

완전 차집합군으로부터 설계된 새로운 불규칙 준순환 저밀도 패리티 체크 부호

박 호 성*

New Irregular Quasi-Cyclic LDPC Codes Constructed from Perfect Difference Families

Hosung Park*

요 약

본 논문에서 다양한 블록 크기를 가지는 완전 차집합군을 이용하여 불규칙 준순환 패리티 체크 부호를 생성하는 방법을 제안한다. 제안하는 부호는 기존의 설계방법들에 비해 부호율, 부호 길이, 차수 분포 측면에서 다양한 값들을 가질 수 있다는 장점을 보인다. 또한 랜덤한 방법으로 설계하기 힘든 매우 짧은 길이의 부호를 체계적으로 설계할 수 있다. 모의실험을 통해 제안하는 부호의 오류 정정 성능을 검증한다.

Key Words : Girth, low-density parity-check codes, perfect difference family, quasi-cyclic codes

ABSTRACT

In this paper, we propose a construction method of irregular quasi-cyclic low-density parity-check codes based on perfect difference families with various block sizes. The proposed codes have advantages in that they support various values with respect to code rate, length, and degree distribution. Also, this construction enables very short lengths which are usually difficult to be achieved by a

random construction. We verify via simulations the error-correcting performance of the proposed codes.

I. 서 론

저밀도 패리티 체크 부호는 새년 한계에 근접한 오류 정정 능력을 보이는 부호로서 터보 부호와 함께 많은 통신 표준에 채택되어 있다^[1]. 특히 병렬 복호의 구현에 탁월한 구조를 가지고 있어서 5G 등의 고속 통신에 적합하다. 한편 고부호율 설계가 용이하고 낮은 오류마루를 보이는 특성으로 인해 낸드 플래시 등 메모리에도 적용되어 이용되고 있다.

통신 및 메모리 분야에서 널리 이용되면서 다양한 부호율 및 부호 길이에 대하여 좋은 성능을 보이는 저밀도 패리티 체크 부호의 설계가 필요하다. 효율적인 구현을 위해 준순환 구조를 가질 필요가 있는데, 짧은 길이 고부호율 준순환 저밀도 패리티 체크 부호에 대한 설계는 많이 알려져 있지 않다.

이에 적합한 구조로서 순환 행렬들이 단일 행으로 구성된 패리티 체크 행렬을 고려할 수 있는데, 순환 차집합군을 이용한 제한된 길이의 규칙 부호^[2]와 불규칙 부호^[3], 알고리즘에 기반한 다양한 길이의 규칙 부호^[4]가 설계된 바가 있다.

본 논문에서는 블록의 크기가 다양한 완전 차집합군을 이용하여 순환 행렬들이 단일 행으로 구성된 불규칙 준순환 저밀도 패리티 체크 부호를 설계하는 방법을 제시한다. 제안하는 부호는 [2-4]와는 달리 차수 분포, 부호율, 부호 길이를 다양하게 선택하여 설계 가능하다. 또한 점진 에지 성장 알고리즘^[5] 등의 랜덤한 방법으로 설계하기 힘든 매우 짧은 길이의 고부호율 부호를 체계적으로 설계할 수 있게 해 준다. 이러한 설계상의 장점들을 가지는 제안하는 부호의 오류 정정 성능의 검증을 위해 모의실험을 통해 점진 에지 성장 알고리즘 부호와 비교하여 동일한 성능을 가짐을 보인다.

