

순환중복확인 기반 극 부호를 위한 2 단계 코드 가중치 구 복호에 관한 연구

조유빈, 최건, 이남윤*
고려대학교, *포항공과대학교

gybin00@korea.ac.kr, simon03062@korea.ac.kr, *nylee@postech.ac.kr

Two-Stage Code-Weight Sphere Decoding for CRC-Aided Polar Codes

Yubeen Jo, Goen Choi, Namyoon Lee*
Korea Univ., *POSTECH

요 약

본 논문은 순환중복확인(cyclic redundancy check, CRC) 기반 극 부호(polar codes)를 위한 새로운 2 단계 근사 최대 우도(near-Maximum Likelihood, near-ML) 복호 기법을 제안한다. 제안하는 방식은 낮은 복잡도의 초기 복호기와 코드 가중치 구 복호(code-weight sphere decoding, WSD) 기술을 결합한다. 초기 복호 결과가 CRC 검증에 실패할 경우, WSD는 초기 추정치 주변의 낮은 가중치를 갖는 코드로 구성된 후보 구(sphere of candidates)를 탐색하여 반복적으로 코드를 개선한다. 이 접근 방식은 높은 신호 대 잡음비 환경에서 계산 복잡도를 크게 줄이면서도 근사 ML 성능을 유지한다. 시뮬레이션 결과는 다양한 부호 파라미터, 특히 낮은 부호율에서 우수한 성능을 보여준다.

I. 서 론

초고신뢰 저지연 통신(Ultra-Reliable Low-Latency Communications, URLLC) 환경에서는 짧은 블록 길이와 낮은 부호율을 갖는 효율적인 채널 부호 및 저복잡도 고성능 복호 알고리즘이 필수적이다 [1]. 기존 연구들은 유한 블록 길이에서의 성능 한계 분석 및 다양한 부호화 기법들을 제시했으나, 특히 낮은 부호율에서 복잡도와 성능을 모두 만족시키는 최대 우도(Maximum-Likelihood, ML) 복호기 개발은 여전히 중요한 과제이다. OSD [2], GRAND [3], SCL [4] 등과 같은 기존의 부최적(suboptimal) 복호 기법들은 대안으로 제시되었지만, 낮은 부호율에서의 근사 ML 성능과 최적화된 복잡도 달성은 여전히 난제이다.

본 논문은 이러한 문제를 해결하게 위해 짧은 블록 길이 및 낮은 부호율 부호에 특화된 새로운 2 단계 근사 ML 복호 방법을 제안한다. 1 단계에서는 저복잡도 초기 복호기로 유효 코드를 빠르게 찾고, 순환중복확인(Cyclic Redundancy Check, CRC) 검증 실패 시 2 단계 코드 가중치 구 복호 (Code-Weight Sphere Decoding, WSD)를 수행한다. WSD는 초기 추정 코드 주변에 낮은 가중치 코드를 이용하여 해밍 구(Hamming sphere)를 구성하고, 이 구 내에서 반복적인 지역 탐색을 통해 점진적으로 코드를 개선한다. 이 방식은 모든 선형 부호 및 초기 복호 방법에 적용 가능하며, 계산 효율성을 유지하면서 근사 ML 성능을 달성한다.

II. 본론

A. 채널 코딩 시스템

부호어 길이 N , 메시지 길이 K 를 갖는 이진 선형 블록 코드 $\mathcal{C}(N, K)$ 는 생성 행렬 $\mathbf{G} \in \mathbb{F}_2^{K \times N}$ 혹은 패리티 확인 행렬 $\mathbf{H} \in \mathbb{F}_2^{(N-K) \times N}$ 으로 정의된다. 부호어 $\mathbf{c} \in \mathbb{F}_2^N$ 는 $\mathbf{c} = \mathbf{m}\mathbf{G}$ 를 통해 생성되고, 이때, $\mathbf{m} \in \mathbb{F}_2^K$ 은 정보 비트 벡터이다. 변조 방식은 이진 위상 편이 변조 (BPSK)를 사용하며, $\mathbf{x}(\mathbf{c}) = \mathbf{1} - 2\mathbf{c}$ 이다. 변조된 심볼 벡터 \mathbf{x} 는 가산 백색 가우스 잡음 채널 (Additive White Gaussian Noise, AWGN)을 통과하며, 이 때, 수신기에서 수신된 신호 벡터는 $\mathbf{y} = \mathbf{x}(\mathbf{c}) + \mathbf{w}$ 이다. 이 때, $\mathbf{w} \in \mathbb{R}^N$ 분산 $\sigma^2 = N_0/$

2를 갖는 는 가산 가우시안 잡음이다. 본 논문에서는 여러 검출 능력 향상을 위해 CRC 코딩을 사용하였다. 기존 정보 벡터 \mathbf{c} 에 CRC 코딩을 적용한 새로운 정보 벡터를 \mathbf{v} 로 명명하고, \mathbf{v} 에 대한 생성 및 패리티 확인 행렬을 각각 \mathbf{G}_{crc} , \mathbf{H}_{crc} 로 정의한다.

