블록 LDPC 부호 설계를 위한 사이클 탐색 알고리즘

명세창, 전기준, 고병훈, 김경준, 김광순
연세대학교 전기전자공학부

myungse@dcl.yonsei.ac.kr, puco201@dcl.yonsei.ac.kr, bhko@dcl.yonsei.ac.kr,
kimkj@dcl.yonsei.ac.kr, ks.kim@yonsei.ac.kr

A Cycle Search Algorithm for Design of Block LDPC Codes

Se Chang Myung, Ki Jun Jeon, Byung Hoon Ko, Kyung Jun Kim, Kwang Soon Kim
Department of Electrical and Electronic Engineering, Yonsei University

요 약

본 논문은 블록 LDPC 부호를 설계하기 위해 테너 그래프에서 메시지-패싱 기반의 사이클을 찾는 알고리즘을 제안한다. 이 알고리즘은 기존 트리 기반의 사이클 탐색 알고리즘에 비해 복잡도가 낮고 특정 노드로 인하여 발생하는 모든 길이의 사이클을 찾아낸다. 블록 단계에서 반복적인 사이클 탐색을 통해 행렬 저장공간을 절약하면서 패리티 검사 행렬의 최소 사이클의 길이를 최대로 만들 수 있다. 또한 사이클의 개수와 길이를 지표로 하여 PEG(Progressive edge-growth)나 ACE(Approximate cycle extrinsic message degree) 알고리즘에 활용하면 효율적으로 LDPC 코드 구조를 설계 할 수 있다.

Ⅰ. 서 론

[1]에서 무한한 블록 길이를 갖고 주기가 없다고 가정한 LDPC(low density parity check)부호의 성능은 거의 샤논의 한계에 가깝다. 하지만 [2]에서 유한한 블록 길이를 갖는 부호의 테너 그래프에서는 사이클이 존재하기 때문에 심각한 성능저하가 발생한다. 높은 성능의 LDPC 부호 구조를 만들기 위해서는 패리티 검사 행렬의 최소 사이클 길이를 최대한 길게 만들어야 한다. 기존의 [3]과 같은 트리 기반의 사이클 탐색 방법은 복잡도가 너무 높고 [4]에서 제시한 메시지-패싱 기반의 사이클 탐색 알고리즘은 복잡도는 낮지만 최소 길이의 사이클 밖에 찾지 못한다. 본 논문에서는 [4]와 [5]를 활용하여 순환 천이 행렬에서 특정 노드가 포함된 모든 길이의 사이클과 개수를 찾는 효율적인 알고리즘을 제안한다. 또한 패리티 검사 행렬과의 관계를 이용하여 행렬 저장 공간을 절약하면서 효율적인 LDPC 부호 구조를 설계를 할 수 있다.

Ⅱ. 본론

1. 특성 행렬에서 사이클과 패리티 검사 행렬과의 관계

[4]를 기반으로 순환 천이 행렬의 테너 그래프에서 메시지-패싱 알고리즘과 유사하게 0 을 포함한 양의 정수를 메시지로 사용한다. 각각의 노드에서 갱신 공식은 아래와 같이 정의된다.

$$y_{ij} = \left(\bigoplus_{j' \in E_i} x_{ij'} \right) \otimes x_{ij} \tag{1}$$

여기서 x_{ij} 는 i 번째 노드로 들어가는 j 번째 엣지의 메시지 값, y_{ij} 는 i 번째 노드에서 j 번째 엣지로 나가는 메시지 값, 그리고 E_i 는 i 번째 노드와 연결된 엣지들의 집합이다. 연산 $\oplus$ 와 $\otimes$ 는 다음과 같이 정의된다.

$$\begin{cases} x \oplus y = x + y, & x, y \in \mathbb{Z}^+ \cup \{0\}, \\ x \otimes 0 = 0 \otimes x = x, & x \in \mathbb{Z}^+ \cup \{0\}, \\ x \otimes y = 0, & x, y \in \mathbb{Z}^+, \end{cases} \tag{2}$$

여기서 $+$ 는 산술 덧셈 그리고 $\mathbb{Z}^+$ 는 양의 정수들의 집합을 나타낸다. 본 논문에서는 노드 관점에서 출발 노드를 포함하는 모든 사이클과 그 길이를 탐색한다. 처음에 출발 변수 노드와 연결된 모든 엣지에는 메시지 1 을 나머지 모든 엣지에는 0 의 메시지를 설정한다.

