논문 2011-48TC-4-4

극 부호의 연속 제거 복호 : 채널의 합성과 분리

(Successive Cancellation Decoding of Polar Codes : Channel Synthesis and Decomposition)

이 문 호*, 이 준**, 박 주 용***

(Moon Ho Lee, Jun Li, and Ju Yong Park)

요 약

본 논문에서는 Arikan이 제안했던 극 부호[6]의 부호화 및 복호화의 대수적 식을 개선하여 이진 이산 무기억 대칭 채널에서 연속 제거 복호 알고리즘을 이용한 극 부호의 채널의 합성과 분리를 확인했다. 이진 이산 무기억 대칭 채널 W에서 양극화 행렬 $G_2^{\otimes n}$을 통하여 블록 길이 2^n인 극 부호를 효과적으로 구성하여 정보 비트를 전송할 수 있다. 특히, $N \geq 2$일 때, Arikan 부호의 복잡도 $O(Nlog_2N)$이다. 극 부호가 향후 다중점 통신의 문제에 대한 하나의 대안이 될 수 있다는 것을 확인하였다.

Abstract

In this paper, we verify the channel synthesis and decomposition of polar codes using successive cancellation decoding algorithm over binary discrete memoryless symmetric channel by modifying Arikan's algebraic formular[6] on encoding and decoding of polar codes. In addition, we found that information bits are sent by efficiently consisting of polar codes with their size 2^n through polarizing matrix $G_2^{\otimes n}$ over binary discrete memoryless symmetric channel W. Expecially, if $N \geq 2$, the complexity of Arikan's encoding and decoding for polar codes is $O(Nlog_2N)$. Furthermore, we found that polar codes are one of the solution to the challenging problems for the multipoint communication.

Keywords : successive cancellation, channel synthesis, channel decomposition, Polar code.

Ⅰ. 서 론

1948년 Shannon의 채널 용량 이론 발표 후 정보 이론에 많은 발전이 이루어져 왔다. 특히 채널 부호 분야는 대수적인 방법을 토대로 부호어간 최소 해밍 거리가 클 뿐만 아니라 좋은 대수적 특성을 가져 정보 전송 중에 발생한 잡음의 영향을 최소화하여 복호할 수 있는 선형 이진 부호를 생성하는 데 초점이 맞추어졌다. 이는 최소 해밍 거리가 클수록 더 많은 오류를 정정할 수 있다는데 착안을 한 것이다.

Hamming이 하나의 오류를 정정할 수 있는 해밍 부호(Hamming code, 1950년)를 제안한 이후 효율적인 대수적 복호 알고리즘으로 알려져 있는 BCH 부호(1959년), 리드-뮬러 부호(1960년), 리드-솔로몬 부호(1960년) 등이 차례로 제안되어 현재 CD, DVD, Modem 분야에서 사용되고 있다.

Elias는 '0'이 아닌 상대적인 해밍 거리와 높은 부호율을 갖는 적부호(product codes, 1955년)를 제안하였고, Forney는 MIT 박사 학위 논문에서 블록 길이가 증가할수록 오류 확률이 지수적으로 감소할 뿐만 아니라 다항식 시간 복호 복잡도를 갖는 부호에 대한 해결책으로서 '안'과 '밖'의 부호를 결합하여 생성하는 연접 부호

* 평생회원-교신저자, 전북대학교 정보통신공학과
(Chonbuk National University)
** 학생회원, 전북대학교 전자정보공학부
(Chonbuk National University)
*** 정회원, 신경대학교 인터넷정보통신학과
(Shingyeong University)
※ 본 연구는 세계수준의 연구 중심 대학 (WCU) R32-2009-20014-0과 기초연구 2010-0020942 NRF (한국연구재단) 지원으로 이루어졌음.
접수일자:2010년10월4일 수정완료일자:2011년4월18일

(concatenated codes, 1966년)를 제안하였다.

이후 복호 알고리즘에 확률적인 개념을 결합하여 복호 성능을 향상시킨 여러 부호들이 제안되었다. Elias가 제안한 길쌈 부호(convolutional codes, 1955년)를 필두로, 블록 크기가 커질수록 복잡도가 선형적으로 증가하지만 블록 오류 확률을 최소화할 수 있는 비터비 알고리즘(1969년)과 BCJR 알고리즘(1974년)이 제안되었다.

반면에, Fano는 상한 전송율보다 작은 전송율로 전송할 때, 블록 크기가 커질수록 복잡도가 선형적으로 증가하는 순차적인 복호 알고리즘(1963년)을 제안했다.

한편, Gallager는 MIT 박사 학위 논문에서 부호의 해밍 거리를 결정하는 적은 수의 '0'이 아닌 원소로 이루어진 패리티 검사 행렬과 낮은 복잡도의 순환적인 복호 알고리즘으로 생성할 수 있는 저밀도 패리티 검사 부호(LDPC codes, 1963년)[13]를 제안하였지만, 그 당시의 미약한 하드웨어 기술로 인하여 주목받지 못했다.

이후 Berrou가 반복 복호 알고리즘을 사용하여 Shannon 채널 용량에 가까운 성능을 얻을 수 있는 터보 부호(Turbo codes, 1993년)[14]를 제안하였다. 한편, MacKay와 Neal은 희소 행렬을 패리티 검사 행렬로 하여 부호어를 생성하고 신뢰 전파 복호 알고리즘을 통하여 Shannon 채널 용량에 가까운 성능을 얻을 수 있는 저밀도 패리티 검사 부호(LDPC codes, 1997년)[15]를 재발견하였다.

터보 부호의 성공과 저밀도 패리티 검사 부호의 재발견으로 인하여 현재까지 저밀도 패리티 검사 부호와 메시지 전달 알고리즘에 대한 연구가 활발히 이루어지고 있다. 현재 다양한 채널에서 터보 부호와 저밀도 패리티 검사 부호가 Shannon 채널 용량에 근접하도록 하는 연구가 많이 진행되고 있지만, 이진 소실 채널 이외의 다른 채널에서 Shannon 채널 용량에 근접함을 증명하지 못했다. Gallager의 제자인 터키의 Bilkent 대학의 Arikan은 채널의 합성과 분리라는 기법으로 주어진 N개의 채널로부터 변환된 N개의 채널을 생성한 다음, 변환된 채널들이 극단적으로 좋거나 나쁘다는, 즉, 채널의 양극화 현상을 이용하여 변환된 채널들이 극단적으로 좋다면, Shannon 채널 용량에 근접하는 극 부호(polarcodes, 2008)[6]를 제안하였고, 입력 채널을 나누어 상한 전송율을 높일수록 채널 용량에 근접한다는 것을 보였다.[1~5]

터보 부호 및 저밀도 패리티 검사 부호를 이용한 점대 점(point to point) 통신에서의 채널 용량의 달성은 더욱 다양한 채널 즉 다중 입출력 안테나(MIMO) 혹은 다중점 채널에서의 채널 용량 통신으로 관심을 돌리게 했다. 예를 들어, 다중 입출력 안테나 채널에서는 고유 빔포밍(eigen beamforming)의 기술과 점 대 점 통신 채널 부호를 동시에 사용하면, 채널 용량 통신이 달성할 수 있다. 또한 방송 채널 등에서의 효율적인 통신을 위하여 터보 부호나 저밀도 패리티 검사 부호에 정보 이론에서 도입하였던 중첩 부호화(superposition coding) 기술을 적절한 변조 기술을 적용하여 실현하기도 하였다[16~18]. 하지만, 일반적인 다중점 채널에서의 채널 용량 계산이나, 부호화 기술의 고안은 오랜 시간 동안 해결하지 못하고 있다. 2008년 터키의 Arikan은 극 부호라는 개념을 제안했고[1~8], 이를 인정받아 2011년 Arikan의 극 부호에 대한 최근 논문이 IEEE Transaction on Information Theory의 최우수 논문으로 선정된 바 있다. 이 극 부호는 최초로 일반적인 채널에서 실용적인 복잡도를 가지는 동시에 채널 용량 통신을 점근적으로 달성시키는 부호이다. 또한, 이 극 부호는 부호의 생성 자체가 채널 용량 통신의 달성의 이론적 입증을 내포한다. 뿐만 아니라, 이 극 부호를 점 대 점 통신이외에 다중점 통신 혹은 분산 소스 부호화 등에도 적용할 수 있음이 입증됨으로써 다중점 통신에서의 다양한 미결 문제를 해결할 대안[20]으로 떠오르고 있다.