B. 코드 가중치를 이용한 해밍 구 구성

선형 블록 코드에서, 코드 가중치의 특성을 이용하여 효율적으로 해밍 구를 구성할 수 있다. 임의의 부호어 $\mathbf{c} \in \mathcal{C}$ 와 해밍 거리 d_ℓ 만큼 떨어진 부호어의 집합 $\mathcal{C}_\ell(\mathbf{c})$ 를 다음과 같이 정의한다:

$$\mathcal{C}_\ell(\mathbf{c}) = \{\mathbf{c}' \in \mathcal{C} : d_H(\mathbf{c}, \mathbf{c}') = d_\ell\}. \quad (1)$$

이때, $d_H(\cdot, \cdot)$ 은 두 부호어 사이의 해밍 거리를 지칭하며, 또한, d_ℓ 은 코드 가중치 분포에서 ℓ 번째 작은 서로 다른 가중치를 의미한다.

코드 가중치 분포 집합이 $L+1$ 개의 오름 차순 ($d_0 = 0 < d_1 (=d_{\min}) < \dots < d_L$)으로 정렬된 서로 다른 요소로 구성되어 있다고 가정하면, 부호어 \mathbf{c} 를 중심으로 해밍 거리 d_1 에서 d_r ($r \leq L$)까지 해당 부호어 집합의 합집합인 해밍 구는 다음과 같이 정의 된다:

$$\mathcal{S}_r(\mathbf{c}) = \cup_{\ell=1}^r \mathcal{C}_\ell(\mathbf{c}). \quad (2)$$

추가적으로, 전체 부호어 집합 \mathcal{C} 는 반지름 L 인 해밍 구로써, $\mathcal{C} = \mathcal{S}_L(\mathbf{c})$ 로 표현된다. 선형 블록 코드의 중요한 특징 중 하나는 임의의 부호어 \mathbf{c} 에 대하여 해밍 거리 d_ℓ 만큼 떨어진 집합은 잉여류(coset)로 표현될 수 있다는 사실이다. 구체적으로,

$$\begin{aligned} \mathcal{C}_\ell(\mathbf{c}) &= \{\mathbf{c}' \in \mathcal{C} : d_H(\mathbf{c}, \mathbf{c}') = d_\ell\} \\ &= \{\mathbf{c} + \bar{\mathbf{c}} : \bar{\mathbf{c}} \in \mathcal{C}_\ell(\mathbf{0})\} \end{aligned} \quad (3)$$

$$= \mathbf{c} + \mathcal{C}_\ell(\mathbf{0}) \quad (4)$$

이 때 $\mathcal{C}_\ell(\mathbf{0})$ 는 영 부호어(zero codeword)에서 d_ℓ 만큼 떨어진 부호어 집합을 의미한다. 이 관계로 인해 임의의 부호어 \mathbf{c} 를 중심으로 하는 해밍 구는 제로 부호어를 중심으로 하는 해밍 구를 잉여류로 표현할 수 있다.

C. ML 근접 2 단계 디코딩

A. 초기 저복잡도 복화 단계

초기 복호 단계에서 복호기는 수신 신호 \mathbf{y} 로부터 CRC 부호화된 $\hat{\mathbf{v}}^{(-1)}$ 를 얻는다. 만약 CRC가 통과되면 $(\mathbf{H}_{\text{crc}}(\hat{\mathbf{v}}^{(-1)})^T = \mathbf{0})$, 디코딩을 종료하고 해당 코드를 반환한다. 실패 시, $\hat{\mathbf{v}}^{(-1)}$ 을 재부호화 하여 $\hat{\mathbf{c}}^{(0)} = \hat{\mathbf{v}}^{(-1)}\mathbf{G}$ 를 얻고, 신뢰도 $M^{(0)} = \|\mathbf{y} - \mathbf{x}(\hat{\mathbf{c}}^{(0)})\|$ 를 계산한다.