[5]와 같이 패리티 검사 행렬과 순환 천이 값을 원소로 갖는 특성 행렬을 정의하고 이 행렬로 정의되는 테너 그래프에서 $\mu = \{\mu_0, \mu_1, \ldots, \mu_{2l_\mu} - 1\}$ 를 사이클 길이 $2l_\mu$ 인 사이클로 정의한다. 여기서 μ_i 는 사이클 μ 의 i 번째 엣지에 해당하는 특성 행렬 C_H 의 원소 값이다.

$$s_l(\mu) = \underbrace{\left(\sum_{k=0}^{l-1} (-1)^k \mu_k \right)}_{p_l(\mu)} \bmod B, \tag{3}$$

여기서 $1 \le l \le 2l_\mu$, $s(\mu) = s_{2l_\mu}(\mu)$, $p_l(\mu)$ 는 부분합, 그리고 $x \bmod B$ 는 $x < 0$ 일 때 $(B + x) \bmod B$ 로 정의한다. 위와 같이 정의하면 [5]의 정리 2 에 의해서 $s_l(\mu)$ 와 B 의 최대 공약수 $\beta(\mu)$ 는 패리티 검사 행렬에서의 사이클 개수가 되고 그 길이는 $2Bl_\mu / \beta(\mu)$ 가 된다.

2. 제안하는 알고리즘의 개요와 예제

다음의 그림 1 은 본 논문에서 제공하는 사이클 탐색 알고리즘의 슈도-부호(pseudo-code)이다.

Input: l_0, N_{iter}, E, C_H, B
if(the new edge is not the first edge of two nodes which it is connected to){

set $k=1, t=1$, Length_cycle=0, Number_cycle=0, $(i_p, j_p)=\mathrm{IND}(l_p)$ $l_p \in E$

set $n(E(j_{l_0}))=1$, $n(l)=0$ $l \in E \setminus \{E(j_{l_0})\}$, $p(t, E(j_{l_0}))=C_H(i_{l_0}, j_{l_0})$

while$(k < N_{iter})\{$ $t=t+1$

for$(l=0; l<|E|; l++)\{$ $m(l)=\left(\underset{i' \in E(i_l)}{\oplus} n(l')\right) \otimes n(l)$

if $(n(l)>0)$ $p(t, E(i_l))=p(t-1, E(j_l))-C_H(i_l, j_l)$

if $\left(w=\sum_{l \in E(j_l)} n(l)>2\right)\{s(t, E(i_l))=p(t, E(i_l)) \bmod B,\ \beta(t, E(i_l))=\gcd(s, B)$

Length_cycle$=2*t*B/\beta$, Number_cycle$={}_wC_2\}\}$ $t=t+1$

for$(l=0; l<|E|; l++)\{$ $n(l)=\left(\underset{i' \in E(i_l)}{\oplus} m(l')\right) \otimes m(l)$

if $(m(l)>0)$ $p(t, E(j_l))=p(t-1, E(i_l))+C_H(i_l, j_l)$

if $\left(w=\sum_{l \in E(i_l)} m(l)>2\right)\{s(t, E(j_l))=p(t, E(j_l)) \bmod B,\ \beta(t, E(j_l))=\gcd(s, B)$

Length_cycle$=2*t*B/\beta$, Number_cycle$={}_wC_2\}\}$ $k=k+1$ $\}$

$\}$

Output: Number_cycle, Length_cycle

그림1. 제안하는 사이클 탐색 알고리즘의 개요

여기서 l_0 는 새로 추가된 엣지의 인덱스, N_{iter} 최대 반복횟수, E 는 모든 엣지들의 집합이다. i_p 와 j_p 는 p 번째 엣지와 연결된 검사노드와 변수노드의 인덱스이다. IND 는 각 엣지가 어떤 노드와 연결되어 있는지를 매핑 해주는 함수이다. $E(i_l)$ 과 $E(j_l)$ 은 각각 검사노드 i_l 과 연결된 모든 엣지의 집합과 변수노드 j_l 과 연결된 모든 엣지들의 집합을 뜻한다.