본 논문에서는 정보 및 부호 이론 분야에서 새로운 패러다임으로 등장한 극 부호를 소개하고, 이 부호의 이론적 의미를 살펴보고, Ⅱ장에서는 2^n 극 부호의 부호화를 다루고, Ⅲ장에서는 2^n 극 부호의 복호화를 다룬다. Ⅳ장에서는 컴퓨터 모의실험 결과를 통하여 극 부호의 성능이 채널 용량에 근접함을 보이고, Ⅴ장에서 결론을 맺는다.

Ⅱ. 블록 길이 2^n 극 부호 채널의 합성

2.1. 채널의 합성(Channel Synthesis)

블록 크기가 N인 이진 이산 무기억 채널에서 N개의 채널을 사용하여 하나의 부호어를 전송하는, 하나의 부호어를 전송하기 위한 N개의 독립적인 채널 W의 합성 및 분리를 통하여 채널의 양극화 현상을 얻는다. 그림 1[20]은 다중점 채널에서 극 부호의 부호화 및 복호화에 관한 블록도를 보여준다. 길이 N인 왼쪽 $\boldsymbol{u}$벡터의 K 비트가 정보 비트이고 나머지 $N-K$ 비트는 의사 비트(dummy bit)이다. $\boldsymbol{u}$벡터를 입력 벡터라 하면, $\boldsymbol{u}$벡터에

G_N을 곱하여 부호어 x를 생성하는데 이를 채널 합성 혹은 부호화인데, 이는 정보 벡터 $\boldsymbol{u}$벡터에 G_N을 곱하여 부호율이 1인 선형 블록 부호화를 수행하게 된다. 단, G_N은 G_2의 크로네커 곱으로 예를 들어 $n=3$일 때 다음과 같이 주어진다.

$$G_8 = G_2 \otimes G_2 \otimes G_2 = G_{RM}(8,8)$$

$$G_{RM}(8,8) = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&0&0&0&1&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}$$

단, $G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\otimes$는 크로네커 곱 연산자이다.

행렬 G_N은 리드-뮬러(Reed-Muller) 부호와 매우 밀접한 관계가 있다. 실제로, 1차 리드-뮬러 부호의 생성 행렬의 행벡터 집합이 G_N의 행벡터 집합의 부분 집합이 되며, 정방행렬인 G_N은 부호율이 1이다.

극 부호는 Arikan이 작은 부•복호화 복잡도를 가지는 임의의 이진 입력 이산 무기억 대칭 채널을 위해 제안한 부호이며, 기본적인 형태는 다음과 같은 행렬로 나타낼 수 있다.

$$W_2(\mathbf{y}_1^2|\mathbf{u}_1^2) = W(y_1|\oplus_{i=1}^2 u_i)W(y_2|u_2) \tag{1}$$

단, $\oplus_{i=1}^2 u_i$은 $u_1 \oplus u_2 = u_1 + u_2 \mod 2$를 나타낸다.

$G_2 = \mathcal{O}_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ 일 때, 입력 W_2와 출력 W^2의 함수 $W_2 : \mathbf{u}_1^2 \to \mathbf{y}_1^2$를 나타내면,

$$W_2(\mathbf{y}_1^2|\mathbf{u}_1^2) = W^2(\mathbf{y}_1^2|\mathbf{u}_1^2 G_2)$$

이는 $G_2 \cdot G_2 = I_2$를 만족한다.

비슷한 방법으로, 채널의 두 번째 단계를 결합하기

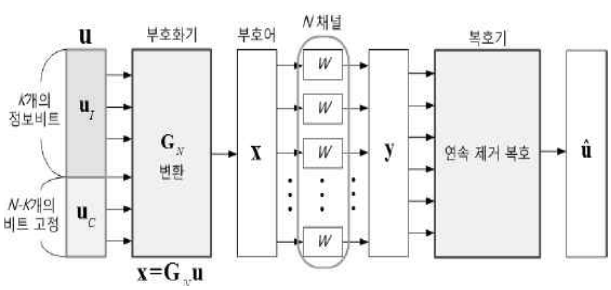


그림 1. 극 부호의 부호화 및 복호화 블록도

Fig. 1. Block diagram of Encoding and Decoding on Polar codes.

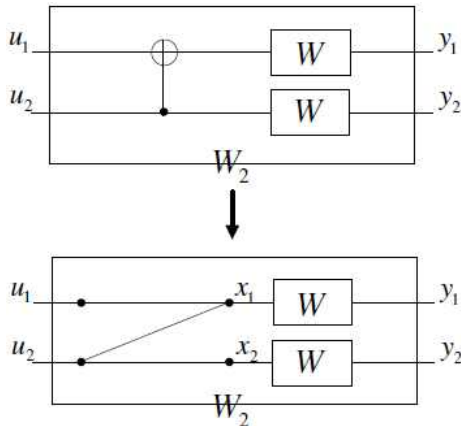


그림 2. $G_2 = \mathcal{O}_2$일 때, $W_1 = W$으로부터의 W_2를 결합하는 채널의 첫 번째 단계

Fig. 2. The first level of channel combining W_2 from two independent copies of $W_1 = W$ based on $G_2 = \mathcal{O}_2$.

위해, 입력 W_4와 출력 W^4의 함수를 $W_4 : \mathbf{u}_1^4 \to \mathbf{y}_1^4$와 같이 정의한다. 이 재귀 방정식을 통하여 식 (2)와 식 (3)을 만족할 때, 그림 2와 같이 W_2의 독립적인 두 개의 복사본을 결합하여 아래와 같은 천이확률을 갖는 채널 W_{2^2}를 구성한다.

$$\begin{aligned} W_4(\mathbf{y}_1^4|\mathbf{u}_1^4) &= W^4(\mathbf{y}_1^4|\mathbf{u}_1^4 G_4) \\ &= W_2(\mathbf{y}_1^2|\oplus_{i=1}^2 u_i, \oplus_{i=3}^4 u_i) W_2(\mathbf{y}_3^4|u_2, u_4) \end{aligned}$$

$$G_4 = R_4 G_2^{\otimes 2} = R_4 \mathcal{O}_2^{\otimes 2} = \begin{pmatrix} 1&0&0&0 \\ 1&0&1&0 \\ 1&1&0&0 \\ 1&1&1&1 \end{pmatrix} \tag{2}$$

$$R_4 = \begin{pmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \end{pmatrix} \tag{3}$$

$G_4 \cdot G_4 = I_4$이고, R_4는 $R_4(\mathbf{u}_1^4) = (u_1, u_3, u_2, u_4)$와 같은 순

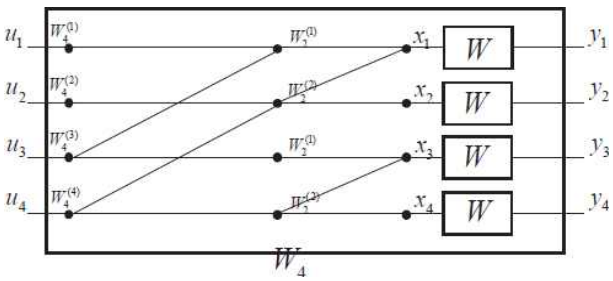


그림 3. W_2의 두 개의 독립적인 복사본을 결합하여 구성하는 채널 W_4의 두 번째 단계

Fig. 3. The second level channel combining W_4 from two independent copies of W_2.