B. 코드 가중치 구 복호 (WSD) 단계

WSD는 영 부호어를 중심으로 하는 반지름 d_r 인 해밍 구 $\mathcal{S}_r(\mathbf{0})$ 을 이용하여 초기 추정지 $\hat{\mathbf{c}}^{(0)}$ 에 대해 반지름 d_r 인 탐색 구 $\mathcal{S}_r(\hat{\mathbf{c}}^{(0)}) = \{\hat{\mathbf{c}}^{(0)} + \bar{\mathbf{c}} : \bar{\mathbf{c}} \in \mathcal{S}_r(\mathbf{0})\}$ 을 구성한다. 각 부스팅 라운드 i 에서, 다음 최적화 문제를 풀어 $\hat{\mathbf{c}}^{(i)} \in \mathcal{S}_r(\mathbf{0})$ 를 찾는다.

$$\hat{\mathbf{c}}^{(i)} = \underset{\bar{\mathbf{c}} \in \mathcal{S}_r(\mathbf{0})}{\operatorname{argmin}} \|\mathbf{y} - \mathbf{x}(\hat{\mathbf{c}}^{(i-1)} + \bar{\mathbf{c}})\| \quad (5)$$

신뢰도 $M^{(i)} = \|\mathbf{y} - \mathbf{x}(\hat{\mathbf{c}}^{(i)})\|$ 를 계산하여 신뢰도가 개선되면 $(M^{(i)} < M^{(i-1)})$, 다음 라운드로 진행하고, 그렇지 않으면 $\hat{\mathbf{c}}^{(i-1)}$ 을 반환하고 종료한다. 이 과정은 최대 J 라운드까지 반복한다. WSD는 선형 블록 코드의 격자 구조와 이동 불변 특성을 활용하여 미리 계산된 해밍 구를 사용함으로써, 기존 구 복호 방식보다 탐색을 단순화하고 복잡도를 줄인다. 또한, 큰 구를 한 번에 탐색하는 대신 작은 구를 반복적으로 탐색하여 점진적으로 해를 개선한다.

A. 복호 복잡도

WSD는 초기 복호 CRC 실패 시에만 활성화되므로, 평균 복잡도는 신호 대 노이즈 잡음비(signal-to-noise ratio, SNR)에 따라 가변적이다. 표. 1와 그림. 2에서 확인할 수 있듯이, 높은 SNR에서는 $P_{e,\text{crc}} = \mathbb{P}[\mathbf{H}_{\text{crc}} \cdot \hat{\mathbf{v}}^T \neq \mathbf{0}]$ 가 낮아 WSD가 거의 동작하지 않지만, 낮은 SNR에서는 $P_{e,\text{crc}}$ 가 높아져 WSD가 더 자주 동작하며 복잡도가 증가한다. 최악의 경우 추가 복잡도는 $P_{e,\text{crc}} \times (N \times J \times \mathcal{S}_r(\mathbf{0}))$ 으로 제한된다.

복호기 종류	복잡도
SCL(L)	$\mathcal{O}(LN \log N)$
SCL(L)+ WSD(r)	$\mathcal{O}(LN \log N) + \mathcal{O}(P_{e,\text{crc}} \times (N \times J \times \mathcal{S}_r(\mathbf{0})))$
MLD	$N \times 2^K$

표. 1. 복잡도 분석.

부호 종류	(N, K)	그림.	$ \mathcal{S}_r(\mathbf{0}) , r = 3$
CA-polar	(64, 15)	1	2344
CA-polar	(128, 15)	1	5040
CA-polar	(256, 15)	1	2263

표. 2. 코드 가중치 구의 크기

B. 시뮬레이션 결과

제안하는 WSD를 CRC 기반(CRC-aided, CA) 극 부호에 적용하여 SCL 복호기와 함께 BLER 성능을 평가하였다. CRC6을 사용하였고, 다항식은 다음과 같다. $g(x) = 1 + x^5 + x^6$. SCL은 list size $L = 4$ 를 사용하였다. WSD에서 사용한 해밍 구의 크기는 표. 2와 같다. 비교를 위해 SCL 단독 사용 시에는 CRC6과 $L = 16$ 를 사용하였다. 블록길이 $N \in \{64, 128, 256\}$ 와 낮은 부호율 $R \in \{\frac{15}{64}, \frac{15}{128}, \frac{15}{256}\}$ 조건에서 실험하였고, 이론적 성능과 비교하기 위해 random coding union (RCU) bound와 meta-converse bound를 계산하여 그래프에 포함하였다[5].

