엣지 추가에 따른 PBRL LDPC 부호의 최소 해밍거리 상한에 대한 분석

한민석, *박호성
전남대학교 ICT융합시스템공학과
email : gksalstjr7@naver.com, hpark1@jnu.ac.kr

Analysis of Upper Bound on Minimum Hamming Distance of PBRL LDPC Codes with Edge Addition

Minseok Han, *Hosung Park
Department of ICT Convergence System Engineering
Chonnam National University

요 약

본 논문에서는 고신뢰도 저지연 무선통신 시스템에 적합한 프토로그래프 기반 랩터 유사 저밀도 패리티 검사(PBRL LDPC) 부호의 프로토그래프에 일부 엣지를 추가한 것을 분석한다. 추가된 엣지는 전체 프로토그래프의 최소 해밍 거리와 관련된 지표인 최소 해밍거리 상한를 증가시키는 역할을 한다. 엣지 추가는 프로토그래프의 기존 엣지 연결을 변경하지 않기 때문에 엣지를 추가하는 구조를 사용하거나 사용하지 않음으로써 적응적으로 사용하는 시스템이다. 제안하는 구조는 5G NR에 정의된 LDPC 부호를 비롯하여 일반적인 PBRL LDPC 부호에 적용 가능하다.

Ⅰ. 서 론

R. G. Gallager가 제안한 저밀도 패리티 검사(LDPC) 부호는 복호기 구현의 높은 병렬성과 우수한 오류 정정 성능으로 인해 고속 통신에서 가장 우수한 채널 부호가 되었다. PBRL LDPC 부호는 채널 상태에 맞게 채널 코딩을 조절하는 부호율 호환성 특징을 가진다. 부호율 호환성이 없으면 모든 부호율에 대해 많은 LDPC 부호를 설계, 저장 및 구현해야 하지만 PBRL LDPC 부호는 패리티 비트 수를 자유롭게 조절하여 다양한 부호율을 하나의 부호로 구현할 수 있다. 따라서 채널 상태가 빠르게 변하는 무선 통신 환경에 적합하다. 본 논문에서는 최소 해밍거리와 관련된 지표인 최소 해밍거리 상한을 증가시키기 위해 PBRL LDPC 부호의 단위행렬 부분의 하삼각부분에 추가한 것을 분석하고자 한다.

Ⅱ. 기존 PBRL LDPC 부호의 최소 해밍거리 상한

PBRL LDPC 부호는 프로토행렬로 표현 가능하며 그 구조는 다음과 같다.

$$P = \begin{bmatrix} P_{HRC} & 0 \\ P_{IRC} & I \end{bmatrix}$$

프로토행렬은 $n_c \times n_v$의 크기로 표현된다. P_{HRC}는 $n_{cH} \times n_{vH}$의 크기, P_{IRC}는 $(n_c - n_{cH}) \times (n_v - n_{vH})$의 크기이다.

정의1(퍼머넌트) :크기 $l \times l$ 사각행렬 A의 퍼머넌트 $perm(A)$는 다음과 같이 정의된다.

$$perm(A) = \sum_{\sigma} \prod_{j=1}^{l} A(j,\sigma(j)) = \sum_{\sigma} \prod_{j=1}^{l} A(\sigma(j),j) \quad -(1)$$

여기서 σ는 $[l]$의 순열을 가리킨다.

보조정리1(프로토행렬의 최소 해밍거리 상한 [1]) : $n_c \times n_v$ 크기의 프로토행렬을 P라고 하자. 프로토행렬 P로부터 얻은 코드워드 C는 다음과 같은 상한을 갖는 최소거리 $d_{\min}(C)$를 가진다.

$$d_{\min}(C) \le \min_{T \subseteq [n_v], |T| = n_c+1}^{*} \sum_{i \in T} perm(P_{T \setminus i}) \quad -(2)$$

집합 T의 크기를 $|T|$라고 표현하고, 행렬의 행과 열의 index는 1부터 시작한다. P_T는 T의 원소로 선택된 열에 의해 형성된 P의 하위행렬을 나타낸다. 편의상, 우리는 항상 T에 의해 선택된 P열이 P에 나타나는 것과 같은 순서로 P_T에 나타나는 것으로 가정한다. 만약 $i \in T$라면, $T \setminus \{i\}$를 $T \setminus i$라고 간단히 표현한다. 음이 아닌 정수 집합의 경우, $\min^*$을 0이 아닌 최솟값을 반환하는 함수로 두거나, 최솟값이 0인 경우 $+\infty$를 반환한다. 기존의 최소 해밍거리 상한 공식에 의하여 크기 $n_c \times n_v$의 프로토행렬 P에서 크기 $(n_c) \times (n_c+1)$의 부분행렬 P'을 ${}_{n_v}C_{n_c+1}$개 만든다. 각각의 P'에서 크기 $n_c \times n_c$의 부분행렬 P''의 Permanent (n_c+1)개를 모두 더한다. ${}_{n_v}C_{n_c+1}$개의 P'의 중 가장 작은 값이 $d_{\min}(C)$이다.