열 행렬이다. 그림 3은 $G_4=(G_2\otimes I_2)(I_2\otimes G_2)$의 변환인 두 개의 W_2의 독립적인 두 복사본을 결합하여 구성하는 채널 W_4를 보여준다. 신호는 왼쪽에서 오른쪽으로 전달되고, 각 에지를 통하여 '0' 혹은 '1'의 신호가 전달된다. 각 노드는 왼쪽으로부터 들어오는 모든 에지의 신호를 더하고 그 결과를 오른쪽으로 전달한다. $W_8:\mathbf{u}_1^8\rightarrow\mathbf{y}_1^8$를 입력 W_8과 출력 W^8의 함수라 정의하면, 그림 4에서 볼 수 있는, W_4의 독립적인 두 복사본을 결합하여 생성하는 채널 W_8의 세 번째 단계를 얻을 수 있다. 그림 4는 $G_8=(G_4\otimes I_2)(I_4\otimes G_2)$의 변환인 W_4의 독립적인 두 복사본을 결합하여 구성하는 채널 W_8의 세 번째 단계이다. $N=2^n$일 때, $W_{N/2}$의 독립적인 두 복사본을 결합하여 채널 W_N를 구성하는 일반적인 재귀방정식의 형태는 그림 5와 같다. $GF(2)$ 위에서 합성 채널의 입력과 기본 RAW 채널의 입력의 함수 $\mathbf{u}_1^N\rightarrow\mathbf{y}_1^N$이 선형이라는 것은 자명하다. 그러므로 $G_N=R_N\mathcal{O}_2^{\otimes n}$, $\mathbf{y}_1^N\in\mathcal{Y}^N$, $\mathbf{u}_1^N\in\mathcal{X}^N$이고, n이 임의의 양의 정수일 때, 차수가 $N=2^n$인 순열 행렬 R_N과 전송율이 1인 생성 행렬 G_N로 $W_N(\mathbf{y}_1^N|\mathbf{x}_1^N)=W^N(\mathbf{y}_1^N|\mathbf{u}_1^NG_N)$ 와 같이 나타낼 수 있다.

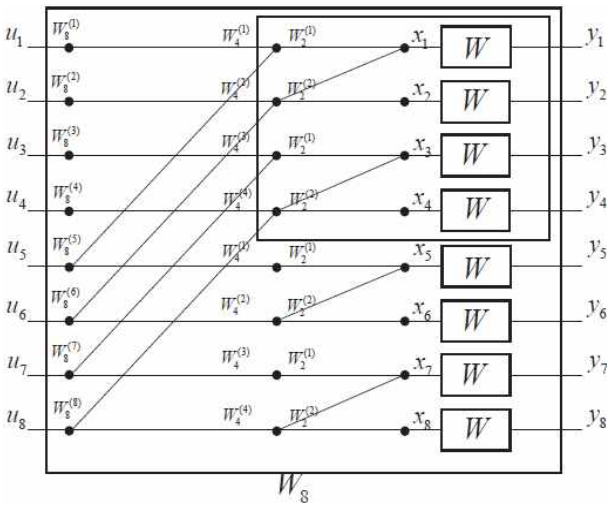


그림 4. W_4의 독립적인 두 복사본을 결합하여 생성하는 채널 W_{2^3}의 세 번째 단계

Fig. 4. The third level channel combining W_8 from two independent copies of W_4

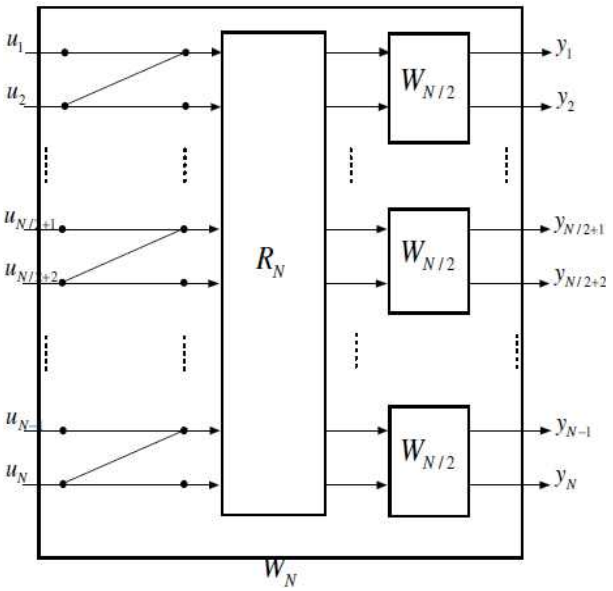


그림 5. $W_{2^{n-1}}$의 독립적인 두 복사본을 결합하여 구성한 일반적인 채널 W_{2^n}의 재귀 구성

Fig. 5. Recursive construction of generalized channel W_{2^n} from two copies of $W_{2^{n-1}}$.

Ⅲ. 블록 길이 2^n 극 부호 채널의 분리

3. 1. 채널 분리(Channel decomposition)

G_N으로 생성한 부호어 $\boldsymbol{x}$를 채널 W를 N회 사용하여 전송한다. 이 때, 채널의 수신값은 $\boldsymbol{y}$로 표시한다.

수신기에서는 수신벡터 $\boldsymbol{y}$를 통한 복호가 이루어지고, 송신 정보 벡터 $\boldsymbol{u}$의 추정치인 $\hat{\boldsymbol{u}}$를 얻을 수 있다. 이 때, 정보 벡터 $\boldsymbol{u}$에서 추정치 $\hat{\boldsymbol{u}}$까지의 가상 채널이 존재한다고 가정한다. 연속 제거 복호 알고리즘을 통한 채널 양극화로 극 부호 를 생성한다. 이미 복호된 비트는 무조건 신뢰하는 것을 전제로, u_1부터 순차적으로 복호가 진행된다. 즉, 수신 벡터 와 이미 복호가 끝난 비트 $\hat{u}_1$

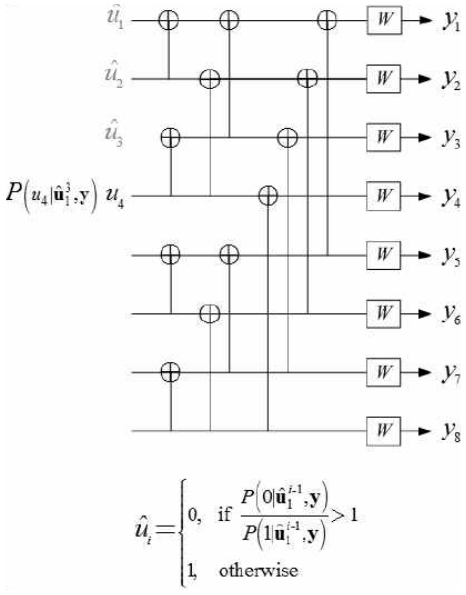


그림 6. 연속 제거 복호

Fig. 6. Succesive Cancellation Decoding.

$\sim\hat{u}_{i-1}$의 정보로 u_i의 복호가 이루어진다. 단, 이미 수신기가 알고 있는 고정된 의사 비트에 속하는 경우에는 이미 알고 있는 비트로 u_i를 복호하고, 정보 비트에 속하는 경우에는 $\hat{u}_i=\arg\max_d P(d|\hat{u}_1^{i-1},\boldsymbol{y})$와 같이 최대 사후 확률 알고리즘을 이용하여 복호가 진행된다. 단, y_a^b는 y_a에서 y_b까지의 모든 변수를 포함하는, 길이가 $b-a$인 벡터이다. 즉, y_1^N은 $\boldsymbol{y}$에 해당한다.

