

## Gallager 코드의 Stopping Set 분석

류정민, 박상준, 이흥노\*  
광주과학기술원 정보통신공학부

jmryu@gist.ac.kr, sjpark1@gist.ac.kr \*heungno@gist.ac.kr

## Stopping set analysis for Gallager Codes

Jeong-Min Ryu, Sangjun Park, Heung-No Lee\*  
Gwangju Institute of Science and Technology  
School of Information and Communications

## 요약

본 논문은 Stopping Set 분석을 통하여 BEC(Bit Erasure Channel)에서의 Gallager LDPC 코드에 대한 성능을 분석하는 방법을 고안하였고, 짧은 LDPC 코드의 복호 실패 확률이 부호화 방법에 따라 서로 다른 곡선에 수렴할 수 있음을 보였다. 또한 Gallager 패리티 체크 행렬보다 더 좋은 성능을 보일 수 있는 패리티 체크 행렬이 존재함을 보였다.

## I. 서론

Regular LDPC(Low-Density Parity Check) 코드[1]는 길이(Block Length)  $n$  와 변수 노드 차수(Degree)  $l$  그리고 체크 노드 차수  $r$  에 의해 대략적인 Tanner Graph[2] 또는 패리티 체크 행렬의 형태가 결정된다. 이때,  $n$  과  $l, r$  에 의해 생성될 수 있는 LDPC 패리티 체크 행렬의 집합을 앙상블(Ensemble)  $C(n, x^{l-1}, x^{r-1})$  이라 정의하자.

[3]은 앙상블  $C(n, x^{l-1}, x^{r-1})$  의 각각의 패리티 체크행렬에 의해 부호화된 LDPC 메시지가 BEC(Bit Erasure Channel)를 통해 전송되고 반복 알고리즘(Iterative Algorithm, [4])에 의해 복호될 때, 모든 복호 실패 확률을 평균한 값이  $n$  이 커짐에 따라 하나의 LDPC 코드의 복호 실패 확률에 수렴하는 것을 보여주었으며, 그 앙상블 평균값을 LDPC 코드의 대략적인 성능 분석의 지표로 이용하였다.

본 논문에서는 Gallager 코드[1]의 분석 방법을 제안하였고 Gallager 코드 보다 더 좋은 성능을 보이는 패리티 체크 행렬이 존재함을 보였다. 또한 짧은 Gallager 코드의 복호 실패 확률에 대한 앙상블 평균값이 모든 LDPC 코드에 대한 앙상블 평균값과 다르다는 것을 보임으로써, 짧은 LDPC 코드는 부호화 방법에 따라 복호 실패 확률이 서로 다른 곡선에 수렴할 수 있음을 보였다.

## II. 본론

하나의 LDPC 패리티 체크 행렬  $H$  에 의해 부호화된 메시지가 BEC 를 통해 전송될 때 메시지 중 몇 개의 비트들은 BEC 의 Erasure 확률에 따라 지워지며, 이는 수신부의 복호기에서 반복 알고리즘에 의해 어느 정도 복호될 수 있다. 이때, 지워진 비트의 위치에 대응되는

패리티 체크 행렬의 열의 형태에 따라 복호 가능성 여부가 결정된다. [3]에서는 반복 알고리즘으로 복호 불가능한 비트들을 패리티 체크 행렬의 Tanner Graph 측면에서 다음과 같이 Stopping Set 이라 정의하였다.

**정의 1[Stopping Set]:** Stopping set  $S$  는 변수 노드 집합  $V$  의 부분집합이며,  $S$  의 모든 이웃은  $S$  에 두 번 이상 연결되어 있다.

본 논문에서는 Gallager 코드의 Tanner Graph 에서 이러한 Stopping Set 의 존재 확률을 구함으로써, Gallager Code 의 복호 실패 확률을 얻고자 한다.

우선 길이  $n$ , 변수 노드 차수  $l$ , 체크 노드 차수  $r$  에 대한 모든 생성 가능한 Gallager LDPC 패리티 체크 행렬의 집합을 앙상블  $C_G(n, x^{l-1}, x^{r-1})$  이라 정의하자. 여기서  $C_G(n, x^{l-1}, x^{r-1})$  는  $C(n, x^{l-1}, x^{r-1})$  의 부분집합이다. 이때 앙상블  $C_G(n, x^{l-1}, x^{r-1})$  에 대한 패리티 체크 행렬  $H$  를 생성하기 위한 부분 행렬  $\hat{H}$  를  $\hat{H} = [I, I, \dots, I]^T$  라 정의하자. 여기서  $I$  는 크기  $l \times l$  의 항등행렬이다. Gallager 코드의 패리티 체크 행렬  $H_G$  는  $l$  개의 임의의 순열 행렬  $\{\pi_i | i=1, 2, \dots, l\}$  와  $\hat{H}$  에 의해  $H_G = [\pi_1(\hat{H}), \pi_2(\hat{H}), \dots, \pi_l(\hat{H})]^T$  로 정의된다.

