

# 낮은 복잡도의 CRC-polar 연접 부호 신뢰 전파 복호 기법

백성열, 고영준, 김서영, 오왕록

충남대학교

[syback@o.cnu.ac.kr](mailto:syback@o.cnu.ac.kr), [koy565900@o.cnu.ac.kr](mailto:koy565900@o.cnu.ac.kr), [sky2622@o.cnu.ac.kr](mailto:sky2622@o.cnu.ac.kr), [kingrock@cnu.ac.kr](mailto:kingrock@cnu.ac.kr)

## Low Complexity of Belief Propagation Decoding Scheme for Concatenated CRC-Polar Codes

Sungyeol Back, Youngjun Ko, Seoyoung Kim and Wangrok Oh

Chungnam National Univ.

### 요약

CRC-polar 연접 부호의 BP 복호 기법은 CRC 팩터 그래프 (CRC factor graph, C-FG) 내의 short cycle로 인해 성능 열화가 발생한다. 이를 완화하기 위해 MaxLLR 기법이 제안되었으나 해당 기법은 CRC 생성에 모든 정보 비트를 사용하여 C-FG를 구현하는데 요구되는 복잡도가 높다. 본 논문에서는 CRC 생성에 사용되는 정보 비트를 선별하여 낮은 복잡도의 CRC-polar 연접 부호 BP 복호 기법을 제안한다. 제안하는 기법은 CRC-polar 연접 팩터 그래프를 간소화하여 구현 복잡도를 낮추고 복호 성능을 개선할 수 있다.

### I. 서론

극 부호 (polar code) [1]는 BI-DMC (binary input discrete memoryless channel)에서 채널 용량 (channel capacity)을 달성할 수 있다고 이론적으로 증명된 최초의 오류 정정 부호이며 대표적인 복호 기법으로는 SC (successive cancellation) [1]와 BP (belief propagation) [2]가 있다. BP 복호기는 반복 복호를 수행하여 SC와 비교했을 때 복호 복잡도가 높은 단점이 있다. 이를 완화하기 위해 외부 부호 (outer code)로 CRC (cyclic redundancy check)를 사용하여 조기 종료 판별에 활용하는 CA-ESBP (CRC aided early stopping belief propagation) [3]가 제안되었으나 CRC를 조기 종료 판별 용도로만 사용하고 SC 대비 성능 열화가 여전히 크다.

CRC를 조기 종료 판별 이외에 용도로도 사용하고자 CRC-polar 연접 부호 (concatenated CRC-polar code)의 복호 기법들에 대해 다양한 연구가 수행되었다. [4]에서는 CRC 팩터 그래프 (CRC factor graph, C-FG) 와 극 부호 팩터 그래프 (polar factor graph, P-FG)를 연접한 상태에서 메시지 전달 알고리즘 (message passing algorithm)을 수행하는 기법이 제안되었다. 해당 기법은 C-FG 내에서 short cycle로 인해 성능 열화가 발생한다. 이를 완화하고자 [5]에서는 C-FG의 variable node가 check node들로부터 전달되는 메시지 중 가장 신뢰도가 높은 메시지를 선택하는 MaxLLR 기법이 제안되었다. 그러나 해당 기법에서는 CRC 생성에 모든 정보 비트를 사용하여 C-FG를 구성하는데 구현 복잡도가 높다. 본 논문에서는 CRC 생성에 사용되는 정보 비트들을 선별하는 기준을 제시하여 낮은 복잡도의 CRC-polar 연접 부호 BP 복호 기법을 제안한다. 제안하는 기법은 C-FG의 구현 복잡도를 낮추고 MaxLLR 기법 대비 복호 성능이 우수하다.

### II. 본론

부호율  $\frac{K}{N}$ 인 CRC-polar 연접 부호의 codeword)  
 $\mathbf{x} = [x_0, x_1, \dots, x_{N-1}]$ 는 식 (1)과 같이 메시지 벡터

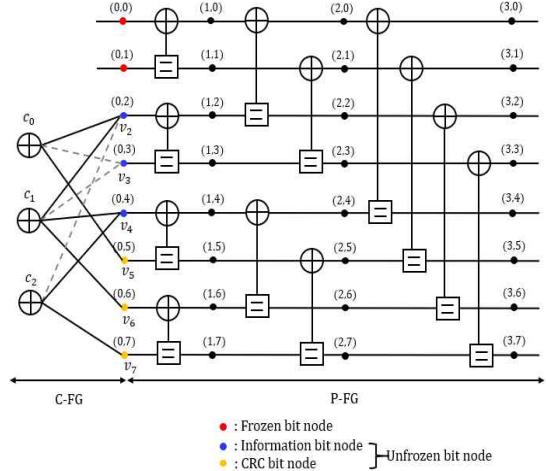


그림 1. CRC-polar 연접 부호의 팩터 그래프.