그림 6[20]은 $N=8$일 때의 연속 제거 복호 과정을 보여준다. 예를 들어 $P(u_4=0|\hat{u}_1^3,\boldsymbol{y})$와 $P(u_4=1|\hat{u}_1^3,\boldsymbol{y})$를 비교하여 확률이 큰 쪽으로 u_4를 복호한다. 복호기에서는 송신기와의 사전 약속에 의해 의사 비트의 위치 및 값을 모두 알고 있어야 한다. 그런데 앞의 연속 제거 복호에서는 u_5가 의사 비트이더라도 u_5의 사전 정보를 이용하지 않기에 u_4에 대한 최적의 복호라고 할 수 없다. 그러나, 고정 비트를 삽입하여 채널 양극화 현상을 유도할 수 있고, 이를 통해 극 부호를 생성할 수 있다는 의의가 있다. 이 연속 제거 복호 알고리즘은 $O(N\log N)$의 계산 복잡도를 갖는다. 앞의 복호 알고리즘에서 u_i의 복호에 필요한 가상 채널을 다음과 같이 정의할 수 있다.

$$W_N^{(i)}=W(\boldsymbol{y},\hat{u}_1^{i-1}|u_i)$$

이를 연속 제거 복호를 위한 채널의 분리이며, 각 가상 채널을 변환 부채널이다.

채널 분리라는 두 번째 단계에서 $1\le i\le N$일 때, 식 (4)와 같은 천이확률을 갖는 함수 $\mathcal{X}\to\mathcal{Y}^N\times\mathcal{X}^{i-1}$로 정의할 수 있는 결합된 채널 W_N을 이진 입력 좌표 채널 $W_N^{(i)}$의 집합으로 분리한다.

$$W_N^{(i)}(\mathbf{y}_1^N,\mathbf{u}_1^{i-1}|u_i)=\sum_{\mathbf{u}_{i+1}^N\in\mathcal{X}^{N-i}}\frac{1}{2^{N-1}}W_N(\mathbf{y}_1^N|\mathbf{u}_1^N) \tag{4}$$

단, $(\mathbf{y}_1^N,\mathbf{u}_1^{i-1})$은 주어진 입력 $u_i\in\mathcal{X}$에 대한 출력 $W_N^{(i)}$이다. 채널 분리의 성능 분석을 위해, 다음과 같이 양극화율을 계산한다.

$$Z(W_N^{(i)})=\sum_{\mathbf{y}_1^N}\sum_{\mathbf{u}_1^{i-1}}\sqrt{W_N^{(i)}(\mathbf{y}_1^N,\mathbf{u}_1^{i-1}|0)W_N^{(i)}(\mathbf{y}_1^N,\mathbf{u}_1^{i-1}|0)}$$

명제 1.[1]

$N=2^n$인 이진 이산 무기억 채널 W에서 분리 채널 $W_N^{(i)}$은 다음과 같은 의미로 양극화된다. 고정된 $\delta\in(0,1)$에 대하여 n이 무한대로 가면, $W_N^{(i)}\in(1-\delta,1]$인 지수 $i\in\{1,\cdots,N\}$의 일부분이 $I(W)$로 수렴하고, $W_N^{(i)}\in[0,\delta]$의 일부분은 '0'으로 수렴한다. 특히, 이진 소실 채널의 경우, 식 (5)와 같은 재귀 관계를 이용하여 채널 분리 값 $I(W_N^{(i)})$을 계산할 수 있다.

$$I(W_N^{(2i-1)})=I(W_{N/2}^{(i)})^2,\ I(W_N^{(2i)})=2I(W_{N/2}^{(i)})-I(W_{N/2}^{(i)})^2 \tag{5}$$

단, $I(W_1^{(1)})=I(W)$은 이진 이산 무기억 대칭 채널 W의 채널 용량이다. 주어진 이진 이산 무기억 대칭 채널 W의 예인 W^2와 $W_2^{(i)}$의 블록 채널 변환을 통하여 채널의 분리와 합성에 대한 천이확률의 관계를 유도하였고, 이는 식 (7), (8)과 같을 때, 식 (6)과 같이 정의할 수 있다.

$$\Xi_2:(W,W)\to(W_2^{(1)},W_2^{(2)}) \tag{6}$$

$$\begin{aligned}W_2^{(1)}(\mathbf{y}_1^2|u_1) &= \sum_{u_2}\frac{1}{2}W_2(\mathbf{y}_1^2|\mathbf{u}_1^2)\\ &= W_2(y_1|u_1\oplus u_2)W(y_2|u_2)\end{aligned} \tag{7}$$

$$\begin{aligned}W_2^{(2)}(\mathbf{y}_1^2,u_1|u_2) &= \frac{1}{2}W_2(\mathbf{y}_1^2|\mathbf{u}_1^2)\\ &= W_2(y_1|u_1\oplus u_2)W(y_2|u_2)\end{aligned} \tag{8}$$

$N=2^n$, $1\le i\le N$일 때, 식 (9)와 같은 결과를 얻을 수 있다.

$$\Xi_{2^n}:(W_N^{(i)},W_N^{(i)})\to(W_{2N}^{(2i-1)},W_{2N}^{(2i)}) \tag{9}$$

단,

$$\begin{aligned}&W_{2N}^{(2i-1)}(\mathbf{y}_1^{2N},\mathbf{u}_1^{2i-2}|u_{2i-1})\\ &= \sum_{u_{2i}}\frac{1}{2}W_N^{(i)}(\mathbf{y}_1^N,\mathbf{u}_{1,o}^{2i-2}\oplus\mathbf{u}_{1,e}^{2i-2}|u_{2i-1}\oplus u_{2i})\\ &\cdot W_N^{(i)}(\mathbf{y}_{N+1}^{2N},\mathbf{u}_{1,e}^{2i-2}|u_{2i})W_{2N}^{(2i)}(\mathbf{y}_1^{2N},\mathbf{u}_1^{2i-1}|u_{2i})\\ &= \frac{1}{2}W_N^{(i)}(\mathbf{y}_1^N,\mathbf{u}_{1,o}^{2i-2}\oplus\mathbf{u}_{1,e}^{2i-2}|u_{2i-1}\oplus u_{2i})\cdot W_N^{(i)}(\mathbf{y}_{N+1}^{2N},\mathbf{u}_{1,e}^{2i-2}|u_{2i})\end{aligned}$$

앞에서 살펴보았듯이, 일부 단계에서 W_N와 $W_N^{(i)}$의 일반화된 블록 채널 변환이 단일 단계의 채널 변환으로 나누어진다. 이러한 변환의 전체 집합은 $N=4$일 때, 그림 2에서 볼 수 있는 것처럼 하나의 천을 형성한다. 오른쪽에서 왼쪽으로 분석해 보면, 변환 $\Xi_2:(W,W)\to(W_2^{(1)},W_2^{(2)})$의 두 복사본으로 출발하여 나비 형태로 계속된다. 그림 4의 각 나비 형태는 오른쪽 끝점의 두 채널에 대한 일반적인 채널 변환 $\Xi_{2^i}:(W_{2^i}^{(k)},W_{2^i}^{(k)})\to(W_{2^{i+1}}^{(2k-1)},W_{2^{i+1}}^{(2k)})$을 표현할 뿐만 아니라 항상 동일하고 독립적이다. 맨 오른쪽 단계에는

$W_{2^i}^{(k)}$의 독립적인 두 복사본이 항상 존재하고, 바로 왼쪽 옆 단계에는 $W_{2^{i+1}}^{(2k)}$의 독립적인 두 복사본과 $W_{2^{i+1}}^{(2k-1)}$의 독립적인 두 복사본이 존재한다. 이와 같은 방법이 나머지 단계에서 적용된다. 맨 왼쪽 단계에는 $W_{2^n}^{(2k-1)}$의 독립적인 두 복사본과 $W_{2^n}^{(2k)}$의 독립적인 두 복사본이 존재한다. 오른쪽에서 왼쪽으로 한 단계 이동하면, 채널의 수가 두 배가 되지만, 독립적인 채널의 복사본의 수는 반으로 줄어든다.

