2020년도 한국통신학회 하계종합학술발표회

이진 소거 채널(BEC)에서 유한 길이 Reed-Muller 부호의 연속적 제거 복호기 성능과 복잡도에 관한 연구

이우용, 고영조
한국전자통신연구원

{wylee, koyj}@etri.re.kr

Decoding performance limit and complexity of Modified Reed Muller codes with Dynamic Frozen bits on the BEC channels

Lee Woo Yong and Ko Yonng Jo
Electronics and Telecommunications Research Institute (ETRI)

요 약

최근에 짧은 또는 중간 블록 길이 1024 비트 이하 채널 부호에 대한 관심은 짧은 길이의 데이터 전송을 필요로 하는 새로운 응용으로 인해 증가하고 있다. 또한 낮은 복잡도의 부호화 및 복호화 알고리즘에서 채널 용량 달성이 가능한 부호가 있다는 사실이 입증되었다. 한편, 유한 길이의 부호로도 낮은 복잡도의 복호화 알고리즘으로 이론적 성능을 달성할 수 있는지에 대한 관심이 고조되고 있다. 이런 환경에서 최근 연구 결과로 동적(dynamic) 동결(frozen) 비트를 갖는 Reed-Muller (RM) 부호가 이진 소거 채널에서 연속적 제거 목록 복호화 기법을 사용하면서 이론적 성능을 달성할 수 있음이 증명되었다. 본 논문은 동적 동결 비트를 사용하는 RM 부호에 대한 연속적 제거 목록 복호화 기법에서 복잡도를 더욱 개선할 수 있을 가능성을 분석하였다. 본 결과가 새로운 실용적인 부호와 복호기 구조와 새로운 통신 방식을 개발하기 위한 이론적 토대로 사용될 수 있을 것으로 기대한다.

Ⅰ. 서 론

Shannon이 채널 용량을 달성 가능성을 소개한 이후[1], 연구자들은 이 용량을 달성하는 부호 기법을 연구하였다. 최근에 짧은 또는 중간 블록 길이 채널 부호에 대한 관심은 짧은 길이의 데이터 전송을 필요로 하는 새로운 응용으로 인해 다시 증가하고 있다[2]. 한편, 임의 이진 입력 이산 무기억 채널 (BMS: binary-input discrete memoryless symmetric channels)에서 극성 부호(polar codes)는 작은 복잡도의 부호화와 복호화 기법으로 채널 용량 달성을 증명한 첫 채널 부호였다[3]. 더구나, 극성 부호는 하다마드 (Hadamard) 행렬의 일부 구조를 따랐으며 결정적인 구조가 있다. 최근 연구 결과로 부호 이론 분야에서 오랫동안 예측으로 남아 있었던, Reed-Muller (RM) 부호는 MAP (maximum a posteriori) 복호기로 이진 소거 채널 (BEC: binary erasure channel) 용량을 달성한다고 입증하였다[4]. 또한 무게 분포(weight distribution) 분석을 통하여, RM 부호가 BMS 채널 용량을 성취한다는 사실을 규명하였다[5-7].

극성 부호는 연속적 제거 목록 (SCL: successive cancellation list) 복호기를 사용하면서[8], 고속 외부 부호 (outer code)를 추가하는 방식으로 짧은 길이에서 중간 길이까지 영역(즉, 128에서 1024까지 비트)에서 채널 부호 연구가 활발히 일어나고 있다[2]. RM 부호는 극성 부호[3]와 밀접한 관련이 있지만, MAP 복호화 성능[9]에서 이들을 능가하기 때문에, 극성 부호용으로 제안된 일부 복호기가 RM 부호에도 사용되었다. [10]의 저자는 어떤 선형 부호가 동적 동결 비트를 갖는 극성 부호로 보여질 수 있는지 분석하였다. 또한 동적 동결 비트를 Reed-Muller (RM) 부호에 적용하여 이진 소거 채널에서 연속적 제거 목록 복호화 기법으로 이론적 성능을 달성할 수 있음이 증명되었다[11].

본 논문에서는 부분 부호들 즉, 동적 동결 비트를 사용하는 RM 부호어 대한 연속적 제거 목록 복호화 기법에서 복잡도를 더욱 개선할 수 있을 가능성을 분석한다.

Ⅱ. 본론

이진 소거 채널에서 SCL 복호화의 효율적인 구현으로서 비활성화(inactivations) 비트(변수)를 갖는 연속적 제거 (SC: successive cancellation) 복호기가 제안되었다[11]. 제안된 복호기는 SC 복호하는 동안 소거되고 복호화를 계속할 때마다 모조 (dummy) 변수를 정보 비트에 할당하는 것이다. 비활성화된 비트는 동결된 비트를 복호하여 수집된 정보를 사용하여 복호된다. 이 복호기는 하다마드 행렬의 구조를 활용하지만 동적 동결 비트를 갖는 극성 부호로 표시함으로써 모든 선형 부호에 적용할 수 있을 것이다. SCL 복호기는, 최대 사후 확률 (MAP) 복호화 성능을 달성하는데 필요한 평균 비활성화 수를 계산하기 위하여, 밀도 진화 (density evolution)를 사용하여 부분적으로 특성화한다. 이 기법은 다른 형태의 동적 동결 비트를 갖는 RM 부호를 분석하는데 적용될 수 있을 것이다. 이러한 수정된 RM 부호는 확장된 BCH (eBCH: extended Bose-Chaudhuri-Hocquengham) 부호 성능에 근접하여 동작되는 것으로 나타났다[11]. 동적 동결 비트를 사용하는 RM 부호에 대한 연속적 제거 목록 복호화 기법에서 복잡도를 더욱 개선할 수 있을 가능성을 분석하고자 한다.

