

조합론과 디자인 이론을 이용한 준순환 저밀도 패리티 체크 부호의 거스 분석 및 프로토타입 설계

*박호성°, *홍석범, *노종선, **신동준

*서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소

**한양대학교 전자통신컴퓨터공학부

Girth Analysis and Protograph Design for Quasi-Cyclic LDPC Codes Using Combinatorics and Design Theory

*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

{lovepark98,fousbyus}@ccl.snu.ac.kr, jsno@snu.ac.kr, djshin@hanyang.ac.kr

요 약

본 논문에서는 준순환 저밀도 패리티 체크 (quasi-cyclic low-density parity-check, QC LDPC) 부호의 거스를 제한하는 프로토타입 (protograph)의 부그래프 패턴을 다중 에지 (multiple edge) 까지 고려하여 분류하고 분석한다. 이에 근거하여 거스 14 이상의 정칙 (regular) QC LDPC 부호를 위한 프로토타입의 설계 방법을 다중 에지를 고려하여 제시한다.

1. 서론

저밀도 패리티 체크 (low-density parity-check, LDPC) 부호는 채널 용량에 근접하는 성능으로 인해 지난 십여년간 많은 주목을 받아 왔다. 특히 준순환 (quasi-cyclic, QC) LDPC 부호는 패리티 체크 행렬이 규칙적인 구조를 가짐에 따라 하드웨어 구현이나 병렬 복호 방식 등에서 강점을 보이게 되어 많은 표준들에서 채택되어 사용되고 있다. 이러한 QC LDPC 부호는 프로토타입 (protograph)에 기반한 LDPC 부호로 볼 수 있다 [2]. 임의의 프로토타입에서 순환 치환 (cyclic permutation)을 이용하여 패리티 체크 행렬을 구성하면 QC LDPC 부호가 되기 때문이다. 따라서 QC LDPC 부호의 성능은 프로토타입의 설계와 밀접한 관련이 있다.

조합론 (combinatorics)과 그래프 이론 (graph theory), 디자인 이론 (design theory) 등은 QC LDPC 부호를 설계하는데 있어서 많이 이용되어 왔다 [1]-[4]. 특히 큰 거스 (girth)를 가지는 QC LDPC 부호를 위해 패리티 체크 행렬 자체의 설계와 프로토타입의 설계 등의 과정에서 이러한 이론들을 사용할 수 있다. [4]에서는 단일 에지 (single edge)로만 구성된 프로토타입의 설계 방법을 디자인 이론을 이용하여 제시하였다. 본 논문에서는 거스가 큰 QC LDPC 부호를 얻기 위하여 단일

에지와 다중 에지 (multiple edge)를 모두 가질 수 있는 프로토타입을 디자인 이론을 이용하여 체계적으로 설계할 것이다. 이를 위해서 QC LDPC 부호가 큰 거스를 가지게 하지 못하는 부그래프 패턴 (subgraph pattern)을 다중 에지를 고려하여 모두 찾고 분석할 것이다.

2. 프로토타입의 부그래프 패턴

본 논문에서는 ‘프로토타입’은 이분 그래프 (bipartite graph) 자체와 그것의 결합 행렬 (incidence matrix)를 모두 의미하는 용어로 사용하겠다. 임의의 프로토타입 $P = [p_{ij}]_{ij}$ 에 대하여 $p_{ij} \geq 2$ 인 경우에는 수평 노드 (horizontal node) i 와 수직 노드 (vertical node) j 사이에 다중 에지가 있다는 것을 의미한다. [5]에 나와 있는 것처럼 다음 두 종류의 그래프를 정의하도록 하자.

정의 1: (x_1, x_2, x_3) -theta 그래프는 $T(x_1, x_2, x_3)$ 로 표기되는데, 서로 만나지 않는 세 개의 경로 (path) X_1, X_2, X_3 로 연결되어 있는 차수 (degree) 3인 두 개의 노드로 이루어지는 그래프이다. 각각의 경로는 $x_1 \geq 1, x_2 \geq 1, x_3 \geq 1$ 개의 에지로 이루어져 있다. $(z_1, z_2; y)$ -dumbbell 그래프는 $D(z_1, z_2; y)$ 로 표기되는데, 에지가

서로 만나지 않는 두 개의 사이클 (cycle) Z_1, Z_2 와 그들을 연결하는 경로 Y 로 구성되는 그래프이다. 여기서 Z_1, Z_2, Y 는 각각 $z_1 \geq 1, z_2 \geq 1, y \geq 0$ 개의 에지로 이루어져 있다.