$\mathbf{u} = [u_0, u_1, \dots, u_{N-1}]$ 와 생성 행렬  $G_N$ 을 통해 생성된다 [1].

$$\mathbf{x} = \mathbf{u}G_N. \quad (1)$$

이때  $\mathbf{u}$ 의 원소에는  $K$ 개의 비고정 비트 (unfrozen bit)와  $N-K$ 개의 고정 비트 (frozen bit)가 극 부호를 설계할 때 결정된 위치에 따라 매핑되고 비고정 비트들은  $K_{\text{CRC}}$ 개의 CRC 비트와  $K_{\text{info}}$ 개의 정보 비트로 구성된다. 부호어  $\mathbf{x}$ 는 BPSK (binary phase shifkeying) 심볼로 변조되어 AWGN (additive white Gaussian noise) 채널을 통과한다. 이때 AWGN 채널은 평균과 분산이 각각  $0, \frac{N_0}{2}$ 인 가우시안 분포 특성을 갖는다. 수신기는 수신된 신호 샘플에서 부호 비트들의 로그 우도 비 (log-likelihood ratio, LLR)를 계산하여 복호기의 입력값으로 사용한다.

그림 1은  $N=8$ ,  $K_{\text{info}}=3$ ,  $K_{\text{CRC}}=3$ 인 CRC-polar 연접 부호의 BP 복호기 팩터 그래프를 나타낸다. 여기서  $(l, k)$ 는  $l \in \{0, 1, \dots, \log_2 N\}$  번째 단계에서  $k \in \{0, 1, \dots, N-1\}$  번째 노드를 나타내고 CRC 생성 단항

표 1. 전산 실험 파라미터

Parameters	Values
Channel model	AWGN
Polar code length $N$	512
Code rate $R$	1/2
CRC generator polynomial	$x^{24} + x^{23} + x^{21} + x^{20} + x^{17}$ $+ x^{15} + x^{13} + x^{12} + x^8 + x^4$ $+ x^3 + x^2 + x + 1$
CRC code length	24
CRC position	Tail
Polar code design scheme	$\beta$ -expansion [7] ( $\beta = 2^{1/4}$ )
Modulation	BPSK
Maximum iteration number	100
$I_{\max}$	
Decoding scheme	CA-ESBP

식은  $x^3 + x + 1$ 이며 CRC 비트들은  $(0, 6), (0, 7), (0, 8)$ 에 매핑된다고 가정하였다. 해당 복호기는 P-FG에서 먼저  $\log_2 N$  번째 단계부터 0 번째 단계까지 왼쪽 방향 메시지 업데이트를 수행하고 C-FG 내에서 메시지 업데이트를 수행한다. 이후 C-FG에서 계산된 메시지는 P-FG의 비교정 비트 노드들로 입력되고 P-FG에서 0 번째 단계에서  $\log_2 N$  번째 단계까지 우측 방향 메시지 업데이트를 수행하며 이러한 과정은 매 반복 복호마다 수행된다. BP 복호기는 미리 설정된  $I_{\max}$  만큼 반복 복호를 수행하고 최종적으로 메시지 비트들을 경판정한 후 이 중 정보 비트들을 추정한다.

BP 복호기는  $I_{\max}$ 에 비례하여 복호에 요구되는 복잡도가 높은 문제가 있다. 이러한 문제를 완화하기 위해 매 반복 복호마다 CRC 검사를 수행하여 통과 시 복호를 종료하는 기법을 적용하거나 경판정된 메시지 비트들을 재부호화한 결과와 경판정된 부호 비트들을 비교하는 G-matrix 기반 조기 종료 판별 기법 [6]을 사용할 수 있다. 본 논문에서는 CRC와 G-matrix를 동시에 사용하여 조기 종료 판별 여부를 결정한다.

