

최소 해밍 거리를 이용한 효율적인 채널 부호 추정

*장민규, *김동영, *윤동원[†]

*한양대학교 융합전자공학과

dwyoona@hanyang.ac.kr[†]Efficient Estimation of Channel Code
Using Minimum Hamming Distance*Mingyu Jang, *Dongyeong Kim, *Dongweon Yoon[†]

*Hanyang University

요약

비협력 통신 상황에서는 송신기와 수신기가 통신 파라미터를 공유하지 않기 때문에 수신기에서는 송신기에서 사용한 통신 파라미터를 스스로 추정하여야 한다. 다양한 통신 파라미터 가운데 채널 부호의 파라미터를 추정하는 연구가 최근 진행되고 있다. 비록 전수조사를 통해 채널 부호의 파라미터를 추정할 수 있지만 이는 계산 복잡도가 높다는 단점이 있다. 본 논문에서는 전수조사 방법의 계산 복잡도를 줄이기 위하여 채널 부호의 파라미터를 추정하기 위한 최소 탐색 수를 계산한다.

I. 서론

비협력 통신 상황에서는 송신기와 수신기가 통신 파라미터를 공유하지 않기 때문에 수신기에서는 송신기에서 사용한 통신 파라미터를 스스로 추정하여야 한다. 이 때 수신 신호로부터 채널 부호 디코딩을 하기 위해선 송신기에서 사용한 채널 부호의 원시 다항식을 추정하여야 하며 이와 관련하여 연구가 진행되고 있다[1]. 채널 부호의 원시 다항식을 추정하는 방법 중 하나는 전수조사이지만 이는 계산 복잡도가 높아 실제 상황에서 활용하기 어렵다는 단점이 있다. 이를 해결하기 위하여 본 논문에서는 계산 복잡도를 낮춘 채널 코드 추정 방법과 이 때 필요한 최대 탐색 수를 제시한다.

II. 시스템 모델

송신기에서 부호의 길이는 n , 메시지의 길이는 k 인 (n, k) 해밍 부호를 사용한다고 가정한다. 이 때 해밍 부호의 파라미터인 n, k 는 [1]에서 제안한 방법을 통해 추정 가능하다. 이 때 M 비트의 수신 데이터를 n 길이의 행벡터로 구분하여 행으로 나열하면 $n \times \frac{M}{n}$ 크기의 행렬을 구성할 수 있으며 각 행이 하나의 해밍 부호로 구성된다. 그리고 이 행렬의 각 열 단위로 해밍 부호의 메시지 비트와 패리티 비트가 정렬된다.

해밍 부호의 선형성은 $(n-k) \times n$ 크기의 패리티 검사 행렬로 표현될 수 있으며, 패리티 검사 행렬의 각 행은 해밍 부호 비트들의 선형 관계를 의미하고 언제나 $\alpha = \frac{n+1}{2}$ 의 해밍 무게를 가진다. 한편, 패리티 검사 행렬의 각 행들 간의 조합 또한 선형성을 보이므로 총 $\beta = 2^{n-k} - 1$ 개의 선형 관계가 한 종류의 채널 부호에 존재한다. (1)은 (7, 4) 해밍 부호에 대한 선형 관계 예시를 나타낸다. (1)에서 보이는 것과 같이 (7, 4) 해밍 부호는 $\beta=7$ 개의 선형 관계를 가지며 (1)의 각 행의 해밍 무게는 모두 $\alpha=4$ 이다. $n \times \frac{M}{n}$ 크기의 행렬에서 (1)의 각 행에서 1에 해당하는 위치의 4개의 열을 모두 더하면, 선형성으로 인해 제로열이 된다.

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

III. 추정 방법 복잡도 분석

채널 부호의 원시 다항식을 추정하기 위해서는 채널 부호의 메시지 비트와 패리티 비트 간의 선형 관계를 추정하여야 하며, β 개의 선형 관계 중 최소 한 개만 찾으면 된다. 이를 위해 선형 관계를 찾는 방법으로 전수조사 방법이 있다. (n, k) 해밍 부호의 경우 n 개의 열에서 α 개를 선택하는 경우의 수는 ${}_nC_\alpha$ 가지이며 원시 다항식을 추정하기 위해 총 ${}_nC_\alpha$ 가지 조합을 탐색하여야 한다. 이는 채널 부호의 크기가 커질수록 계산 복잡도가 기하급수적으로 증가한다는 문제가 있다. 따라서 본 논문에서는 채널 부호의 최소 해밍 거리 성질을 이용하여 확률 1로 오직 한 개의 선형 관계를 찾는 데 필요한 최대 탐색 수를 계산한다.

채널 부호의 각 선형 관계는 채널 부호의 성질에 따라 균일하게 분포하기 때문에 모든 경우의 수에서 가장 인접한 조합들만 조사한다면 반드시 β 개의 선형 관계 중 한 개를 찾을 수 있다. (n, k) 해밍 부호의 경우 총 ${}_nC_\alpha$ 가지 경우의 수에 β 개의 선형 관계가 존재하기 때문에 ${}_nC_\alpha / \beta$ 개의 선형 관계만 조사하면 반드시 하나의 선형 관계를 찾을 수 있고 이를 통하여 채널 부호의 원시 다항식을 추정할 수 있다.

참고 문헌

- [1] A. D. Yardi, S. Vijayakumaran, and A. Kumar, "Blind reconstruction of binary cyclic codes from unsynchronized bitstream," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2693-2706, Jul. 2016.
- [2] A. Bonvard, S. Houcke, R. Gautier, and M. Marazin, "Classification based on Euclidean distance distribution for blind identification of error correcting codes in noncooperative contexts," *IEEE Trans. Signal Process.*, vol. 66, no. 10, pp. 2572-2583, May 2018.