정의 2: 임의의 프로토그래프에 대한 불가피 사이클 (inevitable cycle)은 이동 값이나 순환 치환의 크기에 상관 없이 해당 QC LDPC 부호에서 발생하게 되는 사이클들 중 가장 짧은 길이의 것이다.

정의 3: 부그래프 패턴 P_{2i} 는 다음의 성질을 만족하는 이분 그래프로 정의된다.

- 1) P_{2i} 는 길이 $2i$ 인 불가피 사이클을 가진다.
- 2) P_{2i} 는 길이가 $2i$ 이상인 불가피 사이클을 가지는 부그래프를 갖지 않는다.
- 3) 행의 개수는 열의 개수보다 작다.
- 4) 동형 (isomorphic) 그래프를 고려하여 하나의 그래프만이 P_{2i} 로 표현된다.

[5]에서의 결과에 근거하여 다음의 두 정리를 주장할 수 있다.

정리 1: P_{2i} 는 theta 그래프 형태이거나 dumbbell 그래프 형태이다.

정리 2: $T(x_1, x_2, x_3)$ 와 $D(z_1, z_2; y)$ 는 각각 길이 $2(x_1 + x_2 + x_3), 2(z_1 + z_2) + 4y$ 인 불가피 사이클을 가진다.

위의 두 정리와 P_{2i} 의 정의에 의해 모든 부그래프 패턴을 찾을 수 있으며, 길이 14까지 구한 결과는 다음과 같다.

$$P_6 = [3], \quad P_8 = [22]$$

$$P_{10} = \begin{bmatrix} 21 \\ 11 \end{bmatrix}, \quad P_{12} = \begin{bmatrix} 21 \\ 10 \end{bmatrix}, \begin{bmatrix} 211 \\ 011 \end{bmatrix}, \begin{bmatrix} 111 \\ 111 \end{bmatrix}$$

$$P_{14} = \begin{bmatrix} 210 \\ 101 \\ 011 \end{bmatrix}, \begin{bmatrix} 111 \\ 110 \\ 101 \end{bmatrix}$$

이제부터는 P_{2i} 의 개수에 대해서 분석해 보기로 하겠다. $T(x_1, x_2, x_3)$ 와 $D(z_1, z_2; y)$ 로부터 형성된 P_{2i} 의 개수를 각각 n_{2i}^T, n_{2i}^D 라고 하자. n_{2i}^T 를 구하기 위해서는 방정식 $2(x_1 + x_2 + x_3) = 2i$ 를 풀어야 하며, 해의 개수는 i 가 짝수일 때와 홀수일 때에 따라 다르게 표현된다. 먼저 $i = 2i'$ 일 때 x_1, x_2, x_3 는 모두 짝수이어야 하며, 위의 방정식은 $x_1' + x_2' + x_3' = i'$ 와 동치가 된다. 여기서 $x_1' = \frac{x_1}{2}, x_2' = \frac{x_2}{2}, x_3' = \frac{x_3}{2}$ 이다. 동형사상 (isomorphism)을 고려한 조건 $x_1' \geq x_2' \geq x_3' \geq 1$ 하에서 위의 방정식의 해의 개수를 구하는 문제는 조합론에서의 정수 분할 (integer partitions) [6] 문제에 해당한다. 이를 닫힌 형식 (closed form)으로 표현할 수 없지만 재귀식을 이용하여 $n_{4i'}^T$ ($i' \geq 3$)를 구할 수 있으며, 이와 동일한 방법으로 $n_{4i'-2}^T, n_{4i'}^D, n_{4i'-2}^D$ ($i' \geq 2$)를 구할 수 있다. 이것들을 정리한 결과는 다음과 같다.

$$n_{4i'}^T = \sum_{k=0}^{q_e-1} \left\lfloor \frac{i' - (3k+1)}{2} \right\rfloor$$

$$n_{4i'-2}^T = \sum_{k=0}^{q_e-1} \left\lfloor \frac{i' - 3k}{2} \right\rfloor$$

$$n_{4i'}^D = \frac{1}{2} \left(\binom{i'+2}{2} + \left\lfloor \frac{i'}{2} \right\rfloor - 1 \right) - i'$$

$$n_{4i'-2}^D = 0$$

여기서 $q_e = \left\lfloor \frac{i'}{3} \right\rfloor, q_o = \left\lfloor \frac{i'+1}{3} \right\rfloor$ 이다.