본 논문에서는 Gallager 코드의 한 변수 노드가 생성할 수 있는 Tanner graph 의 Constellation 을

$$C_{fGC}(l) = \prod_{k=1}^l \left( \sum_{m=n^{-(k-1)/r+1}}^{n-k/r} x_m \right) \quad (1)$$

로 정의한다. 여기서  $(x_1, x_2, \dots, x_c)$  는 체크 노드의

변수이다. 그리고  $n$  개의 변수 노드가 생성할 수 있는 Tanner graph 의 경우의 수를 다음과 같이 정의 한다.

$$T_{GC}(e, l, c, r) = \text{coefs}(C_{GC}(l))^c |n_i \in \{0, 1, \dots, r\}, \forall i \in \{1, 2, \dots, c\}|. \quad (2)$$

여기서  $c$  개의 변수로 구성된 다항식  $f(x_1, x_2, \dots, x_c)$  에 대한  $\text{coefs}(f(x_1, x_2, \dots, x_c))$  표현은  $f(x_1, x_2, \dots, x_c)$  의 모든 계수의 합으로 정의한다.

그리고 양상블  $C_G(n, x^{l-1}, x^{r-1})$  에서 Stopping Set 을 포함하고 있는 모든 Tanner graph 의 경우의 수  $S_{GC}(e, l, c)$  를 다음과 같은 함수들을 이용하여 정의한다.

$$H_{GC}(l) = X_1^{n/r} \otimes X_2^{2n/r} \otimes \dots \otimes X_n^{n(l-1)/r+1}, \quad (3)$$

$$U_{GC}(n, t, l, c) = [V_{GC}(t, l, c) \otimes M(H_{GC}(l)^{\otimes(n-t)})] |p_j \in \{0, 1\}, \forall j| \quad (4)$$

$$V_{GC}(n, l, c) = M([M^{-1}(U_{GC}(n, 0, l, c)) |n_i \neq 1, \forall i \in \{1, 2, \dots, c\}| \bigcup_{t=4}^{n-1} U_{GC}(n, t, l, c)], \quad (5)$$

$$N_{GC}(n, l, c) = \sum_m [(M^{-1}(U_{GC}(n, 0, l, c)) \bigcup_{t=4}^n U_{GC}(n, t, l, c)) |n_i \in \{0, 1, \dots, r\}, \forall i \in \{1, 2, \dots, c\}]_m, \quad (6)$$

$$S_{GC}(e, l, c) = T_{GC}(e, l, n \frac{l}{r}, r) - \text{coefs}(N_{GC}(e, l, c)) \quad (7)$$

여기서 초기값은  $S_{GC}(0, l, c) = 1, N_{GC}(0, l, c) = 1$ . 이다.

식 (1)-(7)로부터, BEC 의 Erasure 확률이  $\varepsilon$  일 때 Gallager 코드의 복호 실패 확률  $P_B^{IT}(\varepsilon)$  에 대한 평균은 다음과 같이 구할 수 있다.

$$E_{C_G(n, x^{l-1}, x^{r-1})}[P_B^{IT}(\varepsilon)] = \sum_{e=2}^{n/l/r-(l-1)} \binom{n}{e} \varepsilon^e (\bar{\varepsilon})^{n-e} \left( \frac{S_{GC}(e, l, c)}{T_{GC}(e, l, n \frac{l}{r}, r)} \right) + \sum_{e=n/l/r-(l-2)}^n \binom{n}{e} \varepsilon^e (\bar{\varepsilon})^{n-e}. \quad (8)$$

식 (1)-(7)에서 서술된 표기와 정의는 표 1에 정리되어 있다.