실험 결과, WSD를 적용한 경우 초기 복호기 단독 사용시 보다 일관된 성능 향상을 보였다. 예를 들어, 그림. 1에서 CA-polar (256, 15) 코드에 SCL+ WSD 복호기 사용 시 SCL 단독 사용 대비 BLER 10^{-4} 에서 약

0.5dB 이상의 이득을 보였으며, $N \in \{64, 128\}$ 에서는 ML 복호 성능에 근접했다.

평균 복잡도 분석 결과, 제안된 SCL+ WSD 방식은 SNR이 증가함에 따라 평균 연산량이 감소하였으며, SCL(16) 대비 높은 SNR에서는 평균 연산량이 더 적은 지점을 확인함으로써, 실제 통신 환경에서의 효율성을 입증하였다.

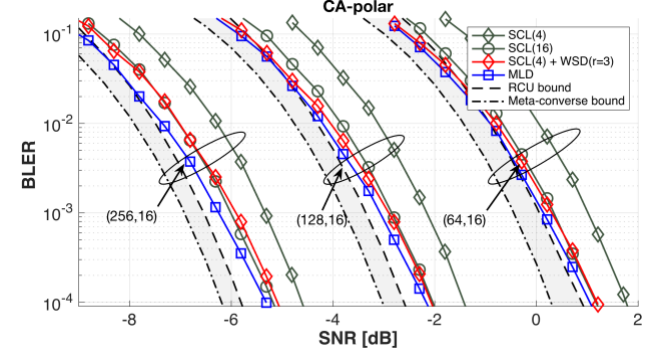


그림. 1. SCL, SCL+WSD, MLD에 따른 BLER 비교

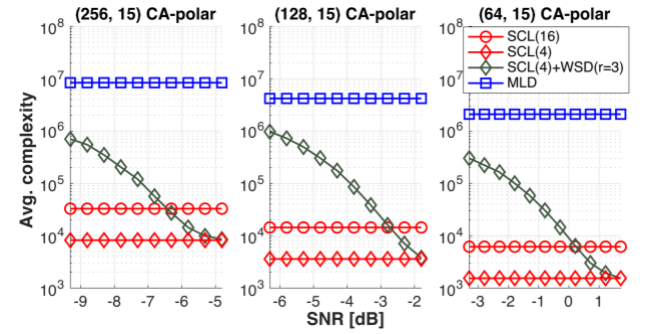


그림. 2. SCL, SCL+WSD, MLD에 따른 복잡도 비교

III. 결론

본 논문은 URLLC를 위한 2 단계 근사 ML 복호 기법인 WSD를 제안하였다. 저복잡도 초기 복호와 WSD를 결합하여, CRC 실패 시에만 코드 가중치 기반 구 탐색을 통해 코드를 반복적으로 개선한다. 이 방식은 선형 부호의 구조적 특성을 활용하여 계산 복잡도를 효율적으로 관리하면서도 근사 ML 성능을 달성한다. 시뮬레이션 결과는 다양한 부호 및 파라미터에 대한 제안 기법의 우수한 성능과 적용 가능성을 보여주며, WSD가 차세대 통신의 신뢰성과 효율성 요구를 만족하는 효과적인 오류 정정 방법임을 입증하였다.

참고 문헌

- [1] M. Rowshan, M. Qiu, Y. Xie, X. Gu, and J. Yuan, "Channel coding toward 6g: Technical overview and outlook," IEEE Open Journal of the Communications Society, vol. 5, pp. 2585-2685, 2024.
- [2] M. P. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," IEEE Trans. Inf. Theory, vol. 41, no. 5, pp. 1379-1396, 2002.
- [3] K. R. Duffy, W. An, and M. Médard, "Ordered reliability bits guessing random additive noise decoding," IEEE Trans. Sig. Process., vol. 70, pp. 4528-4542, 2022.
- [4] I. Tal and A. Vardy, "List decoding of polar codes," IEEE Trans. Inf. Theory, vol. 61, no. 5, pp. 2213-2226, 2015.
- [5] G. Durisi and A. Lancho, "Transmitting short packets over wireless channels—an information-theoretic perspective." [Online]. Available: <https://gdurisi.github.io/fbl-notes/>