명제 2.

$N=2^n$일 때, 이진 이산 무기억 대칭 채널 W에서의 변환 $\Xi_{2^n}:(W_N^{(i)},W_N^{(i)})\rightarrow(W_{2N}^{(2i-1)},W_{2N}^{(2i)})$은 식 (10)과 같은 의미에서 전송율이 보장되고 신뢰성이 향상된다.

$$\sum_{j=0}^{1} I(W_{2N}^{(2i-j)}) = 2I(W_N^{(i)})$$
$$\sum_{j=0}^{1} Z(W_{2N}^{(2i-j)}) \le 2Z(W_N^{(i)}) \tag{10}$$

$I(W)=0$ 혹은 $I(W)=1$일 때에만 등호가 성립하는 두 개의 삼각 부등식 $I(W_{2N}^{(2i-1)}) \le I(W_N^{(i)}) \le I(W_{2N}^{(2i)})$과 $Z(W_{2N}^{(2i-1)}) \ge Z(W_N^{(i)}) \ge Z(W_{2N}^{(2i)})$로부터 채널 분리는 전송율과 신뢰성이 중앙으로부터 멀리 떨어뜨린다. 더 나아가, 신뢰성 항은 식 (11)을 만족시킨다.

$$Z(W_{2N}^{(2i-1)}) \le 2Z(W_N^{(i)}) - Z(W_N^{(i)})^2$$
$$Z(W_{2N}^{(2i)}) = Z(W_N^{(i)})^2 \tag{11}$$

소실 확률 $Z(W)=Z(W_1^{(1)})=\epsilon$을 갖는 이진 소실 채널 W에서의 채널 소실 확률은 식 (12)를 이용하여 계산할 수 있다.

$$Z(W_N^{(2i-1)}) = 2Z(W_{N/2}^{(i)}) - Z(W_{N/2}^{(i)})^2$$
$$Z(W_N^{(2i)}) = Z(W_{N/2}^{(i)})^2 \tag{12}$$
$$\mathcal{O}_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$G_N = B_N\mathcal{O}_2^{\otimes n}$이 위와 같은 핵 행렬 $\mathcal{O}_2$에 대한 N차의 생성 행렬이고, $R_2=I_2$일 때, B_N이 식 (13)과 같은 순열 행렬일 때, 주어진 $N=2^n$에 대한 극 부호 수열의 고속 생성을 유도하기 위하여, 입력 $\mathbf{u}_1^N$ 각각을 식 (14)을 이용하여 부호화한다고 가정한다.

$$\mathbf{x}_1^N = \mathbf{u}_1^N G_N \tag{13}$$

$$B_N = R_N(I_2\otimes R_{N/2})(I_4\otimes R_{N/4})\cdots(I_{N/2}\otimes R_2) \tag{14}$$
$$R_N(\mathbf{s}_1^N) = (\mathbf{s}_{1,o}^N, \mathbf{s}_{1,e}^N)$$
$$= (s_1,\cdots,s_{2k+1},\cdots,s_{N-1},s_2\cdots,s_{2k},\cdots,s_N)$$

$N=2$일 때, $G_2=\mathcal{O}_2$이다. 연산자 R_N이 위와 같이 정의된 순열 연산일 때, 식 (15)와 같은 재귀 관계를 얻을 수 있다.

$$B_N = R_N(I_2\otimes B_{N/2}) \tag{15}$$

$R_N(G_2\otimes I_{N/2}) = (I_{N/2}\otimes G_2)R_N$은 쉽게 증명할 수 있다. 그러므로, $G_N=(I_{N/2}\otimes G_2)R_N(I_2\otimes G_{N/2})$이고 식 (16)과 같이 표현할 수 있다.

$$\begin{aligned} G_N &= (I_{N/2}\otimes G_2)R_N(I_2\otimes G_{N/2}) \\ &= R_N(G_2\otimes I_{N/2})(I_2\otimes G_{N/2}) \\ &= R_N(G_2\otimes G_{N/2}) \end{aligned} \tag{16}$$

이와 비슷하게 식 (17)도 쉽게 증명할 수 있다.

$$G_{N/2} = R_{N/2}(G_2\otimes G_{N/4}) \tag{17}$$

식 (16)과 식 (17)을 결합하여, 식 (18)과 같은 재귀 관계를 유도해 낼 수 있다.

$$\begin{aligned} G_N &= R_N(I_2\otimes R_{N/2})(G_2^{\otimes 2}\otimes G_{N/4}) \\ &= B_N G_2^{\otimes n} = B_N\mathcal{O}_2^{\otimes n} \end{aligned} \tag{18}$$

부호화 복잡도를 쉽게 설명하기 위해서, 순열 연산 B_N의 효과를 무시하면, $\mathcal{G}_N=\mathcal{O}_2^{\otimes n}$라 나타낼 수 있고, $\mathcal{G}_2=\mathcal{O}_2$이고, $\mathcal{G}_N^i = I_{2^{n-i}}\otimes\mathcal{G}_2\otimes I_{2^{i-1}}$일 때, 식 (19)와 같이 표현할 수 있다.

$$\begin{aligned} \mathcal{G}_N &= \mathcal{G}_{N/2}\otimes\mathcal{G}_2 \\ &= (I_{N/2}\cdot\mathcal{G}_{N/2})\otimes(\mathcal{G}_2\cdot I_2) \\ &= (I_{N/2}\otimes\mathcal{G}_2)\cdot(\mathcal{G}_{N/2}\otimes I_2) \\ &= \prod_{i=1}^{n}(I_{2^{n-i}}\otimes\mathcal{G}_2\otimes I_{2^{i-1}}) \\ &= \prod_{i=1}^{n}\mathcal{G}_N^i \end{aligned} \tag{19}$$

각 요소는 단계 $\mathcal{G}_N^i$로 정의할 수 있고, 생성 행렬 $\mathcal{G}_N$은 리드 -뮬러 부호에 사용된다. $\mathcal{G}_N^i$의 N개의 행 순열 연산 $P_N^r(i)$과 N개의 열 순열 연산 $P_N^c(i)$을 $P_N^r(i)\cdot P_N^c(i) = P_N^c(i)\cdot P_N^r(i)$과 같이 정의하면, $\hat{\mathcal{G}}_N^i = P_N^r(i)\cdot\mathcal{G}_N^i\cdot P_N^c(i)$[12]를 임의의 단계 $\mathcal{G}_N^i$에 대해서 얻

을 수 있고, $\mathcal{G}_2 = G_2$일 때, 식 (20)을 얻을 수 있다.

$$\begin{aligned}\hat{\mathcal{G}}_N^i &= P_N^r(i)\cdot\mathcal{G}_N^i\cdot P_N^c(i)\\ &= P_N^r(i)\cdot(I_{2^{n-i}}\otimes\mathcal{G}_2\otimes I_{2^{i-1}})\cdot P_N^c(i)\\ &= I_{2^{n-1}}\otimes\mathcal{G}_2\end{aligned} \tag{20}$$