II. 준순환 저밀도 패리티 체크 부호

하나의 정사각행렬에서 각 열이 이전 열을 아랫방

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였고 [B0717-16-0023, IoT 환경에서 massive connectivity를 위한 5G 기반 저전력, 저복잡도의 전송 및 변조·부호화 원천기술 개발] 또한 2015년도 전남대학교 학술연구비 지원에 의하여 연구되었음

* First and Corresponding Author: School of Electronics and Computer Engineering, Chonnam National University, hpark1@jnu.ac.kr, 종신회원

논문번호 : KICS2016-10-330, Received October 28, 2016; Revised November 23, 2016; Accepted December 20, 2016

향으로 1만큼 순환이동한 것에 해당하고 첫 번째 열이 마지막 열을 아래방향으로 1만큼 순환이동한 것에 해당할 때 그 행렬을 순환행렬이라 부른다. 크기 $z \times z$ 이고 가중치가 w 인 순환행렬은 각각 다른 횟수만큼 순환이동한 w 개의 $z \times z$ 단위행렬들을 이진함수로 표현할 수 있다. 순환이동한 횟수들의 집합을 그 순환행렬의 이동값 집합이라고 부른다. 준순환 저밀도 패리티 체크 부호의 패리티 체크 행렬은 $z \times z$ 크기의 순환행렬들의 배열로 정의된다.

본 논문에서는 패리티 체크 행렬이 $z \times z$ 순환행렬들의 $1 \times L$ 배열로 구성된 경우만을 생각하며 다음과 같이 표시할 수 있다.

$$H = [H_0 H_1 \dots H_{L-1}] \quad (1)$$

여기서 H_i 는 $z \times z$ 순환행렬을 나타낸다. H_i 의 가중치를 w_i 라고 하고 그 이동값 집합을 $S_i = \{s_{i,0}, s_{i,1}, \dots, s_{i,w_i-1}\}$ 라고 하자. 그러면 위의 패리티 체크 행렬은 S_i 들로 완벽히 정의됨을 알 수 있다.

III. 완전 차집합군을 이용한 부호 설계

완전 차집합군을 다음과 같이 정의한다. 집합 $A = \{a_0, a_1, \dots, a_{n-1}\} \subset Z_v$ ($a_0 < \dots < a_{n-1}$)에 대하여 멀티셋 $\Delta_+(A) = \{a_j - a_i \mid 0 \leq i < j \leq n-1\}$ 를 정의하자. 멀티셋을 위한 표기법으로 멀티셋 M 이 c 종류의 원소 m_0, \dots, m_{c-1} 을 포함하고 각 m_i 의 빈도수가 λ_i 일 때 $\{m_0^{(\lambda_0)}, \dots, m_{c-1}^{(\lambda_{c-1})}\}$ 로 표기하기로 한다. 임의의 빈도수를 가지는 원소의 경우에는 위첨자를 표시하지 않는다. Z_v 의 h 개 부분집합들의 모임을 $B = \{B_0, \dots, B_{h-1}\}$ 라 하고 B_i 안에 원소의 개수를 k_i 라고 하면 $B_i = \{b_{i,0}, \dots, b_{i,k_i-1}\}$ 으로 표현된다. 또한 멀티셋 $K = \cup_{i=0}^{h-1} \{k_i\}$ 를 정의하자. $\cup_{i=0}^{h-1} \Delta_+(B_i) = \{1^{(\lambda)}, \dots, (v-1)^{(\lambda)}\}$ 를 만족할 때 B 를 (v, K, λ) 완전 차집합군이라고 정의한다. 그리고 각각의 B_i 를 완전 차집합군의 블록이라 부른다.

본 논문에서 $k \in \{4, 5, 6, 7\}$ 일 때 $(v, \{3, k^{(1)}\}, 1)$ 완전 차집합군을 이용하여 식 (1) 형태의 패리티 체크 행렬을 가지는 준순환 패리티 체크 부호를 설계한다. 이러한 완전 차집합군이 존재하기 위한 필요충분조건은 다음과 같으며 해당 설계 방법은 [6]에 제시되어

있다.

