논문 2008-45TC-2-1

LDPC 부호화를 위한 효율적 알고리즘

(An Efficient Algorithm for LDPC Encoding)

김 성 훈*, 이 문 호**

(Sung Hoon Kim and Moon Ho Lee)

요 약

LDPC 구조는 1개의 개수가 적은 구조의 패리티 체크 행렬을 구성하여도, H행렬의 역행렬을 구하는 과정 중에 가우시안 소거법으로 인하여 H 행렬은 1의 개수가 적은 성질이 없어지고 계산량도 블록 크기 당 n^2의 계산량이 요구되어지고 있다. 그러므로 LDPC 패리티 체크 행려인 H는 좀 더 효율적인 부호화에 초점을 두고 개발되고 있다. 본 논문에서는 edge-by-edge 방법으로 체크 노드와 심볼 노드사이를 연결하거나 연결선을 정하는 것으로 큰 girth를 가지는 Tanner 그래프를 구성할 수 있는 PEG 알고리즘을 변형 시킨 M-PEG를 패리티 체크 행렬인 H를 구성하고 좀 더 효율적으로 부호화기를 구성할 수 있도록 dual-diagonal 형태를 지니는 H를 구성한다.

Abstract

Although we can make a sparse matrices for LDPC codes, the encoding complexity per a block increases quadratically by n^2. We propose modified PEG algorithm using PEG algorithm having a large girth by establishing edges or connections between symbol and check nodes in an edge-by-edge manner. M-PEG construct parity check matrices. So we propose parity check matrices H form a dual-diagonal matrices that can construct a more efficient decoder using a M-PEG(modified Progressive Edge Growth).

Keywords : PEG, LDPC, dual-diagonal

Ⅰ. 서 론

통신에서 가장 근본적인 문제는 채널(Channel)을 통하여 얼마나 효율적이고 신뢰성 있게(reliabley) 데이터를 전송할 수 있느냐 하는 것이다. 통신 시스템의 기본적인 블록도는 그림 1과 같다.

LDPC 부호(Low Density Parity Check)는 패리티 검사 행렬의 원소가 대부분 0인 선형 블록 부호(linear block code)로써 Shannon의 채널 용량의 한계에 근접하는 우수한 부호이다. 1962년 Gallager에 의해 처음 제안되었지만 당시의 기술력으로는 구현이 불가능한 정도의 복잡도로 인해 오랜 기간동안 사용하지 않았으나 1995년 Mackey와 Neal의 재발견 이후 LDPC 부호에 대한 활발한 연구가 이루어지고 있다.[7]

LDPC 부호는 우수한 성능에도 터보 부호에 비하여 부호화 복잡도가 너무 크다는 단점을 가지고 있다. LDPC 부호의 부호화 과정은 검사 행렬로부터 가우스 소거법을 통해 생성 행렬을 구한 후 행렬 곱셈을 통하여 부호화 과정이 이루어지게 되며, 이 경우 생성행렬의 1의 개수가 적은 성질이 유지되지 않으므로 부호화 과정의 복잡도가 크게 증가되는 문제가 발생한다.

이러한 이유 때문에 IEEE 802.16e에 제안된 대부분

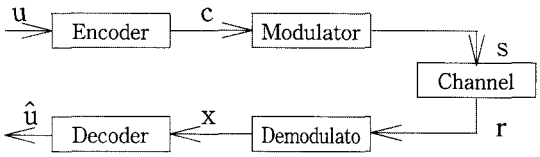


그림 1. 기본적인 통신시스템의 블록도
Fig. 1. Basic Communication system Block.

* 학생회원, ** 정회원, 전북대학교 전자정보공학부
(Chonbuk National University)

※ 이 논문은 2007년도 정부(과학기술부)의 재원으로 국제과학기술협력재단의 지원을 받아 수행된 연구임 (No. K20711000013-07A0100-01310).
접수일자: 2007년11월14일, 수정완료일: 2008년2월15일

의 LDPC 부호는 효율적인 부호화에 초점을 맞추어 개발되고 있으며, 여러 가지 다양한 구조를 가진 LDPC 부호들이 제안되었다. 본 논문에서는 Tanner그래프를 이용하여 패리티 체크 행렬인 H의 girth 조건을 좋게 하고 효율적으로 구성할 수 있는 PEG 알고리즘에 대해 설명하고 PEG 알고리즘을 변형을 통해 좀 더 효율적으로 부호화기를 구성할 수 있는 알고리즘을 구성한다.