그러므로, 극 부호 순열의 생성 행렬 G_N에 대하여 식 (21)과 같은 두 개의 행렬 P_N^r, P_N^c을 얻을 수 있다. 이는 각 단계사이에 규칙적인 연결 형태와 같은 요소를 가짐을 보여준다.

$$P_N^r G_N P_N^c = \prod_{i=1}^{n} P_N^r(i)\cdot\mathcal{G}_N^i\cdot P_N^c(i) = \prod_{i=1}^{n}\hat{G}_N^i \tag{21}$$

(예제 1)

$N=4$일 때, 직접 계산을 통해 식 (22)와 같은 결과를 얻을 수 있다.

$$\begin{aligned}\mathcal{G}_4 &= \mathcal{O}_2^{\otimes 2}\\ &= \begin{pmatrix}1&0\\1&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\1&1\end{pmatrix}\\ &= \begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{pmatrix}\end{aligned} \tag{22}$$

식 (19)를 이용하여, 식 (23)과 같이 분해할 수 있다.

$$\begin{aligned}\mathcal{G}_4 &= (I_2\otimes\mathcal{O}_2)(\mathcal{O}_2\otimes I_2)\\ &= \left[\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\1&1\end{pmatrix}\right]\cdot\left[\begin{pmatrix}1&0\\1&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\right]\\ &= \begin{pmatrix}1&0&0&0\\1&1&0&0\\0&0&1&0\\0&0&1&1\end{pmatrix}\cdot\begin{pmatrix}1&0&0&0\\0&1&0&0\\1&0&1&0\\0&1&0&1\end{pmatrix}\\ &= \begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{pmatrix}\end{aligned} \tag{23}$$

제안한 분해 방법은 극 부호 수열의 계산을 위하여 $2\log_2 4$회의 덧셈이 필요하다. $n=3$이면, 아래와 같은 행렬 $\mathcal{G}_8 = \mathcal{O}_2^{\otimes 3}$을 얻을 수 있다.

$$\begin{aligned}\mathcal{G}_8 &= \prod_{i=1}^{3}(I_{2^{3-i}}\otimes\mathcal{G}_2\otimes I_{2^{i-1}})\\ &= (I_4\otimes\mathcal{G}_2\otimes I_1)\cdot(I_2\otimes\mathcal{G}_2\otimes I_2)\cdot(I_1\otimes\mathcal{G}_2\otimes I_4)\end{aligned}$$

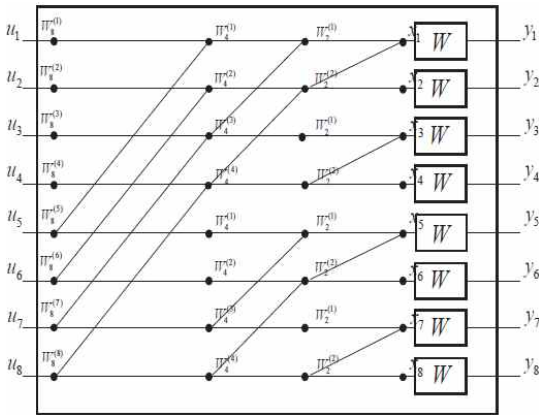


그림 7. $G_8 = (G_2\otimes I_4\otimes I_1)(I_2\otimes G_2\otimes I_2)(I_4\otimes G_2\otimes I_1)$의 고속 변환

Fig. 7. The fast transformation of G_8.

제안한 분해 방법은 그림 7과 같은 변환의 계산을 위해 12회의 덧셈이 필요하다. 이는 제안한 분해 방법은 직접 계산을 위해 $n2^n$회[1]의 연산이 필요한 기존의 기법보다 작은 복잡도를 갖는다는 것은 자명하다. $\mathcal{A}\cup\mathcal{A}^c = \{1,\cdots,N\}$, $\mathcal{A}\cap\mathcal{A}^c = \phi$와 같은 부분집합 $\mathcal{A}\subset\{1,\cdots,N\}$에 대한 부호어를 생성하기 위한 부호화 과정을 식 (24)와 같이 나타낼 수 있다.

$$\mathbf{x}_1^N = \mu_{\mathcal{A}}G_N(\mathcal{A})\oplus\mu_{\mathcal{A}^c}G_N(\mathcal{A}^c) \tag{24}$$

단, $G_N(\mathcal{A})$는 $\mathcal{A}$의 원소를 지수로 갖는 행들에 의해 형성된 G_N의 부분 행렬을 나타낸다. $\mathcal{G}_N$에 대하여 적절한 행 순열 연산 B_N을 취하여 G_N을 얻을 수 있다. 그러므로, 극 부호화 처리[18]의 간단한 방법으로 생성 행렬 $\mathcal{G}_N$을 통하여 극 부호 수열을 생성할 수 있다. $\mu_{\mathcal{A}}$는 수정하지 않고, $\mathcal{A}$와 $\mu_{\mathcal{A}^c}$를 수정하여, 생성 행렬 $\mathcal{G}_N(\mathcal{A})$을 갖는 선형 블록 부호의 동집합인 $\mathbf{x}_1^c$를 구할 수 있다. 이는 부호어 블록이라고도 부르는데, 고정 벡터 $\mu_{\mathcal{A}^c}\mathcal{G}_N(\mathcal{A}^c)$에 의해 결정된다. $\mathcal{A}$의 크기의 의해 결정되는 부호 차원이 K일 때, 매개변수 벡터 $(N,K,\mathcal{A},\mu_{\mathcal{A}^c})$를 이용하여 출력 동집합 부호 G_N을 검증할 수 있다. K/N는 부호율이다. 정보 집합을 $\mathcal{A}$, 동결 비트를 $\mu_{\mathcal{A}^c}$라 한다. $\mu_{\mathcal{A}^c} = \mathbf{0}_{\mathcal{A}^c}$일 때, 리드-뮬러 부호가 얻어진다. 예를 들어, $G_4 = B_4\mathcal{G}_4 = B_4\mathcal{O}_2^{\otimes 2}$일 때, $(4,2,\{2,4\},(1,0)$ 부호는 다음과 같은 부호기 함수를 갖는다.

$$\begin{aligned}\mathbf{x}_1^4 &= \mathbf{u}_1^4 G_4\\ &= (u_2,u_4)\begin{pmatrix}1&0&1&0\\1&1&1&1\end{pmatrix}+(1,0)\begin{pmatrix}1&0&0&0\\1&1&0&0\end{pmatrix}\end{aligned}$$

$\mathbf{x}_1^4 = (1,1,0,1)$은 정보원 블록 $(1,1)$에 대한 부호 블록

이다. 이는 정보 집합 $\mathcal{A}$의 선택에 대한 특별한 규칙에 의해 극 부호를 생성할 수 있음을 의미한다. $k=1,2,2^2,\cdots,2^{n-1}$, $Z_{1,1}=1/2$인 벡터 $Z(N)=(Z_{N,1},Z_{N,2},\cdots,Z_{N,N})$를 이용하는 채널 양극화의 신뢰성 관점에서 극 부호 수열을 생성할 수 있다. 이는 식 (25)[18]를 통하여 생성할 수 있으므로, $\mathcal{G}_N$의 행에 해당하는 집합 $\{1,\cdots,N\}$의 순열 $\pi_N=(i_1,\cdots,i_N)$을 생성할 수 있다.