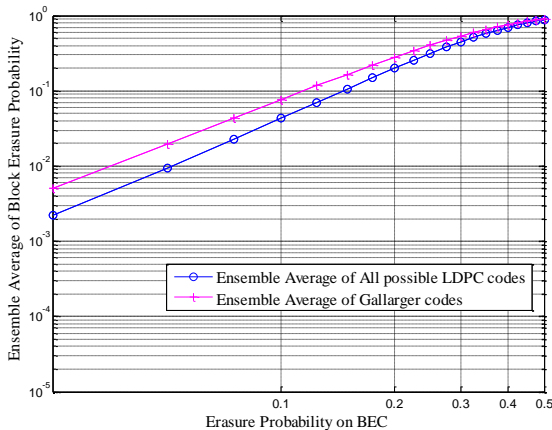


그림 1. LDPC 코드 길이가 12 일 때,  $C_G(n, x^{l-1}, x^{r-1})$  와  $C(n, x^{l-1}, x^{r-1})$  에 대한 복호 실패 확률의 양상블 평균 비교.

표 1. 식 (1)-(7)에서 서술된 표기와 정의

표기	정의
$X_i^j$	벡터 $X = [x_1, x_2, \dots, x_n]$ 와 $1 \leq i, j \leq c$ 에 대해 $[x_i, x_{i+1}, \dots, x_j]$ 로 정의한다
$U \otimes V$	크기가 $m \times n$ 인 행렬 $U$ 와 크기가 $p \times q$ 인 행렬 $V$ 에 대하여 $U \otimes V$ 는 $U \otimes V = \begin{bmatrix} u_{11}V & \dots & u_{1n}V \\ \vdots & \ddots & \vdots \\ u_{m1}V & \dots & u_{mn}V \end{bmatrix},$ 이며 크기는 $mp \times nq$ 이다. 그리고 Kronecker 제곱 $U^{\otimes n}$ 는 $n \geq 1$ 에 대하여 $U^{\otimes n} = U \otimes U^{\otimes(n-1)}$ ( $U^{\otimes 0} = 1$ )이다.
$[X Condition]$	조건(Condition)을 만족하는 벡터 $X$ 의 원소들의 집합을 벡터로 다시 변환한 $X$ 의 부분 벡터이다. 예를 들면, 벡터 $X = [-1, -5, 6]$ 에 대하여 $[x_i   x_i > 0 \forall i = 1, 2, 3]$ 는 $[6]$ 이다.
$\bar{U}X = [U_i \{x_i\}]$	$X$ 벡터의 원소에 대한 합집합을 순서 고려 없이 벡터로 다시 변환한 값으로 정의한다. 예를 들면, $\bar{U}[1, 1.5, 3, 3]$ 은 $[1, 3, 5]$ 이다.
$B \setminus A$	여집합 표현과 같이 $B \setminus A := [x \in B   x \notin A]$ 로 정의한다. 예를 들면, $[1, 2, 5] \setminus [1, 2]$ 은 $[5]$ 이다.
$M: X \rightarrow Y$	사상함수 $M: X \rightarrow Y$ 는 $X = H_{GC}(l)$ 와 $Y = \{y_j   j \in \{1, 2, \dots, c\}\}$ 에 대해 일대일 대응관계를 갖는 함수이다.
$p_j$	$p_j$ 는 $j \in \{1, 2, \dots, c\}$ 에 대한 $y_j$ 의 차수(Order)이다.

### III. 결론

Gallager 코드에 대한 양상블 평균 식 (8)을 구하여 그림 1에 나타내었다. 그림 1에서 볼 수 있듯이  $C_G(n, x^{l-1}, x^{r-1})$  에 대한 양상블 평균값과  $C(n, x^{l-1}, x^{r-1})$  에 대한 양상블 평균값[3]이 BEC 의 Erasure 확률이 감소함에 따라 차이가 더 증가하는 것을 볼 수 있다. 결과적으로 Gallager 부호화 방법보다 더 좋은 성능을 보일 수 있는 LDPC 의 패리티 체크 행렬이 존재함을 알 수 있고, 짧은 길이의 LDPC 코드는 부호화 방법에 따라서 다른 곡선에 수렴하는 것을 알 수 있다.

### ACKNOWLEDGMENT

이 논문은 2012년도 정부 (교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (중견연구자-핵심연구사업, NO. 2012-047744)

### 참고 문헌

- [1] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: M.I.T. Press, 1963.
- [2] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, no. 5, pp. 533- 547, Sep. 1981.
- [3] C. Di, D. Proietti, I.E. Telatar, T.J. Richardson, and R.L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel", *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1570-1579, Jun. 2002.
- [4] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599- 618, Feb. 2001.