Ⅱ장에서는 PEG 알고리즘을 이용한 패리티 체크 행렬인 H를 구성하는 방법에 대해 알아보고, Ⅲ장에서는 제안한 알고리즘으로 효율적인 부호화기를 생성할 수 있는 방법에 대해 논의하기로 한다. Ⅳ장에서는 모의실험 결과로 본 논문에서 제시한 알고리즘일 효율적이라는 것을 증명한다.

Ⅱ. 본 론

1. PEG 알고리즘

가장 큰 가능성 있는 girth를 가진 Tanner 그래프를 구성하는 것은 어려운 결합 문제이다. 하지만 이런 어려움에도 불구하고도 상대적으로 큰 girth를 가진 Tanner 그래프를 구성하기 위한 알고리즘은 가능하며, 특히 이런 알고리즘을 PEG알고리즘이라 한다. 이 PEG 알고리즘에서 심볼 노드의 국부 girth는 새로운 edge가 이 심볼 노드에 추가될 때마다 최대화 된다. 주어진 그래프에는 심볼 노드의 수 n, 체크 노드의 수 m, 그리고 심볼 노드의 차 수열 D_s를 파라미터로 한다. 이 파라미터들을 가지고 연결선 선택 절차가 시작된다. 또한 그래프의 새로운 모서리의 배치의 조건으로 가능한 girth의 충돌을 작게 할 것이다. PEG 알고리즘을 이용한 그래프는 edge-by-edge방법으로 성장한다. 따라서 최종적인 Tanner 그래프는 PEG Tanner 그래프를 나타낸다. 그 기초적인 idea는 가장 먼 거리의 체크 노드를 찾는 것과 그리고 나서 심볼 노드와 가장 먼 거리에 있는 체크 노드를 연결하여 새로운 모서리를 배치하는 것이다. 심볼 노드 s_j로부터 부그래프의 연결선이 확정되기 전까지는 확장될 때 마다 2가지 상황이 발생할 수 있다.

1) $N_{s_j}^{l}$의 집합원의 개수는 성장을 멈춘다. 하지만, m 보다는 작다.

2) $\overline{N}_{s_j}^{l} \neq \varnothing$, 하지만 $\overline{N}_{s_j}^{l+1} = \varnothing$ 이다.

1) 의 경우, 모든 체크 노드들이 s_j로부터 닿지는 않는다. 그래서 PEG알고리즘은 닿지 않는 것 하나를 선택한다. 그러므로 어떤 추가적인 cycle도 만들어 지지 않는다. 이것은 종종 그래프 구성의 초기 단계에서 일어난다. 2) 의 경우, 모든 체크 노드들이 s_j에 닿아있다. 그리고 그 알고리즘은 하나의 모서리가 자리를 잡게 됨으로써 만들어지는 cycle이 가장 큰 가능성의 길이 $2(l+2)$이기 위해 깊이 $l+1$이라 말한 s_j로부터 가장 먼 위치에 있는 것 하나를 선택한다.

PEG 알고리즘을 다음과 같이 요약했다.[6]

Generic Progressive Edge-Growth Algorithm:
for $j = 0$ to $n-1$ **do**
begin
  for $k = 0$ to $d_{s_j} - 1$ **do**
  begin
    if $k = 0$
    $E_{s_j}^{0} \longleftarrow$ edge (c_i, s_j), where $E_{s_j}^{0}$ denotes the first edge incident to s_j, and c_i is a check node having the lowest check degree under the current graph setting $E_{s_0} \cup E_{s_1} \cup \cdots \cup E_{s_{j-1}}$.
    else
    expanding a tree from symbol node s_j up to depth l under the current graph setting such that $\mathcal{N}_{s_j}^{l} \neq \varnothing$ but $\mathcal{N}_{s_j}^{l+1} = \varnothing$, or the cardinality of $\mathcal{N}_{s_j}^{l}$ stops increasing but is less than m, then $E_{s_j}^{k} \longleftarrow$ edge (c_i, s_j), where $E_{s_j}^{k}$ is the k-th edge incident to s_j and c_i is one check node picked from the set $\overline{\mathcal{N}}_{s_j}^{l}$ having the lowest check-node degree.
  end
end

집합 $N_{s_j}^{l}$ 와 그것의 여집합 $\overline{N}_{s_j}^{l}$은 반복적 방법을 통해 효과적으로 얻을 수 있다. 한 가지 방법으로는 체크 노드들에 집합 {0, 1}의 원소 값들을 수용하여 각각의 체크 노드 c_i를 위한 척도 I_{c_i}를 정하는 것이다. 그 척