임의의 선형 블록 부호는 다음과 같이 가역 행렬 (Invertible Matrix) A로 구성할 수 있다.

$$A = B^m F^{\otimes m}$$

여기서 B^m은 비트 역 치환 행렬 (bit reversal permutation

matrix)이고. $\mathrm{F}=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$이다. ⊗m는 m번 관련 형렬에 대한 크로네커 곱(Kronecker product) 연산이다. i ∈ {1, ..., n}에 대하여 n개의 원소 u_i를 갖는 입력 벡터 u에 대한 부호어 C는 uA로 나타낼 수 있다. 예를 들어 밀도 진화를 사용하여 설계된 극성 부호인 경우 복호화 오류를 최소화 하도록 발생(generator) 행렬 A에서 k개의 행을 선택한다. 그러므로 나머지 n-k개의 입력 u_j=0으로 하고 이 비트들을 동결 비트(frozen bit)라고 부른다. 색인 $j \in \mathfrak{I}=\{i \mid u_i=0, i \in \{1, ..., n\}\}$이다.

밀도 진화를 사용하여 설계된 선형 블록 부호인 극성 부호 또는 RM 부호는 부호어간 아주 작은 최소 거리(minimum distance)를 갖는다. 이를 해결하기 위하여 동결 비트를 모두 u_j=0로 설정할 필요는 없다는 것을 발견하였다[]. j < i에 대하여 동결 비트 u_i는 미리 정의된 정보 비트 u_j들의 함수일 수 있다. 이것은 A에 의해 선형 변환된 비트 부채널의 성능과 SC(successive cancellation) 복호기의 성능에 영향을 주지 않는다.

홀짝 검사(parity-check) 행렬 H를 갖는 선형 부호 C (n=2^m, k, d)에 대하여 $uAH^T=uV^T=0$을 만족하면 어떤 적당한 개수의 행을 더한 길이의 부호어 얻을 수 있다. 이것은 부호어간 최소 거리를 키우는 효과를 가져올 수 있다.

$1 \le j \le n-k$ 에 대하여 $i_j = \max\{t \in \{1, \cdots, n\} \mid V_{j,t} = 1\}$라 할 때 동결 비트 색인 집합 $\mathfrak{I}$은 $\{t \mid \exists j : i_j = t\}$과 같이 나타낼 수 있다. $\mathfrak{I}=\{t \mid \exists j: i_j = t\}$이고, $S_j = \{t \mid V_{j,t} = 1, t < i_j\}$ 일 때 동적 동결 비트 u_j 의 제한 조건은 다음과 같다.

$$u_j = \sum_{t \in S_j} u_t, \quad j \in \mathfrak{I}$$

이때 S_j 가 공집합이면 기존의 정적인 동결 비트를 나타내고, $|S_j| \ge 1$ 이면 동적 동결 비트를 의미한다. 한편, 동결 비트로 사용하기 위한 정보 비트 색인은 $I_f = \{t \in \{1, \cdots, i_j\}, t \notin \mathfrak{I} \mid V_{j,t} = 1, 1 \le j \le n-k\}$이다. 동적 동결 비트 색인 $D_f = \{i \in \mathfrak{I}, S_i \neq \emptyset\}$이다. 채널에 대한 출력 에 대하여 SC 복호화 과정에서 비트 u_i에 대한 추정 값 $\widehat{u_i}$은 최근 연구 결과[12]를 확장하면 다음과 같다.

$$\widehat{u_i} = \begin{cases} \underset{u_i \in \{0,1\}}{\operatorname{argmax}} \mathrm{P}\left(u_i \mid y_1^n, \hat{u}_1^{i-1}\right), & for \ \ i \notin \mathfrak{I}, \ i \notin I_f \\ u_i, & for \ \ i \in \mathfrak{I}, \ S_i = \emptyset \\ \underset{u_i \in \{0,1\}}{\operatorname{argmax}} \mathrm{P}\left(u_i, \sum_{t \in S_i} \widehat{u_t} \mid y_1^n, \hat{u}_1^{i-1}\right), & for \ \ i \in \{I_f, D_f\} \end{cases}$$

이때 SC 복호기의 i 번째 u_i 비트의 오류 확률 b_i 는 동적 동결 비트에 대한 최대 사후 확률 복호를 고려하면 다음과 같다.