- $(v, \{3, 4^{(1)}\}, 1) \Leftrightarrow v \equiv 1 \pmod{6}, v \geq 19$
- $(v, \{3, 5^{(1)}\}, 1) \Leftrightarrow v \equiv 9, 15 \pmod{24}, v \geq 33$
- $(v, \{3, 6^{(1)}\}, 1) \Leftrightarrow v \equiv 1 \pmod{6}, v \geq 43$
- $(v, \{3, 7^{(1)}\}, 1) \Leftrightarrow v \equiv 1, 7 \pmod{24}, v \geq 73$

이제 준순환 패리티 체크 부호의 식 (1) 형태의 패리티 체크 행렬을 $(v, \{3, k^{(1)}\}, 1)$ 완전 차집합군 $B = \{B_0, B_1, \dots, B_{h-1}\}$ 를 이용하여 이동값 집합 S_i 를 정의함으로써 설계하고자 한다. 일반성을 잃지 않고 B_0 는 크기가 k 인 블록이라고 하겠다.

- $z \geq v, L \leq 3h-2$ 을 만족하도록 z 와 L 을 선택한다.
- $S_0 = B_0$
- $1 \leq i \leq h-1$ 에 대하여 B_i 의 부분집합 중 크기가 2인 것들을 $B_{i,0}, B_{i,1}, B_{i,2}$ 라 하고 $B' = \cup_{i=1}^{h-1} \{B_i, B_{i,0}, B_{i,1}, B_{i,2}\}$ 라 하자. 그러면 모든 $1 \leq i \leq h-1, 0 \leq j \leq 2$ 에 대하여 $\{B_i, B_{i,j}\} \not\subset \{S_1, \dots, S_{L-1}\} \subset B'$ 을 만족하도록 이동값 집합들을 선택한다.

제안하는 부호는 길이 zL 와 설계 부호율 $(L-1)/L$ 을 가진다. 부호율 불규칙 저밀도 패리티 체크 부호의 경우 패리티 체크 행렬의 열 중 일부는 큰 가중치를 가지고 나머지는 가중치 2 또는 3을 가지는 경우가 많은데, 제안하는 설계방법은 $4 \leq k \leq 7$ 에 대해 열 가중치 $\{2, 3, k\}$ 를 가능하도록 하므로 유효한 차수 분포를 가진다. 따라서 제안하는 부호는 다양한 길이 및 부호율을 가질 수 있으며 차수 분포의 선택도 유동적으로 할 수 있다. 또한 제안하는 부호는 다음 정리와 같이 사이클 4를 가지지 않는다.

정리 1. 제안하는 부호는 거스 6이다.

증명. 가중치가 3 이상인 순환행렬을 포함하는 패리티 체크 행렬의 거스는 6 이하임이 알려져 있다 [7]. 식 (1)인 구조의 패리티 체크 행렬에서 사이클 4를 가지지 않을 조건은 $\cup_{i=0}^{L-1} \Delta_+(S_i)$ 에 빈도수 2 이상인 원소가 존재하지 않는 것이다. 제안하는 부호는 정의상 위의 성질을 만족하므로 거스는 6 이상이다. 따라서 위 정리는 증명된다.

예시 1. $(31, \{3^{(3)}, 4^{(1)}\}, 1)$ 완전 차집합군 $B = \{\{0, 4, 9, 15\}, \{0, 1, 8\}, \{0, 2, 14\}, \{0, 3, 13\}\}$ 로부터 이동값

집합들을 $\{0,4,9,15\}$, $\{0,1,8\}$, $\{0,2,14\}$, $\{0,3\}$, $\{0,13\}$ 으로 선택하여 길이 $n \geq 31$ 이고 부호율 4/5인 준순환 패리티 체크 부호를 설계할 수 있다.

IV. 모의실험

예시 1에서와 같이 $(31, \{3^{(3)}, 4^{(1)}\}, 1)$ 완전 차집합군을 이용하여 제안하는 부호를 생성하고 오류 정정 성능을 검증하기 위하여 점진 에지 성장 알고리즘으로 생성된 저밀도 패리티 체크 부호와 비교한다. 먼저 부호율 4/5이고 거스 6을 보장하는 설계는 제안하는 방법으로는 부호 길이 $n \geq 155$ 부터 가능하지만 점진 에지 성장 알고리즘으로는 $n \geq 190$ 부터 가능한 것을 확인하였다. 이로부터 제안하는 방법이 준순환 구조를 가짐에도 불구하고 더 짧은 길이의 부호 설계를 가능하게 하는 장점을 갖는 것을 볼 수 있다.