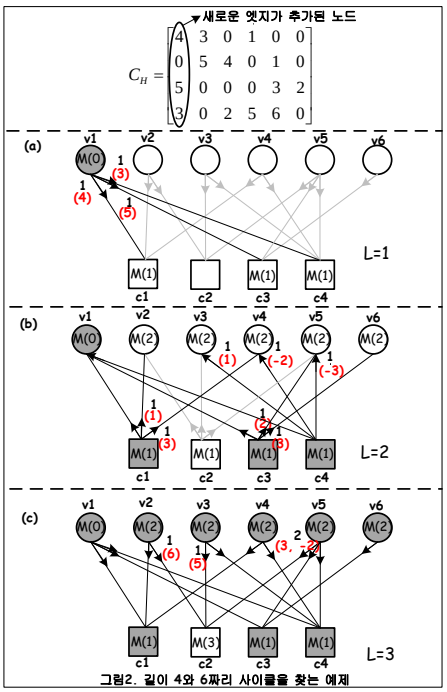

그림2. 길이 4와 6짜리 사이클을 찾는 예제

위의 그림은 순환 천이 값을 원소로 갖고 $B=6$ 인 특성 행렬을 테너 그래프로 나타낸 것이다. $M(0)$ 은 출발 변수 노드만을 포함하는 집합이고 $M(l-1)$, $l=1,2,\ldots$ 은 l 번째 반복에 0 이 아닌 메시지가 적어도 한번 거쳐간 노드들의 집합이다. 엣지 옆의 숫자는 현재 메시지 값과 부분합 $p_l(\mu)$ 이다. L 은 반복 횟수로 그림 2 의 (b)에서 v_4 와 v_5 로 0 이 아닌 두 개의 메시지가 들어오기 때문에 반복 횟수의 두 배인 4 를 길이로 갖는 사이클 두 개가 검출되고 최종 부분합 값은 각각 5 가 된다. 따라서 식(3)에 의해 $s_l(\mu)$ 과 $\beta(\mu)$ 값은 각각 5 와 1 이 되어, 패리티 체크 행렬에서 길이가 $6\times4/1=24$ 인 사이클이 두 개 존재한다. 마찬가지로 그림 2 의 (c)에서 $(1,1,2)$ 세 개의 메시지가 c_2 노드로 들어오므로 길이가 6 인 사이클이 존재하고 개수는 5 가 된다. 또한 방향과 조합을 고려한 부분합은 $(1,3,8,2,7)$ 이 되어 패리티 검사 행렬에서는 길이가 $(36,12,18,18,36)$ 인 사이클이 각각 $(1,3,2,2,1)$ 개씩 존재함을 계산 할 수 있다.

제안하는 알고리즘은 출발 노드에 연결된 모든 엣지로 메시지를 보내기 때문에 각각 시계/반시계 방향으로 이동하던 0 이 아닌 두 개 이상의 메시지가 한 노드에서 만나면 사이클이 형성된 것으로 정의한다. 식(1)에 의해 각 노드에 메시지가 들어오면 그 메시지가 거친 경로의 수를 갱신하여 나머지 엣지들로 메시지를 전파한다. 메시지가 들어온 엣지로는 다시 메시지를 보내지 않기 때문에 중복 없이 메시지 값은 경로의 수가 된다. 따라서 메시지들의 조합 수는 곧 사이클의 개수가 되고 반복 횟수의 두 배는 그 사이클의 길이가 된다. 반복 과정을 거치면서 모든 노드와 엣지를 적어도 한번은 거쳐가게 되므로 모든 사이클과 그 길이를 찾을 수 있다. 반복과정에서 메시지가 모두 사라지거나 두 개 이상의 0 이 아닌 메시지가 들어오는 노드가 한 개도 없다면 사이클이 존재 하지 않는 것이다.

Ⅲ. 결론

본 논문에서는 순환 천이 행렬로 정의되는 테너 그래프에서 메시지-패싱 알고리즘을 기반으로 사이클을 검출하고 그 길이와 개수를 찾는 낮은 복잡도의 알고리즘 제안하였다. 이와 동시에 순환 천이 값을 활용하여 패리티 검사 행렬의 사이클 길이와 개수를 계산하였다. 이를 통하여 적은 행렬 저장 공간으로도 패리티 검사 행렬의 최소 사이클 길이를 최대로 만들 수 있다. 또한 사이클의 길이뿐만 아니라 개수가 포함된 지표를 사용하면 PEG 나 ACE 알고리즘에 결합하여 효율적인 LDPC 부호 설계를 할 수 있다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 및 정보통신산업진흥원의 IT 융합 고급인력과정 지원사업의 연구결과로 수행되었음 (NIPA-2013-H0401-13-2006).

참 고 문 헌

[1] 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. 638-656, Feb. 2001.

[2] D. J. C. Mackay," Good error correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399-431, Mar. 1999.

[3] Y. Mao and A.H. Banihashemi," A heuristic search for good low-density parity-check codes at short block lengths," in *Proc. IEEE Int. Conf. Comm.*, vol. 1, pp. 11-14, Helsinki, Finland, June 2001.

[4] S. H. Lee, K. S. Kim, Y. H. Kim and J. Y. Ahn," A cycle search algorithm based on a message-passing for the design of good LDPC codes," *IEICE Trans. Fundam.*, vol.E88-A, no. 6, pp. 1955-1604, June 2005.

[5] K.S. Kim, S.H. Lee, Y.H. Kim and J.Y. Ahn," Design of binary LDPC code using cyclic shift matrices," *Electro. Lett.*, vol. 40, no. 5, pp. 325-326, Mar. 2004.