다중 에지를 갖는 P_{2i} 의 개수에 대해서 분석해 보자. $T(x_1, x_2, x_3)$ 와 $D(z_1, z_2; y)$ 로부터 형성된 P_{2i} 의 개수를 각각 m_{2i}^T, m_{2i}^D 라고 하자. 그리고 다중 에지를 갖는 부그래프 패턴은 모두 $T(x_1, 1, 1)$ 과 $D(z_1, 2; y)$ 로부터 기인함을 알 수 있다. 위에서의와 동일한 방법으로 $i' \geq 2$ 에 대해 다음의 결과를 얻을 수 있다.

$$m_{4i'}^T = 0, m_{4i'-2}^T = 1, m_{4i'}^D = i' - 1, m_{4i'-2}^D = 0$$

3. 거스 14 이상인 QC LDPC 부호를 위한 프로토그래프 설계

불가피 사이클의 길이가 $2i$ 이상인 프로토그래프를 설계하기 위해서는 그 내부에 $P_{2i'}$ ($i' < i$)를 부그래프로 가지고 있지 않아야 한다. 불가피 사이클의 길이가 8 또는 10 이상인 프로토그래프를 설계하는 것은 간단하며, 12 이상인 정칙 (regular) 프로토그래프의 설계는 [7]에서 제시하였다. 본 장에서는 불가피 사이클의 길이가 14 이상인 정칙 프로토그래프의 설계 방법을 제시한다.

크기가 $J \times L$ 이고 열 가중치 (column weight)와 행 가중치 (row weight)가 각각 d_v, d_c 인 프로토그래프를 고려해 보자. 불가피 사이클의 길이가 14 이상인 정칙 프로토그래프 설계의 기준이 되는 두 가지 정리는 다음과 같다. 증명은 생략하기로 한다.

정리 3: $d_v = 3, d_c \geq 4$ 이고 불가피 사이클의 길이가 14 이상인 정칙 프로토그래프는 이중 (double) 에지를 최대 $J-2$ 개까지 가질 수 있다.

정리 4: $d_v = 3, d_c \geq 4$ 이고 이중 에지의 개수가 $J-2$ 인 정칙 프로토그래프가 길이가 14 이상인 불규칙 사이클을 갖는다고 가정해 보자. 그러면 J 와 d_c 사이에는 다음의 관계가 성립한다.

- 1) $J \equiv 0 \pmod{6}$ 일 때 $d_c = \frac{J-2}{2}, \frac{J}{2}$
- 2) $J \equiv 1 \pmod{6}$ 일 때 $d_c = \frac{J-1}{2}$
- 3) $J \equiv 2 \pmod{6}$ 일 때 $d_c = \frac{J-2}{2}$
- 4) $J \equiv 3 \pmod{6}$ 일 때 $d_c = \frac{J-1}{2}, \frac{J+1}{2}$
- 5) $J \equiv 4 \pmod{6}$ 일 때 $J=10, d_c=6$ 인 경우를 제외하면 존재하지 않음
- 6) $J \equiv 5 \pmod{6}$ 일 때 $d_c = \frac{J+1}{2}$

본 논문에서는 $d_v = 3$ 이고 프로토그래프에 이중 에지가 최대로 존재하는 경우에 대한 설계 기준과 방법을 제

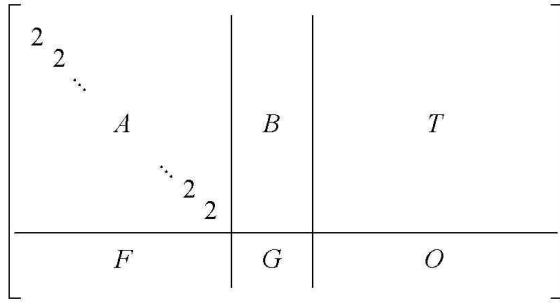


그림 1. 불가피 사이클의 길이가 14 이상인 정칙 프로토그래프의 구조

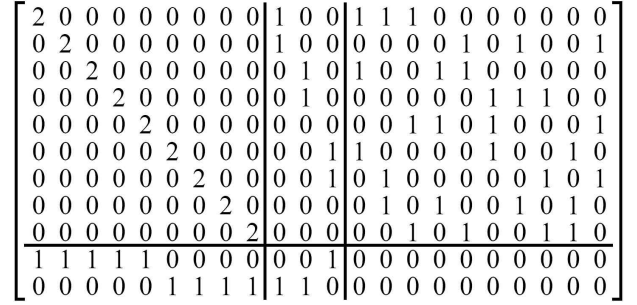


그림 2. 불가피 사이클의 길이가 14 이상인 11×22 정칙 프로토그래프 ($d_v = 3, d_c = 6$)

시한다. 다중 에지의 개수가 최대가 아니거나 $d_v \geq 4$ 인 경우에도 제시한 방법과 비슷하게 설계할 수 있다.

