

준순환 저밀도 패리티 체크 부호를 위한 새로운 이중 대각 구조에 대한 연구

*박호성°, *홍석범, *노종선, **신동준

*서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소

**한양대학교 전자통신컴퓨터공학부

New Dual-Diagonal Structure for Quasi-Cyclic Low-Density Parity-Check Codes

*Hosung Park°, *Seokbeom Hong, *Jong-Seon No, and **Dong-Joon Shin

*Department of Electrical Engineering and Computer Science, INMC, Seoul National University

**Department of Electronic Engineering, Hanyang University

lovepk98@snu.ac.kr, fousbyus@ccl.snu.ac.kr, jsno@snu.ac.kr, djshin@hanyang.ac.kr

요 약

본 논문에서는 낮은 오류 마루 (error floor)를 보이면서 동시에 효율적인 부호화를 가능하게 하는 불규칙 준순환 (quasi-cyclic, QC) 저밀도 패리티 체크 (low-density parity-check, LDPC) 부호를 설계하기 위해 패리티 체크 행렬의 패리티 부분으로 사용할 수 있는 새로운 블록 이중 대각 (block dual-diagonal, BDD) 구조를 제안한다. 제안하는 BDD 구조는 QC LDPC 부호가 큰 최소 해밍 거리 (minimum Hamming distance)를 가질 수 있게 하고, 특히 이러한 장점은 낮은 부호율을 가지는 QC LDPC 부호의 경우에 극대화된다. 모의 실험을 통해 제안하는 BDD 구조를 채택한 QC LDPC 부호가 기존의 BDD 구조를 채택한 QC LDPC 부호보다 낮은 오류율 영역에서 더 좋은 성능을 나타내는 것을 보인다.

1. 서론

불규칙 (irregular) 저밀도 패리티 체크 (low-density parity-check, LDPC) 부호는 일반적으로 폭포 영역 (waterfall region)에서 규칙 (regular) LDPC 부호보다 좋은 성능을 보이지만 오류 마루 (error floor) 영역에서는 좋지 않은 성능을 나타내는 경향이 있다 [1]. 이러한 오류 마루 현상은 작은 최소 해밍 거리 (minimum Hamming distance) 또는 트래핑 집합 (trapping set) [1]과 같은 부호 내부의 구조에 의해 발생하는 것으로 알려져 있다. 일반적으로 성능이 좋은 것으로 알려진 불규칙 LDPC 부호에는 다수의 차수 (degree) 2 인 변수 노드 (variable node)가 포함되어 있는데 [2]-[4] 이런 경우 최소 해밍 거리가 작게 될 가능성이 많고 성능 열화에 크게 기여하는 트래핑 집합이 나타날 가능성 또한 많다 [5], [6]. 최근에 사용되는 불규칙 준순환 (quasi-cyclic, QC) LDPC 부호들은 대부분 패리티 체크 행렬의 패리티 부분에 블록 이중 대각 (block dual-diagonal, BDD) 구조를 가지고 있다 [3], [4]. 이러한 BDD 구조는 대부분 차수 2 인 변수 노드들로 구성되어 있기 때문에 해당 LDPC 부호의 차수 분포 (degree distribution)를

선택하는데 있어서 제약이 생기게 된다. 특히 이러한 BDD 구조를 가지는 낮은 부호율의 QC LDPC의 경우에는 불가피하게 차수가 2 인 변수 노드들을 매우 많이 가지게 된다. 따라서 기존의 BDD 구조는 최소 해밍 거리를 작게 하거나 성능 열화에 크게 기여하는 트래핑 집합들을 유발시키게 된다. 본 논문에서는 오류 마루 영역에서 좋은 성능을 나타내는 불규칙 준순환 LDPC 부호를 설계하기 위해 새로운 BDD 구조를 제안한다. 제안하는 BDD 구조는 복수 가중치 (multi-weight)를 가지는 순환 행렬 (circulant)을 도입함으로써 패리티 체크 행렬의 패리티 부분이 자유로운 차수 분포를 가질 수 있게 하는 한편 효율적인 부호화 [7] 또한 가능하게 한다. 따라서 차수 2 인 변수 노드의 수를 적절히 조절하면 해당 QC LDPC 부호는 큰 최소 해밍 거리를 가질 수 있게 되고 이에 따라 오류 마루 영역에서 좋은 성능을 나타내게 된다. 모의 실험을 통해 제안하는 BDD 구조를 가지도록 설계된 QC LDPC 부호가 기존의 BDD 구조를 가지는 QC LDPC 부호보다 오류 마루 영역에서 더 좋은 성능을 나타내는 것을 보인다.