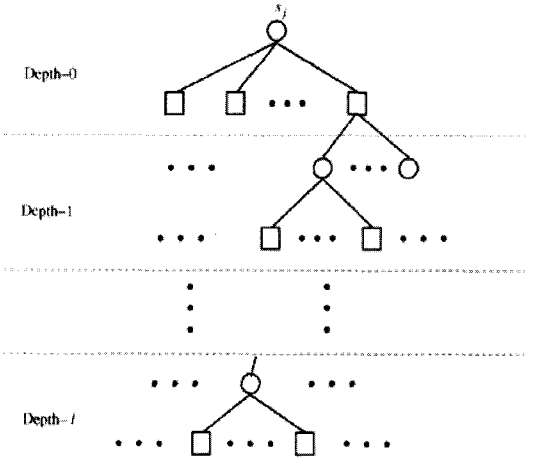


그림 2. 심볼 노드 깊이 l까지 s_j로부터 확장된 부그래프

Fig. 2. a subgraph spreading from symbol node s_j.

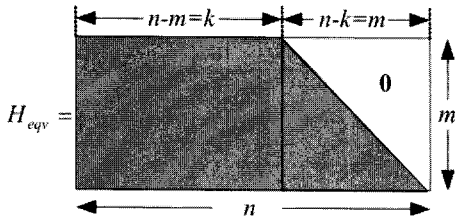
도 집합 I 는 0으로 초기화된다. s_j에서 시작한 트리는 깊이 l 까지 진행함으로서 spanning tree 안에 모든 체크 노드들의 척도를 '$N_{s_j}^{l}$에 속한다.'라는 것을 나타내기 위해 1 로 세팅한다. 마찬가지로, $\overline{N}_{s_j}^{l}$는 척도 집합 I_{c_i}가 1인지 0인지를 검사함으로써 얻을 수 있다. 이 단순한 방법이 절대적으로 가장 효과적인 것은 아니다. 하지만 그럼에도 불구하고, 실질적인 PEG Tanner 그래프 코드들을 구성할 때 충분히 좋은 성능을 나타내고 있다.

2. 제안한 PEG 알고리즘 구조

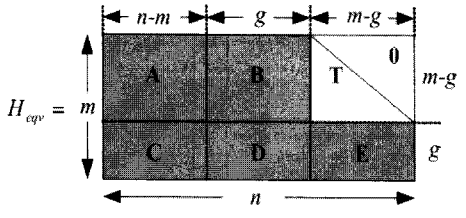
가. 효율적인 LDPC 부호화기 구조

일반적으로 Tanner 그래프에 대해서 BP와 SPA를 사용하여 반복 복호를 하는 경우 블록 당 계산 복잡도는 블록의 길의 n에 대해서 선형적으로 증가하게 되어진다. 하지만, 부호화의 경우 블록 당 복잡도는 n^2으로 증가한다. 그리하여 대부분의 LDPC 부호는 효율적인 부호화에 초점을 맞추고 LDPC Tanner 그래프를 구성하게 된다.

그 중 그림 3과 같이 LDPC 부호화기의 구조를 하삼각 구조를 가진 패리티 체크 행렬 구조 설계하기도 하며 또는 Richardson 구조를 설계하기도 한다.



(a) 하삼각 구조의 패리티 체크 행렬
(a) lower triangular parity check martix.



(b) 리차드슨 구조의 패리티 체크 행렬
(b) parity check marix of a Richardson.

그림 3. LDPC 부호화기 구조
Fig. 3. LDPC encoder construction.

나. M-PEG알고리즘

linear-time 부호화 원리에 따르면 코드워드 c는 $c=[d,\ p]$으로 패리티 체크 행렬 H는 $H=[H^d, H^p]$로 나누어진다. 다음 식을 만족한다.

$$[H^d, H^p]c^T = 0 \tag{1}$$

위 식의 $H^p=\{h_{i,j}^p\}$는 $m\times m$로 구성되고, 다음 형태를 갖는다.

$$H^p = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ h_{2,1}^p & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ h_{m,1}^p & \cdots & h_{m,m-1}^p & 1 \end{pmatrix} \tag{2}$$

본 논문에서는 PEG 알고리즘에서 열을 구성하여 패리티 체크 행렬을 구성하는 것이 아닌 행을 구성하여 패리티 체크 행렬 H 를 구성하였다. 여기서 우리는 (3, 6)LDPC Tanner 그래프를 구성한다.