최소거리를 구하기 위한 계산 복잡도가 너무 크기 때문에 최소거리와 연관된 최소 해밍거리 상한이라는 설계기준을 도입했다. 하지만 다양한 길이의 부호어를 위해서는 그에 따라 다양한 크기의 행렬이 필요하다. 이를 부호율 호환이라고 하며, 부호율 호환을 만족하고, 최소 해밍거리 상한을 계산할 수 있는 절차가 필요하다.

최소 해밍거리 상한을 최대화하는 프로토행렬을 찾는 절차를 위해 논문 [1]의 정리 6에 의해 값이 최소가 되도록 하는 T에는 I 행렬의 모든 열의 인덱스가 항상 포함하도록 설정하고, P_{HRC}의 열 인덱스 부분에서 집합 T에서 제외되는 인덱스를 선택하도록 하였다.

먼저 프로토행렬의 부분행렬 $n_{cH} \times n_{vH}$의 P_{HRC}에서 (2) 수식을 사

용하고, $OPtimal\,Vector$ 행렬에 저장한다. 이때 그 후, P_{HRC}의 아래에 P_{IRC}의 첫 행을 추가하면서 크기 $(n_{cH}+1)\times n_{vH}$의 퍼머넌트를 계산하고, 그 값을 $SumMatrix$ 행렬에 저장한다. $OPtimal\,Vector$의 크기는 $1\times {}_{n_{vH}}C_{n_{cH}+1}$이고, $SumMatrix$는 P_{IRC}의 두 번째 행을 추가하면서 연산을 반복하기 때문에 $SumMatrix$의 크기는 $(n_c-n_{cH})\times {}_{n_{vH}}C_{n_{cH}+1}$이다.

Ⅲ. 엣지 추가에 따른 PBRL LDPC 부호의 최소 해밍거리 상한 분석

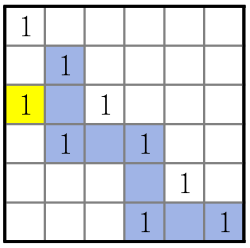

그림 2. 프로토행렬의 단위행렬 부분

프로토행렬에 엣지를 추가하면 할수록 임계값이 커지고, 부호화/복호 복잡도가 증가하게 된다. 따라서 추가하는 엣지의 개수를 최소화하면서 증가하는 최소 해밍거리 상한을 최대화하는 방법이 필요하다. 본 논문에서는 사슬구조의 개수가 0개 아니면 1개가 존재하는 것을 고려한다.

행렬 S의 크기는 $(n_c-n_{cH}+1)\times {}_{n_{vH}}C_{n_{cH}+1}$이고, 행의 크기는 P의 부분행렬 P'의 개수와 같다. $S[0][j]=OptimalVector[j]$, $j=\{1,\ldots,{}_{n_{vH}}C_{n_{cH}+1}\}$ 이고, $S[i][j]=SumMatrix[i][j]$, $i=\{1,\ldots,(n_c-n_{cH})\}$, $j=\{1,\ldots,{}_{n_{vH}}C_{n_{cH}+1}\}$ 이라고 한다.

아래 정리에서 T의 개수는 행렬 S의 열과 대응하므로, $S[i][T]$를 $S_T(i)$로 간단히 나타낸다.

또한 단위행렬의 크기가 $(n_c-n_{cH})\times(n_c-n_{cH})$이므로, 추가할 수 있는 최대 엣지의 개수는 $n_c-n_{cH}-1$개다.

보조정리2 : (r,c)의 좌표에 엣지를 1개 추가했을 때 증가하는 최소 해밍거리 상한은 다음과 같다.

$$d_{\min}(C)\le \min_{T\subseteq[n_{vH}],|T|=n_{cH}+1}^{*}\{(\sum_{i=0}^{n_c-n_{cH}}S_T(i))+S_T(c)\}$$

증명 : 크기 $n_c\times(n_c+1)$의 P'에서 크기 $n_c\times n_c$의 P''가 (n_c+1)개 형성이 되는데, 엣지를 추가하게 되면 r번째 열을 제외한 부분행렬 P''의 단위행렬 부분에서 퍼머넌트 값의 변화가 일어나게 된다. 엣지가 추가됨에 따라, (c,c), (r,r)을 제외한 모든 대각 원소와 (r,c)가 선택될 수 있다. 왜냐하면 (r,r)이 선택되면 (r,c)가 선택되지 못하기 때문에, 엣지를 추가하지 않는 것과 같기 때문이다. 해당 행과 열을 제외한 부분행렬의 퍼머넌트의 값은 $S_T(c)$와 같다. 그렇기에 엣지를 1개 추가하게 된다면 기존보다 $S_T(c)$만큼의 퍼머넌트 값이 증가하게 된다.