2. 새로운 블록 이중 대각 구조의 제안

이진 QC LDPC 부호를 \mathcal{C} 로 표기하고 그 패리티 체크 행렬을 \mathbf{H} 라고 하자. 그리고 \mathbf{H} 는 $z \times z$ 크기의 순환 행렬들이 행 방향으로 J 개, 열 방향으로 L 개씩 쌓여 있다고 가정하자. $M = Jz$, $N = Lz$ 라고 하면 \mathbf{H} 는 $M \times N$ 크기의 행렬이 되고 \mathcal{C} 의 부호율은 $R = 1 - M/N = 1 - J/L$ 가 된다.

QC LDPC 부호의 \mathbf{H} 는 [8]에서와 같이 이진 다항식들의 행렬로 표현될 수 있다. 이에 따라 다항식 패리티 체크 행렬 $\mathbf{H}(x)$ 를 다음과 같이 정의한다.

$$\mathbf{H}(x) = \begin{bmatrix} h_{0,0}(x) & h_{0,1}(x) & \cdots & h_{0,L-1}(x) \\ h_{1,0}(x) & h_{1,1}(x) & \cdots & h_{1,L-1}(x) \\ \vdots & \vdots & \ddots & \vdots \\ h_{J-1,0}(x) & h_{J-1,1}(x) & \cdots & h_{J-1,L-1}(x) \end{bmatrix}$$

여기서 $h_{j,l}(x)$ 는 해당 순환 행렬의 이동 값 (shift value)에 해당하는 차수의 항들을 갖는 이진 다항식이다. 이러한 표현 방식에 따라 순환 치환 행렬 (circulant permutation matrix)은 단항식으로, 복수 가중치를 가지는 순환 행렬은 2 개 이상의 항을 가지는 다항식으로, 영행렬 (zero matrix)은 0 으로 각각 표현된다.

편의상 모든 행렬과 벡터들은 다음과 같이 메시지 부분과 패리티 부분으로 나누어서 표현하기로 하자.

$$\mathbf{H} = [\mathbf{H}_m | \mathbf{H}_p], \quad \mathbf{H}(x) = [\mathbf{H}_m(x) | \mathbf{H}_p(x)], \quad \mathbf{c} = [\mathbf{m} | \mathbf{p}]$$

본 논문에서 새롭게 제안하는 BDD 구조를 다항식 패리티 체크 행렬로 표현하면 본 페이지 아래와 같이 정의된다. 이차 다항식은 행렬의 대각선 상의 원소에서만 나타날 수 있다. $\mathbf{H}_p(x)$ 에서 이차 다항식의 개수를 n_2 라고 하자. n_2 는 고정된 값이 아니므로 원하는 차수 분포에 따라 결정하면 된다. 그리고 이차 다항식에서 하나의 항의 차수 (혹은 이동값)는 항상 0 으로 한다. 이차 다항식의 나머지 이동값들을 왼쪽 위부터 차례로 s_1, s_2, \dots, s_{n_2} 라고 하고 이것들을 원소로 가지는 중복 집합 (multiset)을 S 라고 하자. 설계하고자 하는 QC LDPC 부호의 인자들 (parameter)이 주어졌을 때 S 를 결정하는 과정은 3장에서 다루게 된다. 또한 S 의 각각의 원소가 어떠한 순서로 어느 위치에 배치되는지는 4장에서 언급하기로 한다.

3. 효율적인 부호화

본 장에서는 n_2, J, z 가 정해졌을 때 효율적인 부호화 [7]를 위해 S 를 어떻게 결정하면 되는지를 다룬다.

$$\mathbf{H}_p(x) = \begin{bmatrix} x^0 + x^{s_1} & x^0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & x^0 + x^{s_2} & x^0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & x^0 & x^0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & x^0 + x^{s_3} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & x^0 & x^0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & x^0 + x^{s_{n_2}} & x^0 \\ x^0 & 0 & 0 & 0 & \cdots & 0 & 0 & x^0 \end{bmatrix}$$

여기서는 $n_2 = J$ 인 경우만을 다루기로 하자. 그 외의 경우는 거의 동일한 방법으로 생각할 수 있다. [7]에서와 마찬가지로 다항식 패리티 체크 행렬을 다음과 같이 분할하여 생각할 수 있다.