IEEE 802.16e에 제안된 많은 LDPC 부호는 dual-diagonal 형태의 행렬 구조나 혹은 그와 유사한 형태의 행렬 구조를 가지고 있다. 패리티 검사 행렬에서 패리티에 해당하는 부분이 dual-diagonal 형태가 되면 간단한 부호화 기법을 사용하여 부호화를 할 수 있다는 장점이 있으므로 본 논문에서는 dual-diagonal 형태의 패리티 체크 행렬 H를 구성한다.[8]

$$H_{dual-diagonal} = \begin{bmatrix} 1 & & & & & \\ 1 & 1 & & & 0 & \\ & 1 & 1 & & & \\ & & \ddots & & & \\ & & & 1 & 1 & \\ & 0 & & & 1 & 1 \\ & & & & & 1 \end{bmatrix} \tag{3}$$

또한 daul-diagonal 행렬은 매우 효과적인 부호화기의 설계를 가능하게 하다. 패리티 검사 행렬에 대응하는 생성 행렬 G는 다음과 같이 주어진다.

$$G = [I \quad H_1^T H_2^{-T}] \tag{4}$$

H_2의 inverse transpose 행렬은 다음과 같이 상삼각 구조로 되어있다.

$$H_2^{-T} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ & 1 & \cdots & \vdots \\ & & \ddots & 1 \\ & & & 1 \end{bmatrix} \tag{5}$$

이것은 변환 함수가 $1/1\oplus D$인 차등 부호화기에 대응된다. 따라서 그림 7과 같은 구조로 부호화기를 사용할 수 있다.

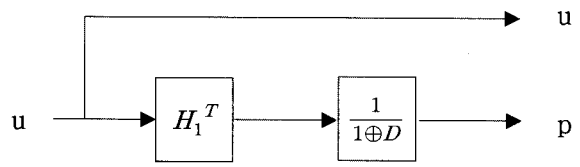


그림 4. dual-diagonal 행렬을 이용한 차등 부호화기
Fig. 4. A dual-diagonal matrix using different encoder.

다음 알고리즘을 수행하기 위해 필요한 파라미터로 체크노드 D_c의 차수열이 필요하다. 또한 패리티 체크 행렬의 크기 n과 m이 필요하다. 알고리즘을 통해 행의 위치 정보를 가진 형태의 결과 값이 나온다. 다음은 dual- diagonal 형태를 갖는 M-PEG알고리즘을 다음같이 요약하였다.

for(i = 0 to m-1){
  for(k = 0 to $d_{c_i} - 1$){
    if(k = 0){
      $E_{c_i}^0 \leftarrow$ 연결선(c_i, s_j), $E_{c_i}^0$는 c_i에 부속되는 첫 번째 연결선이다. 이것은 행렬 H^p의 dual-diagonal에 있는 "1"에 대응하는 연결선이다.
    } // if end
    else{
      $\overline{N}_{c_i}^l \neq \varnothing$ 하지만 $\overline{N}_{c_i}^{l+1} = \varnothing$ 또는 $N_{c_i}^l$의 개수가 증가하지 않는다는 조건으로 구성되어 있는 현재의 그래프에 체크 노드 c_i로부터 깊이 l까지 부그래프를 확장한다. $E_{c_i}^k \leftarrow$ 연결선 (c_i, s_j)한다. 여기서 $E_{c_i}^k$는
      c_i에 k 번째로 부속되어지는 연결선이다. s_j는 $\overline{N}_{c_i}^l$에서 가장 차수가 낮은 것으로 고른다.
    } // end else
  } // for end
} // for end

Ⅲ. 실 험

우리는 $d_s = 3$, $d_c = 6$인 길이 1024의 부호율 0.5 균일 Proposed PEG LDPC 부호와 같은 파라미터를 갖는 Mackay의 랜덤 LDPC 부호, PEG부호를 비교하였다. 표 1 cycle 분포를 나타내고 있는데 Proposed PEG LDPC 부호의 girth가 두 길이에서 10으로 Mackay 부

표 1. 부호율 0.5 균일 LDPC 부호의 cycle 분포
Table 1. a cycle LDPC for code rate 0.5 regualr LDPC code.

length	code	4-cycle	6-cycle	8-cycle	10-cycle
1024	Mackay	0	544	457	1
	PEG	0	0	79	945
	Proposed PEG	0	0	120	904