보조정리3 : $(r_1,c_1),(r_2,c_2),\ldots,(r_k,c_k)$의 좌표에 엣지를 k개 추가한다. 추가한 엣지는 길이 $(2k+1)$의 단일 사슬구조를 형성하고 이의 좌표는 다음과 같다.

$$(c_1,c_1)-(r_1,c_1)-(r_1,c_2)-,\ldots,(c_k,c_k)-(r_k,c_k)-(r_k,r_k)$$

이때 증가하는 최소 해밍거리 상한은 다음과 같다.

$$d_{\min}(C)\le \min_{T\subseteq[n_{vH}],|T|=n_{cH}+1}^{*}\{\sum_{i=0}^{n_c-n_{cH}}S_T(i)+\sum_{j=1}^{k}(k+1-j)S_T(c_j)\}$$

증명 : 크기 $n_c\times(n_c+1)$의 P'에서 크기 $n_c\times n_c$의 P''가 (n_c+1)개 형성이 되는데, 엣지를 추가하게 되면 $r_1,r_2,\ldots,r_k$ 번째 열을 제외한 k개의 부분행렬 P''의 단위행렬 부분에서 퍼머넌트 값의 변화가 일어나게 된다.

r_1번째 열을 제외한 부분행렬 P''에서는 엣지가 추가됨에 따라, $(r_1,r_1),(c_1,c_1)$을 제외한 모든 대각 원소와 (r_1,c_1)가 선택된다.

해당 행과 열을 제외한 부분행렬의 퍼머넌트의 값은 $S_T(c_1)$와 같다.

r_2번째 열을 제외한 부분행렬 P''에서는 엣지가 추가됨에 따라, (r_2,c_2)를 선택해서 증가하는 퍼머넌트의 값은 $S_T(c_1)+S_T(c_2)$와 같다.

r_k번째 열을 제외한 부분행렬 P''에서는 엣지가 추가됨에 따라, (r_k,c_k)를 선택해서 증가하는 퍼머넌트의 값은 $S_T(c_1)+S_T(c_2)+,\ldots,+S_T(c_k)$와 같다. 그렇기에 엣지를 사슬구조의 형태로 k개 추가하게 된다면 퍼머넌트의 값은 $\sum_{j=1}^{k}(k+1-j)S_T(c_j)$ 만큼 증가하게 된다.

정리1 : 보조정리 2, 3를 종합하면 길이 $(2k+1)$의 사슬구조와 이 사슬구조에 포함되지 않고, 다른 길이 5 이상의 사슬구조를 만들지 않는 엣지의 개수가 l개일 때 좌표는 다음과 같다,$(p_1,q_1),(p_2,q_2),\ldots,(p_l,q_l)$

이때 증가하는 최소 해밍거리 상한은 다음과 같다.

$$d_{\min}(C)\le \min_{T\subseteq[n_{vH}],|T|=n_{cH}+1}^{*}\{(\sum_{i=0}^{n_c-n_{cH}}S_T(i))+\sum_{j=1}^{k}(k+1-j)S_T(c_j)+\sum_{h=1}^{l}S_T(q_h)\}$$

증명 : 보조정리 2와 보조정리 3의 결과로 정리 1을 증명할 수 있다. 그러나 이에 대한 자세한 증명은 본 논문의 페이지 제한으로 생략한다.

Ⅳ. 결론

본 논문에서는 PBRL LDPC 부호의 프로토행렬에 새로운 엣지를 추가한 구조를 이론적으로 분석한다. 추가된 엣지는 전체 프로토그래프의 최소 해밍 거리와 관련된 지표인 최소 해밍거리 상한를 증가시키는 역할을 하고, 엣지를 추가하는 위치에 따라 다르게 증가하는 최소 해밍거리 상한을 분석한다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원(No. 2021001016001)의 지원을 받았고, 동시에 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0(IITP-2022-RS-2022- 00156385) 사업의 연구결과임.

참 고 문 헌

[1]S. V. S. Ranganathan, D. Divsalar and R. D. Wesel, "Quasi-Cyclic Protograph-Based Raptor-Like LDPC Codes for Short Block-Lengths," IEEE Trans. Inf. Theory vol. 65, no. 6, pp. 3758-3777, Jun. 2019