$$\mathbf{H}(x) = \begin{bmatrix} \mathbf{A}(x) & \mathbf{B}(x) & \mathbf{T}(x) \\ \mathbf{C}(x) & \mathbf{D}(x) & \mathbf{E}(x) \end{bmatrix}$$

제안하는 BDD 구조의 정의에 따라 $\mathbf{B}(x) = [1 + x^{s_1} \ 0 \ \cdots \ 0]^T$, $\mathbf{D}(x) = [1]$, $\mathbf{E}(x) = [0 \ \cdots \ 0 \ 1 + x^{s_J}]$,

$$\mathbf{T}(x) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 + x^{s_2} & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 + x^{s_3} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 + x^{s_{J-1}} & 1 \end{bmatrix}$$

가 된다. 이로부터 $\mathbf{T}^{-1}(x)$ 를 어렵지 않게 구할 수 있으며 $\phi(x)$ 는 다음과 같다.

$$\phi(x) = \mathbf{E}(x)\mathbf{T}^{-1}(x)\mathbf{B}(x) + \mathbf{D}(x)$$

$$= (1 + x^{s_1})(1 + x^{s_2}) \cdots (1 + x^{s_J}) + 1$$

따라서 ϕ 는 $\phi(x)$ 에 있는 항의 수에 해당하는 가중치를 가지는 $z \times z$ 순환 행렬이 된다.

효율적인 부호화를 위해서는 ϕ^{-1} 가 존재해야 한다. 이를 위해 $\phi(x) = x^k, 0 \leq k \leq z-1$ 이 되게 만들 수 있다면 매우 간단하고 효율적인 방법일 것이다. 여기서 주의해야 할 점은 z 가 짝수일 경우 가중치가 2인 각 순환 행렬의 내부에서 거스 (girth) 4를 피하기 위해서는 s_i 는 $z/2$ 가 되어서는 안 된다는 것이다. 다음 정리들을 통해 $\phi(x) = x^k$ 가 되도록 하는 S 를 찾을 수 있다.

정리 1. $k < J$ 를 만족하는 모든 정수 k 에 대하여 $z \neq 2^k$ 라고 가정하자. 그러면 $S = \{2^0 \bmod z, 2^1 \bmod z, 2^2 \bmod z, \dots, 2^{J-2} \bmod z\}$ 로 놓으면 $\phi(x) = x^{2^{J-1} \bmod z}$ 를 얻을 수 있고 가중치가 2인 순환 행렬 각각에서 길이 4인 사이클 (cycle)은 발생하지 않는다.

정리 2. $\log_2 J + 1 \leq l \leq J - 1$ 을 만족하는 임의의 정수 l 에 대하여 $z = 2^l$ 으로 가정하자. 그러면 $\phi(x) = x^{2^{l-1}}$ 이 되게 하는 s_i 들이 존재하고 가중치가 2인 순환 행렬 각각에서 길이 4인 사이클은 발생하지 않는다.

정리 2에서의 가정 아래 중복 집합 $S' = \{2^0 \bmod z, 2^1 \bmod z, 2^2 \bmod z, \dots, 2^{l-2} \bmod z\}$ 에서 각각의 원소들을 분할하는 방법을 통해 우리가 원하는 S 를 구할 수 있음을 명시한다.