불가피 사이클의 길이가 14 이상인 정칙 프로토그래프의 구조는 그림 1과 같이 표현된다. A 에서는 대각 원소들은 모두 '2'이고 나머지는 '0'이 되는데, 이는 P_{12} 의 첫 번째 패턴을 피하기 위함이다. 행렬 F 는 d_v 를 맞추기 위한 '1'들이 존재하게 되고, G 는 d_c 를 맞추기 위한 가중치가 0이 아닌 열들을 가진다. B 역시 d_v 를 맞추기 위한 '1'들을 가지게 된다. O 는 영행렬이며 T 는 기 설계된 A 와 B 에 따라 d_c 를 맞추기 위한 '1'들이 존재하게 된다. 정리 4를 만족하는 인자들에 대해서 불가피 사이클의 길이가 14 이상이 되기 위한 F, G, B 는 항상 존재하며 그 설계 과정은 다음과 같다.

- 1) F 에서 $J-2$ 개의 '1'들은 열 가중치가 모두 1이면서 두 행의 가중치는 같거나 1 차이 나게 배치된다.
- 2) G 는 d_c 를 맞추기 위한 나머지 '1'들을 가지게 되는데 각 열의 가중치가 1이 되게 한다.
- 3) B 는 가중치가 2인 열들을 가지게 되는데, 각 행의 가중치는 1을 넘지 않으며 A, B, F, G 전체에서 P_{10} 이 발생하지 않도록 '1'을 배치한다.

이제는 T 의 설계에 대해서 살펴보자. T 안에 있는 열들의 가중치는 모두 3이고, P_{12} 의 두 번째와 세 번째 패턴이 발생하지 않기 위해서는 동일한 쌍의 '1'이 B 와 T 전체에 나타나서는 안된다. 정리 4에서 제시된 J 와 d_c 들은 T 가 최적 패킹 (optimal packing) [8]에 거의 근접하는 경우에서 도출되었다. 따라서 각 경우의 J 에 대하여 B 에 있는 '1'의 쌍들을 피하면서 최적 패킹의 결합 행렬에서 작은 개수의 열을 제거함으로써 T 를 만들 수 있다. 그림 2에서는 $J=11, d_c=6$ 인 경우에 Steiner system [8]으로부터 얻어진 프로토그래프가 제시되어 있다.

4. 결론

조합론과 그래프 이론을 이용하여 QC LDPC 부호의 거스를 제한하는 프로토그래프의 부그래프 패턴을 단일 에지와 다중 에지까지 고려하여 모두 분류하였고, 각각의 패턴에 대하여 분석하였다. 이를 바탕으로 거스 14 이상의 정칙 QC LDPC 부호를 위한 프로토그래프의 설계 기준을 디자인 이론을 이용하여 제시하였다.

5. 감사의 글

본 연구는 방송통신위원회의 차세대 통신 네트워크 원천기술 개발사업 (KCA-2011-08913-04003)과 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2011-0000328).

6. 참고 문헌

- [1] 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, June 2004.
- [2] M. Fujisawa and S. Sakata, "A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8," *IEICE Trans. Fund.*, vol. E90-A, no. 5, May 2007.
- [3] M. Esmaeili and M. Tadayon, "A novel approach to generating long low-density parity-check codes using two configurations," *IET Commun.*, vol. 2, no. 4, pp. 587-597, 2008.
- [4] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, "Quasi-cyclic low-density parity-check codes with girth larger than 12," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2885-2891, Aug. 2007.
- [5] C. Kelley and J. Walker, "LDPC codes from voltage graphs," in *Proc. IEEE Int'l Symp. on Inf. Theory*, Toronto, Canada, July 2008, pp. 792-796.
- [6] M. Bona, *A Walk Through Combinatorics, 2nd ed.* Toh Tuck Link, Singapore: World Scientific, 2006.
- [7] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "Protograph design for QC LDPC codes with large girth," in *Proc. Int'l Conf. ICT Convergence*, Cheju Island, Korea, Nov. 2010, pp. 175-176.
- [8] C. Colbourn and J. Dinitz, *The CRC Handbook of Combinatorial Designs*. Boca Raton, FL: CRC, 1996.