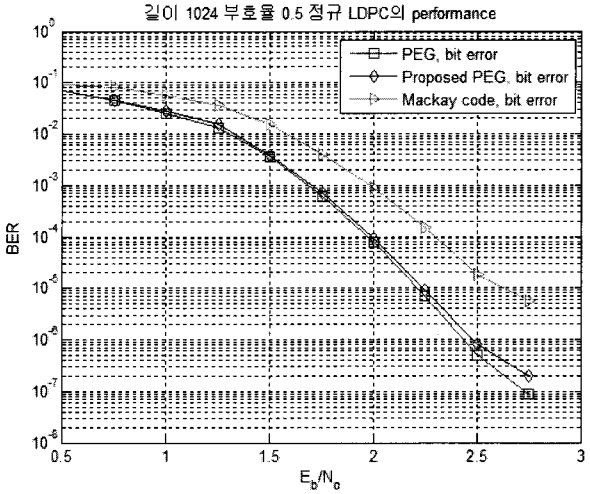


그림 5. 부호율 0.5 길이 1024 균일 LDPC 부호 성능
Fig. 5. the regular LDPC in code rate 0.5 and length 1024.

호[3]보다 높고 PEG 부호와 비슷함을 알 수 있다.

그림 5는 부호율 0.5인 균일 LDPC 부호의 성능을 비교한 결과이다 Proposed LDPC 부호의 성능은 높은 SNR에서 Mackay 부호보다 좋고 PEG부호와 거의 비슷한 결과를 보여준다. 하지만, 부호화기에서 요구되어지는 계산량과 저장 공간이 줄어든다. 왜냐하면 패리티 체크 행렬은 dual-diagonal로 구성되어졌고, 또한 H는 여전히 sparse한 성질을 지녔기 때문이다.

Ⅳ. 결 론

본 논문에서는 변환된 PEG알고리즘을 통해 기존 LDPC 구조를 구성하고 PEG 알고리즘을 LDPC Tanner 그래프의 국부 girth를 최대로 하여 LDPC 패리티 체크 매트릭스 구성을 제안하였다. 이것은 임의의 패리티 체크 H를 구성하면서도 girth를 크게 함으로써 LDPC 성능을 향상 시킬 수 있다는 것이 장점이다. 또한 효율적 부호화기인 dual-diagonal 형태의 행렬을 변형된 PEG 알고리즘을 통해 쉽게 구성할 수 있다.

앞으로 좀 더 낳은 알고리즘과 구성을 위해 Tanner 그래프의 연구가 더 필요하다.

참 고 문 헌

[1] A. John, R. Peter, "*Electric Communication Development,*" Communications of the ACM, 40, pp. 71-79, May 1997.
[2] D. J. C. MacKay, R. N. Neal, "*Near Shannon limit pergormance of low-density parity-check*

codes," Electron. Lett,. vol. 33, pp. 457-458, Mar. 1997.

[3] 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.

[4] R. M. Tanner, *"A Recursive Approach to Low Complexity Codes", IEEE Trans. Inf. Theory*, vol. IT-27, no. 6, pp. 533-547, Sep. 1981.

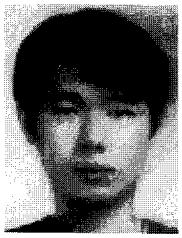
[5] R. G. Gallger, *"Low-density parity-check codes," IRE Trans. Inform. Theory,* vol. IT-8, pp. 21-28, Jan. 1962.

[6] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, *"Progressive edge-growth Tanner graphs", in Proc. IEEE Global Telecommunications Conf. (GLOBECOM),* San Antonio, TX, Nov. 2001. CD Proceedings, paper no. 0-7803-7208-5/01.

[7] 강충구, 김일환, *"IEEE 802.16e 계열 Wireless MAN 표준 기술", TELECOMMUNICATION REVIEW*, pp 149-182, 2003.

[8] 김준성, 배슬기, 정비웅, 송홍엽, *"IEEE 802.16e의 LDPC 부호화 기술 분석," 텔레콤,* 제 20권, 제 2 호. 2004. 12.

저 자 소 개



김 성 훈(학생회원)
2006년 전북대학교 전자정보 공학부 학사 졸업.
2008년 전북대학교 전자정보 공학부 석사
<주관심분야 : 이동통신, 정보이론>

이 문 호(정회원)
1967년 전북대학교 전자공학과 학사
1984년 전남대학교 전기공학과 박사
1990년 동경대학교 정보통신 공학과 박사
1984년~1985년 미국 미네소타대 전기과 포스트 닥터
1980년 10월~현재 전북대학교 전자정보공학부 교수
<주관심분야 : 이동통신, 정보이론, UWB>