점진 에지 성장 알고리즘의 부호와의 성능 비교를 위하여 예시 1의 이동값 집합들을 이용하고 $z = 40$, $L = 5$ 로 설정하여 부호 길이 $n = 200$ 이고 부호율 4/5인 부호를 생성하였다. 마찬가지로 점진 에지 성장 알고리즘으로 동일한 파라미터를 가지고 거스 6인 부호를 생성하였다. 이 두 부호의 프레임 오류율과 비트 오류율의 성능이 그림 1에 나타나 있다. PROP는 제안한 부호의 성능, PEG는 점진 에지 성장 알고리즘으로 생성한 부호의 성능이다. 그림에서 볼 수 있듯이 제안하는 부호는 동일한 파라미터 하에서 점진 에지 성장 알고리즘과 같은 성능을 나타낸다. 이는 준순환 구조의 장점 하에서도 점진 에지 성장 알고리즘으로 설계 불가능한 파라미터도 설계할 수 있고, 비교할 수

있는 파라미터에 대해서도 동일한 성능을 보장함을 의미한다.

V. 결론

본 논문에서 $k \in \{4, 5, 6, 7\}$ 에 대하여 $(v, \{3, k^{(1)}\}, 1)$ 완전 차집합군을 이용하여 준순환 패리티 체크 부호를 설계하는 방법을 제안하였다. 제안하는 부호는 $n \geq v$ 인 임의의 부호 길이를 가능하게 하며 부호율도 다양한 값 중 선택할 수 있게 한다. 또한 거스 6을 보장하고 오류 정정 성능도 부호율 4/5, 길이 200에 대해 점진 에지 성장 알고리즘으로 생성한 부호와 동일함을 확인하였다.

References

- [1] C.-U. Baek and J.-W. Jung, "A study on turbo equalization for MIMO systems based on LDPC codes," *J. KICS*, vol. 41, no. 5, pp. 504-511, May 2016.
- [2] B. Vasic and O. Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1156-1176, Jun. 2004.
- [3] S. J. Johnson and S. R. Weller, "A family of irregular LDPC codes with low encoding complexity," *IEEE Commun. Lett.*, vol. 7, no. 2, pp. 79-81, Feb. 2003.
- [4] T. Xia and B. Xia, "Quasi-cyclic codes from extended difference families," in *Proc. IEEE Wireless Commun. Netw. Conf.*, pp. 1036-1040, New Orleans, LA, USA, Mar. 2005.
- [5] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386-398, Jan. 2005.
- [6] D. Wu, M. Cheng, and Z. Chen, "Perfect difference families and related variable-weight optical orthogonal codes," *Australian J. Combin.*, vol. 55, pp. 153-166, 2013.
- [7] R. M. Tanner, "Spectral graphs for quasi-cyclic LDPC codes," in *Proc. IEEE Symp. Inf. Theory*, p. 226, Washington, D.C., USA, Jun. 2001.

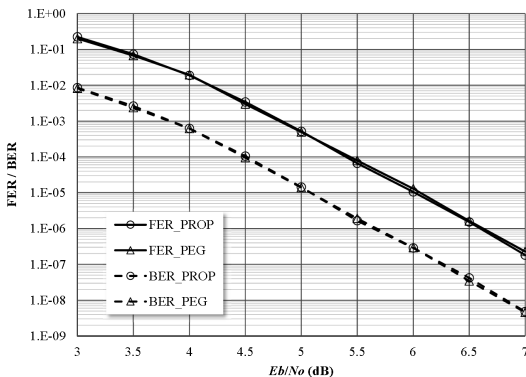


그림 1. 점진 에지 성장 알고리즘 부호와 제안하는 부호의 프레임 오류율과 비트 오류율 비교
Fig. 1. Comparison of frame error rate and bit error rate between the proposed LDPC codes and the codes constructed from the progressive edge growth algorithm