4. 모의 실험

제안한 BDD 구조의 실효성을 검증하기 위해 기존 BDD 구조와 제안한 BDD 구조를 가지는 QC LDPC 부호를 각각 발생시켜서 성능을 비교할 것이다. 이를 위해서는 3 장에서의 방법으로 S 를 정해야 할 뿐만 아니라 s_i 들을 어느 곳에 어떤 순서로 배치할 것인지도 정해야 한다. 또한 메시지 부분도 어떻게 설계하는가 또한 오류 마루 영역의 성능에 큰 영향을 미친다. [9], [10]에서는 각각 기존의 BDD 구조와 제안한 BDD 구조를 가지는 좋은 QC LDPC 부호들을 설계하기 위한 알고리즘이 제시되었다. 특히 [10]에서는 패리티 부분의 거스가 최대가 되도록 s_i 를 배치함으로써 성능 열화를 초래하는 트래핑 집합을 최대한 억제하여 오류 마루 영역에서 좋은 성능을 얻도록 하였다. 본 장에서도 역시 위의 알고리즘들을 이용하여 $J = 30$, $L = 45$, $z = 45$, $N = 2025$, $R = 1/3$ 인 4 종류의 QC LDPC 부호를 발생시킨다. ‘Prop1’는 제안하는 BDD 구조를 가지고 알고리즘을 통해 발생시킨 QC LDPC 부호이고, ‘Conv1’은 기존의 BDD 구조를 가지고 알고리즘을 통해 발생시킨 부호이다. ‘Prop2’는 제안하는 BDD 구조를 가지고 무작위적인 방법으로 발생시킨 부호이고, ‘Conv2’는 기존의 BDD 구조를 가지고 무작위적인 방법으로 발생시킨 부호이다. AWGN 채널 하에서 최대 반복수가 100 인 합곱 (sum-product) 복호 알고리즘을 사용하여 모의실험을 수행하였고 그 결과는 그림 1 과 같다. 제안하는 BDD 구조를 가진 QC LDPC 부호들이 기존의 BDD 구조를 가진 QC LDPC 부호들보다 오류 마루 영역에서 더 좋은 성능을 가진다.

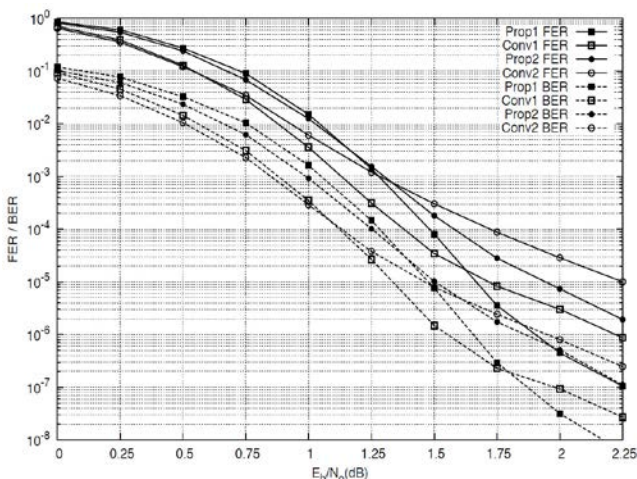


그림 1. 기존 BDD 구조와 새로운 BDD 구조를 가지는 QC LDPC 부호들의 성능 비교

5. 결론

본 논문에서는 오류 마루 영역에서 성능이 좋은 불규칙 QC LDPC 부호의 설계를 위한 새로운 BDD 구조를 제안하였다. 제안한 BDD 구조는 가중치 2 인

순환 행렬을 사용하여 차수 분포를 유동적으로 조절함으로써 최소 해밍 거리를 크게 하였다. 또한 효율적인 부호화를 지원함으로써 실제 시스템에 적용 가능한 구조임을 증명하였다. 모의 실험을 통해 기존의 BDD 구조를 가지는 QC LDPC 부호보다 제안하는 부호가 오류 마루 영역에서 더 좋은 성능을 가지는 것을 보였다.

6. 감사의 글

본 연구는 방송통신위원회의 차세대 통신 네트워크 원천기술 개발사업 (KCA-2012-08-911-04-003)과 2012 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2012-0000186).

7. 참고 문헌

- [1] T. Richardson, "Error floors of LDPC codes," in *Proc. Allerton Conf. Commun., Control, Comput.*, Oct. 2003, pp. 1426-1435.
- [2] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619-637, Feb. 2001.
- [3] IEEE, "IEEE standard for local and metropolitan area networks. Part 16: Air interface for broadband wireless access systems," *IEEE Std 802.16-2009*, May 2009.
- [4] IEEE, "IEEE standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. Amendment 5: Enhancements for higher throughput," *IEEE Std 802.11n-2009*, Oct. 2009.
- [5] S. Kudekar, T. Richardson, and R. Urbanke, "Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 803-834, Feb. 2011.
- [6] J. Chen, R. Tanner, J. Zhang, and M. Fossorier, "Construction of irregular LDPC codes by quasi-cyclic extension," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1479-1483, Apr. 2007.
- [7] T. Richardson and R. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 638-656, Feb. 2001.
- [8] R. Smarandache and P.O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto- and Tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 585-607, Feb. 2012.
- [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] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "A new block dual-diagonal structure for QC LDPC codes with low error floor," *submitted to IEEE Trans. Inf. Theory*.