$$b_i = \begin{cases} 0 \ for \ \ i \in \mathfrak{I}, \ S_i = \emptyset \\ \left(\prod_{t \in \{I_f, D_f\}} \epsilon_t\right)^{\frac{1}{|I_f|}} \ for \ \ i \in \{I_f, D_f\} \\ \epsilon_i \quad otherwise \end{cases}$$

$\epsilon_i < 1$에 대하여 $\left(\prod_{t \in \{I_f, D_f\}} \epsilon_t\right)^{\frac{1}{|I_f|}} \approx 0$이면, u_i 비트의 오류 확률 b_i는 다음 식으로 간소화 될 수 있다.

$$b_i = \begin{cases} 0 \ for \ \ i \in \mathfrak{I} \ \text{or} \ i \in I_f \\ \epsilon_i \quad otherwise \end{cases}$$

복호화 복잡도를 분석하기 위하여 확률 변수(RV: random variables)에 대한 SC-목록 복호화를 가정하면[11], 무경계(Unbounded) 목록 개수 B 의 평균 값 $E(B)$은 다음과 같다.

$$E(B) = \sum_{i \in \mathfrak{I}^c} \epsilon_i - \sum_{i \in I_f} \epsilon_j = \sum_{i \in \{\mathfrak{I}, I_f\}^c} \epsilon_i$$

목록 개수 B의 평균 값 $E(B)$는 복호화 복잡도를 의미하며 [11]의 선행 결과에 비하여 $2^{\sum_{i \in I_f} \epsilon_j}$ 배 만큼 개선되었다는 것을 의미한다.

Ⅲ. 결론

기존 연구 결과는 동적 동결 비트를 갖는 RM 부호가 BEC 채널에서 연속적 제거 목록 복호화를 사용하면서 채널용량을 달성할 수 있음이 최근에 증명되었다[11]. 본 논문에서는 같은 조건에서 동적 동결 비트를 사용하는 RM 부호에 대한 연속적 제거 목록 복호화에서 복잡도를 더욱 개선할 수 있을 가능성을 분석하였다. 그러므로 본 결과가 새로운 구현 가능한 채널 부호와 복호기 구조 설계에서 미래 통신 방식을 연구 개발하기 위한 이론적 기반으로 적용될 수 있을 것이다.

ACKNOWLEDGMENT

이 논문은 2020 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이다. [No.2019-0-00002, (전문연구실) 초정밀 서비스 실현을 위한 On-Time·On-Rate 무선액세스 및 광에지 클라우드 네트워킹 핵심기술 개발].

참 고 문 헌

[1] C. E. Shannon, “A mathematical theory of communication,” The Bell Syst. Techn. J., vol. 27, pp. 379–423, 623–656, July / Oct. 1948.

[2] M. C. Coskun, G. Durisi, T. Jerkovits, G. Liva, W. Ryan, B. Stein, and F. Steiner, “Efficient error-correcting codes in the short blocklength regime,” Elsevier Physical Communication, vol. 34, pp. 66–79, Jun. 2019.

[3] E. Arıkan, “Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels,” IEEE Trans. Inform. Theory, vol. 55, no. 7, pp. 3051–3073, July 2009.

[4] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Sasoglu, and R. L. Urbanke, “Reed-Muller codes achieve capacity on erasure channels,” submitted to IEEE Trans. Inform. Theory, vol. 63, no. 7, pp. 4298–316, Jul. 2017.

[5] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, and R. L. Urbanke, “Comparing the bit-MAP and block-MAP decoding thresholds of Reed-Muller codes on BMS Channels,” in Proc. ISIT 2016, pp. 1755–1759, Jul. 2016.

[6] 이우용, “이진 비기억 대칭 (BMS) 채널에서 극성 부호와 Reed-Muller 부호의 복호 성능 한계에 관한 연구,” 한국통신학회 동계종합학술발표회, pp. 120-2, 2017.

[7] 이우용, “이진 비기억 대칭 (BMS) 채널에서 선형 블록 부호의 최대우도 (ML) 복호 성능 한계에 관한 연구,” 한국통신학회 추계종합학술발표회, pp. 78-9, 2016.

[8] I. Tal and A. Vardy, “List decoding of polar codes,” IEEE Trans. Inf. Theory, vol. 61, no. 5, pp. 2213–2226, May 2015.

[9] M. Mondelli, S. H. Hassani, and R. L. Urbanke, “From polar to Reed-Muller codes: A technique to improve the finite-length performance,” IEEE Trans. Commun., vol. 62, no. 9, pp. 3084–3091, Sep. 2014.

[10] P. Trifonov and V. Miloslavskaya, “Polar subcodes,” IEEE J. Sel. Areas Commun., vol. 34, no. 2, pp. 254–266, Feb. 2016.

[11] M. C. Coskun, J. Neu and H. D. Pfister, “Successive Cancellation Inactivation Decoding for Modified Reed Muller and eBCH Codes,” Apr. 2020, https://arXiv: 2004.05969v1.