C-FG에서 발생하는 short cycle 영향을 완화하기 위해 MaxLLR 기법이 제안되었으나 CRC 생성 시 모든 정보 비트들을 사용하여 C-FG를 구성하는데 구현 복잡도가 높다. 본 논문에서는 CRC-polar 연결 팩터 그래프 구성 시 CRC 생성에 사용되는 정보 비트들을 선별하는 기준을 제안한다. P-FG에는 다양한 길이를 갖는 서브 극 부호의 팩터 그래프가 존재하며 이 중 최대한 2의승수 길이를 갖도록 부호율 1인 서브 극 부호 팩터 그래프 (sub-polar factor graph, SP-FG)를 구성할 수 있다. 각 부호율이 1인 SP-FG에서 첫 번째 비교정비트의 인덱스를 선별하여 임계 집합 (critical set)을 구성할 수 있다. 제안하는 기법은 임계 집합에 포함된 인덱스에 해당하는 정보 비트 노드들을 이용하여 CRC를 생성하여 CRC-polar 연결 팩터 그래프 구조를 구성하며 그림 1의 실선과 같이 메시지 업데이트를 수행한다. 이때 CRC 생성에 사용되는 정보 비트 노드는  $(0, 2), (0, 4)$ 에 해당한다. 이를 통해 C-FG를 구성하는데 필요한 variable node의 개수가 줄어들 뿐만 아니라 C-FG에서 수행되는 메시지 업데이트 횟수를 줄일 수 있다.

### III. 전산 실험

제안하는 기법의 성능을 확인하기 위해 전산 실험에 사용된 파라미터들은 표 1과 같다. 표 1에서  $I_{\max}$ 은 더 이상 성능 개선이 없는 100으로 설정하였다. 그림 3은 제안하는 기법의 BER과 FER 성능을 나타낸 것이다. 이 때 제안하는 기법과 성능을 비교하기 위해 MaxLLR 기법의 성능을 같이

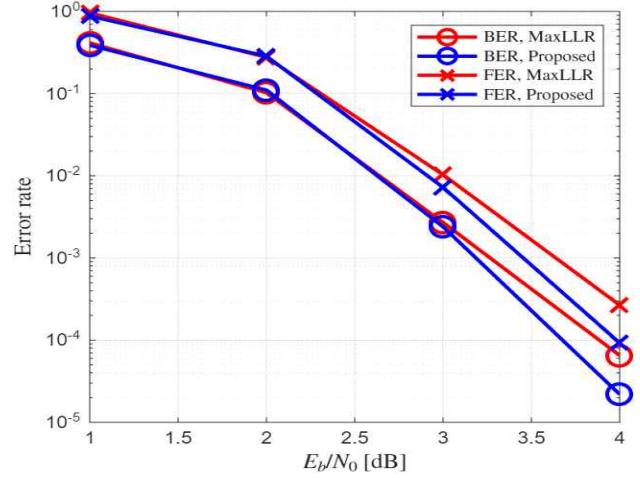


그림 2. 제안하는 기법의 오율 성능.

나타내었다. 그림 3에서 볼 수 있듯이 제안하는 기법은 MaxLLR 기법 대비 우수한 오율 (error rate)을 달성할 수 있다. 또한, 제안하는 기법은 C-FG에서 메시지 업데이트에 요구되는 복잡도를 동시에 낮출 수 있다.

### IV. 결론

본 논문에서는 임계 집합에 해당하는 정보 비트들을 통해 FG를 구성하여 낮은 복잡도의 CRC-polar 연결 부호 BP 복호 기법을 제안했다. 제안하는 기법은 MaxLLR 기법 대비 FG를 구성하는데 필요한 구현 복잡도를 낮출 수 있는 동시에 오율 성능이 우수하다.

### 참 고 문 헌

- [1] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," in *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051-3073, Jul. 2009.
- [2] Arikan, Erdal. "Polar codes: A pipelined implementation." Proc. 4th ISBC. Vol. 2010.
- [3] K. Niu and K. Chen, "CRC-Aided Decoding of Polar Codes," in *IEEE Communications Letters*, vol. 16, no. 10, pp. 1668-1671, October 2012.
- [4] M. Geiselhart, A. Elkelesh, M. Ebada, S. Cammerer and S. ten Brink, "CRC-Aided Belief Propagation List Decoding of Polar Codes," *2020 IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, CA, USA, 2020, pp. 395-400.
- [5] Hong, S. and Chung, J.-M. (2021), Improved CRC aided BP decoding for polar codes. *Electron. Lett.*, 57: 526-528.
- [6] B. Yuan and K. K. Parhi, "Early Stopping Criteria for Energy-Efficient Low-Latency Belief-Propagation Polar Code Decoders," in *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6496-6506, Dec. 15, 2014.
- [7] G. He et al., "Beta-Expansion: A Theoretical Framework for Fast and Recursive Construction of Polar Codes," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, 2017, pp. 1-6.