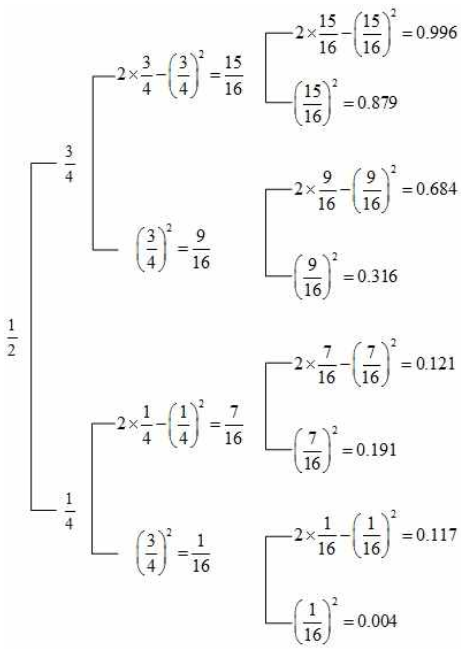
단, $1\le j<k\le N$일 때, 부등식 $Z_{N,i_j}\le Z_{N,i_k}$이 성립한다.

$$Z_{2k,j}=\begin{cases}2Z_{2k,j}-Z_{k,j}^2, & \text{for } 1\le j\le k;\\ Z_{k,j-k}^2, & \text{for } k+1\le j\le 2k\end{cases} \tag{25}$$

$\{i_1,\cdots,i_K\}\subseteq\{1,\cdots,N\}$인 지수를 갖는 행렬로 이루어진 $\mathcal{G}_N$의 부분 행렬로 (N,K) 극 부호의 생성 행렬 $\mathcal{G}_P(N,K)$을 정의할 수 있다. 이러한 부호의 생성 복잡도는 $2^{n-1}n$으로, 기존의 방법[1, 4]의 복잡도 $n2^n$보다 작음을 알 수 있다. 이는 식 (19)의 고속 알고리즘을 이용하여 쉽게 증명할 수 있다.

(예제 2)

$Z_8=(0.996,0.684,0.809,0.121,0.879,0.191,0.316,0.004)$는 행렬 $\mathcal{G}_8=\mathcal{O}_2^{\otimes 3}$을 통해 얻어지고, $\pi_8=(8,4,6,7,2,3,5,1)$를 생성한다. 그러므로, $(N,K)=(8,5)$ 부호의 생성 행렬과 동결 행렬은 다음과 같다.



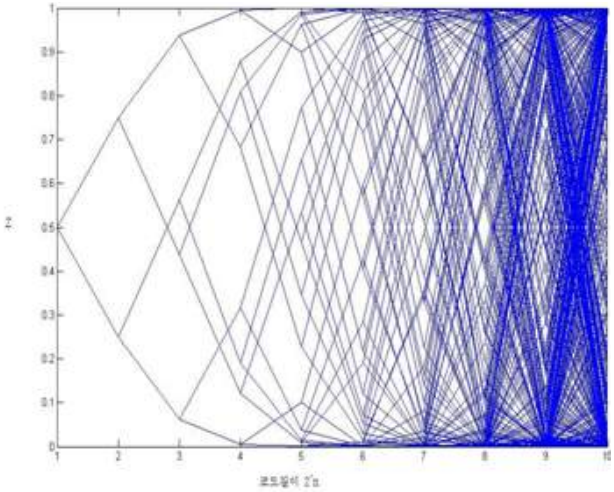


그림 8. $g_{2^n}=O_2^{\otimes n}$의 Bhattacharyya bound

Fig. 8. Bhattacharyya bound on $g_{2^n}=O_2^{\otimes n}$.

$$\begin{array}{c}\\1\\2\\3\\4\\5\\6\\7\\8\end{array}\begin{bmatrix}1&0&0&0&0&0&0&0\\1&1&0&0&0&0&0&0\\1&0&1&0&0&0&0&0\\1&1&1&1&0&0&0&0\\1&0&0&0&1&0&0&0\\1&1&0&0&1&1&0&0\\1&0&1&0&1&0&1&0\\1&1&1&1&1&1&1&1\end{bmatrix}$$

$$g_{Information}=\begin{pmatrix}1&1&0&0&0&0&0&0\\1&1&1&1&0&0&0&0\\1&1&0&0&1&1&0&0\\1&0&1&0&1&0&1&0\\1&1&1&1&1&1&1&1\end{pmatrix}$$

$$g_{Frozen}=\begin{pmatrix}1&0&0&0&0&0&0&0\\1&0&1&0&0&0&0&0\\1&0&0&0&1&0&0&0\end{pmatrix}$$

동결 블록 $(0,0,0)$을 갖는 정보원 블록 $(1,1,1,1,1)$에 대한 부호 블록은 $\mathbf{x}_1^8=(1,0,1,0,1,0,0,1)$이다.

$$L_N^{(2i-1)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-2})=\frac{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-2}|0)}{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-2}|1)}$$

$$=\frac{\frac{1}{2}\sum_{u_{2i}}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^2\hat{\mathbf{u}}_{1,j}^{2i-2}|0\oplus u_{2i})W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N,\hat{\mathbf{u}}_{1,2}^{2i-2}|u_{2i})}{\frac{1}{2}\sum_{u_{2i}}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^2\hat{\mathbf{u}}_{1,j}^{2i-2}|1\oplus u_{2i})W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N,\hat{\mathbf{u}}_{1,2}^{2i-2}|u_{2i})}$$

$$=\frac{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^2\hat{\mathbf{u}}_{1,j}^{2i-2}|0)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N,\hat{\mathbf{u}}_{1,2}^{2i-2}|0)}{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^2\hat{\mathbf{u}}_{1,j}^{2i-2}|1)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N,\hat{\mathbf{u}}_{1,2}^{2i-2}|0)}$$

$$+\frac{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|1)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|1)}{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|0)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|1)}$$

$$=\frac{L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2})L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2})+1}{L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2})+L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\hat{\mathbf{u}}_{1,2}^{2i-2})}$$

$$L_N^{(2i)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-1})=\frac{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-1}|0)}{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-1}|1)}$$

$$=\frac{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|\hat{u}_{2i-1}\oplus 0)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|0)}{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|\hat{u}_{2i-1}\oplus 1)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|1)}$$

$$=[L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2})]^{1-2\hat{u}_{2i-1}}L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}) \tag{26}$$

3. 2. 복호 알고리즘

본 절에서는, 제안한 극 부호의 복호 알고리즘에 대해 살펴본다. 앞 장에서 무작위 접근 메모리를 갖는 단일 프로세서 기계를 제안하였다. $p=2,3,4$, 블록 길이가 $N=p^n$, 매개변수가 $(N,K,\mathcal{A},\mu_{\mathcal{A}^c})$일 때, G_N-동집합 부호의 복호에 대하여 고려한다.

$\mathbf{u}_1^N=\{\mu_{\mathcal{A}}\cup\mu_{\mathcal{A}^c}\}$에서 정보원 벡터 $\mathbf{u}_1^N$은 임의의 부분 $\mu_{\mathcal{A}}$과 동결 부분 $\mu_{\mathcal{A}^c}$으로 구성된다. W_N를 가로질러 $\mathbf{u}_1^N$가 전송되면, 확률이 $W_N(\mathbf{y}_1^N|\mathbf{u}_1^N)$인 채널 출력 $\mathbf{y}_1^N$을 얻을 수 있다. 복호기는 $(\mathbf{y}_1^N,\mu_{\mathcal{A}^c})$를 검출하고, $\mathbf{u}_1^N$의 추정치 $\hat{\mathbf{u}}_1^N$를 생성한다. $i\in\mathcal{A}^c$일 때, 원소 u_i를 안다고 가정하면, i번째 결정 원소는 $\hat{u}_i=u_i$과 같다. $i\in\mathcal{A}$이라면, 전 단계 결정 원소 $\hat{\mathbf{u}}_1^{i-1}$을 받은 후 i번째 결정원소가 결정된다. $\hat{\mathbf{u}}_1^{i-1}$와 $\hat{u}_i$을 받은 즉시 복호기는 아래와 같이 우도비를 계산한다.

