인하였다.

근래의 많은 LDPC 부호 연구는 기존의 LDPC의 제한사항을 개선 할 수 있는 결과를 내었으며, 그 중 Dual-Diagonal Quasi-cyclic LDPC 구조는 무선 통신 시스템에서 LDPC 응용의 가능성을 더욱 높여 주고 있다.



<그림 8> LDPC 복호기의 성능 예

감사의 글

본 논문은 정보통신부의 출연금으로 수행한 IT SoC 핵심 설계 인력양성 사업의 수행결과입니다.

참고 문헌

- [1] M. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," IEEE Trans. Inf. Theory, vol.50, no.8, pp.1788 - 1793, 2004.[CrossRef][ISI].
- [2] Min-seok Oh, Kyuhyun Chung, "Scalable LDPC coding scheme for OFDMA," IEEE C802.16e-04/242, 2004,08
- [3] Richardson, T.J., Urbanke, R.L., "Efficient encoding of low-density parity-check codes," Information Theory, IEEE Transactions on Volume 47, Issue 2, Feb 2001 Page(s):638 - 656
- [4] Panyuh Joo, et. al., "Optional B-LDPC coding for OFDMA PHY," IEEE C802.16e-04/78, 2004, 05
- [5] R. G. Gallager, "Low density parity check codes," IRE Trans. Inform. Theory, vol. IT-8, pp. 21 - 28, Jan. 1962.
- [6] Tanner, R.M, et. al., "LDPC block and convolutional codes based on circulant matrices," Information Theory, IEEE Transactions on Volume 50, Issue 12, Dec. 2004 Page(s):2966 - 2984
- [7] Bernhard M.J. Leiner, "LDPC Codes -- a brief Tutorial," bleiner@gmail.com, April 8, 2005
- [8] 이문호, 박주용, "4세대 이동통신을 위한 LDPC 원리 및 응용", 텔레콤, 제 17권. 2호, 2001
- [9] Yanni Chen, "Overlapped Message Passing for Quasi-Cyclic Low-Density Parity Check Codes," Circuits and Systems I: Regular Papers, IEEE Transactions on Volume 51, Issue 6, June 2004 Page(s):1106 - 1113 Digital Object Identifier 10.1109/TCSI.2004.826194
- [10] Hao Zhong and Tong Zhang, "Design of VLSI Implementation-Oriented LDPC Codes," Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th Volume 1, 6-9 Oct. 2003 Page(s):670 - 673 Vol.1
- [11] Jian Sun, "An Introduction to Low Density Parity Check (LDPC) Codes," WCRL Seminar Series, 2003, 6
- [12] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," IEEE Trans. Infor. Theory, vol. 45, pp. 399-431, Mar. 1999.