$$L_N^{(i)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1})=\frac{W(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1}|0)}{W(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1}|1)}$$

$$=L_N^{(2i-1)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-2})=\frac{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-2}|0)}{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-2}|1)}$$

$$=\frac{\frac{1}{2}\sum_{u_{2i}}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|0\oplus u_{2i})W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|u_{2i})}{\frac{1}{2}\sum_{u_{2i}}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|1\oplus u_{2i})W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|u_{2i})}$$

$$=\frac{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|0)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|0)}{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|1)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|0)}$$

$$+\frac{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|1)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|1)}{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|0)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|1)}$$

$$=\frac{L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2})L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2})+1}{L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2})+L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\hat{\mathbf{u}}_{1,2}^{2i-2})}$$

$$=L_N^{(2i)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-1})=\frac{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-1}|0)}{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{2i-1}|1)}$$

$$=\frac{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|\hat{u}_{2i-1}\oplus 0)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|0)}{\frac{1}{2}W_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2}|\hat{u}_{2i-1}\oplus 1)W_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}|1)}$$

$$=[L_{N/2}^{(i)}(\mathbf{y}_1^{N/2},\oplus_{j=1}^{2}\hat{\mathbf{u}}_{1,j}^{2i-2})]^{1-2\hat{u}_{2i-1}}L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^{N},\hat{\mathbf{u}}_{1,2}^{2i-2}) \tag{27}$$

또한, 다음의 모든 결정 원소에 $\hat{u}_i$가 전달될 때, 복호기는 이를 이용하여 결정 원소들을 결정한다.

$$\hat{u}_i=\begin{cases}0, & \text{if } L_N^{(i)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1})\geq 1\\ 1, & \text{otherwise.}\end{cases} \tag{28}$$

이는 추정치에 수정이 필요 없는 단일 전달 알고리즘이다. 이런 알고리즘의 복잡도는 주로 우도비를 계산하는 복잡도에 의해 결정된다.

블록 길이가 2^n인 극 부호 수열에 재귀적 공식을 적용하는 간단한 계산 방법으로 식 (26)에서 표현된 공식을 유도할 수 있다. 그러므로 블록 길이가 2^n인 수열의 우도비 계산을 블록 길이가 2^{n-1}인 두 개의 수열의 우도비 계산으로 간략화할 수 있다. 이 재귀 방정식은 이진 이산 무기억 채널 W 위에서의 블록 길이가 1이 될 때까지 계속된다.

$$L_1^{(1)}=W(y_i|0)/W(y_i|1) \tag{29}$$

Ⅳ. 모의실험

그림 9는 이진 대칭 채널에서의 오류 확률에 따른 극 부호의 비트 오류 확률을 보여준다. 이를 통해 이진 대

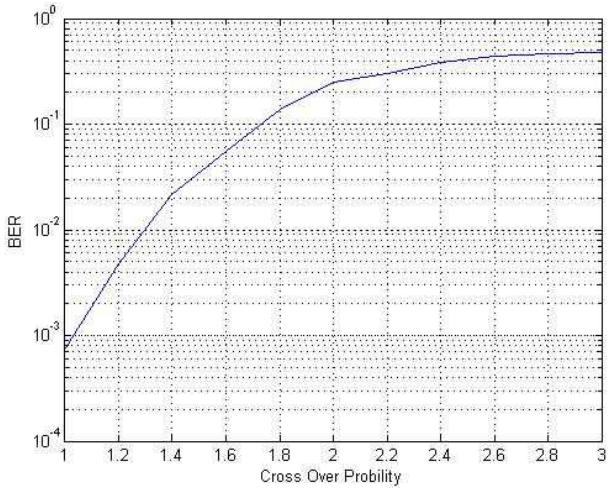


그림 9. 오류 확률에 따른 극 부호의 비트오류확률
Fig. 9. Bit error rate of Polar code for different cross over probability.

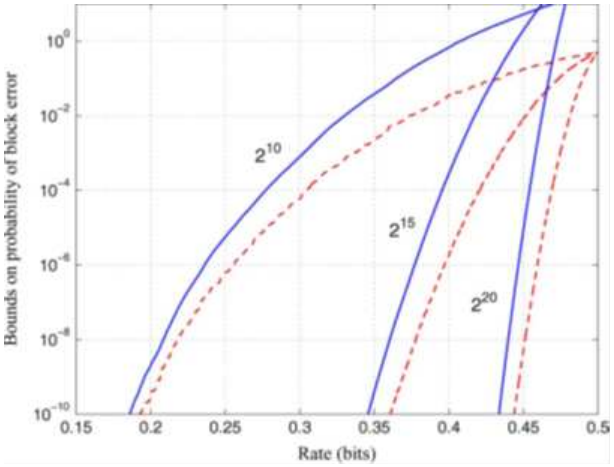


그림 10. 블록 길이와 전송율에 대한 블록 오류율[1]
Fig. 10. Block error rate for rate with various block lengths[1].

칭 채널에서의 오류 확률이 커질수록 비트 오류 확률 측면에서의 성능이 나빠짐을 알 수 있다. 즉, 나쁜 채널을 더 많이 사용할수록 극 부호의 성능이 더 나빠지고, 좋은 채널을 더 많이 사용할수록 극 부호의 성능이 더 좋아진다. 10^{-2}의 비트 오류 확률을 얻으려면, 극 부호는 이진 대칭 채널에서의 오류 확률이 0.21 이하이어야 한다. 10^{-3}의 비트 오류 확률을 얻으려면, 극 부호는 이진 대칭 채널에서의 오류 확률이 0.17 이하이어야 한다. 단, 그림 9는 보기의 편의를 위하여 오류 확률 축을 6배 늘려 나타내었다. 즉, 3은 0.5를 의미한다.

그림 10은 블록 길이 $N=2^{10},2^{15},2^{20}$일 때, 전송율에 대한 블록 오류율을 보여준다. 이를 통해 전반적으로 블록 길이가 클수록, 큰 전송율 영역에서의 블록 오류율이 작음을 알 수 있다. 이는 신뢰성 측면에서 좋은 성능을 갖는다는 것을 의미한다.

V. 결 론

본 논문에서는 Arikan이 제안했던 극 부호의 부호화 및 복호화의 대수적 식을 개선하여 이진 이산 무기억 대칭 채널에서의 극 부호의 종합적인 부호화 및 복호화의 구조와 체계에 대해 고찰했다. 이진 이산 무기억 대칭 채널 W에서 정보 비트를 전송하기에 양극화 행렬 $G_2^{\otimes n}$로 블록 길이 2^n인 극 부호를 효과적으로 구성할 수 있다.

향후 터보 부호와 같은 작은 길이의 부호에서도 오류 정정이 가능하도록 반복적 복호 알고리즘을 적용하는 방법에 대한 연구가 필요할 뿐만 아니라, q진 비선형 채널에 대한 연구도 필요하다. 기존의 불완전한 복호 알고리즘을 발전시키는 연구 또한 필요하다. 나아가 정보원 부호화, 암호 분야의 키 동의 프로토콜 등에 적용하는 방법에 대한 연구도 필요하다. 해밍 부호(1950년), 비터비 알고리즘(1969년), 터보 부호(1993년), 저밀도 패리티 검사 부호(1962년) 이후의 5세대 채널 부호화에 본 논문에서 소개한 극 부호(2008년)가 연구의 중심으로 자리 잡아 갈 것이다.

참 고 문 헌

[1] E. Arikan, “Channel Polarization : A Method for Constructing Capacity-Achieving codes for Symmetric Binary-Input Memoryless Channel”, IEEE Transactions on Information Theory, vol. 55, no.7, July 2009.
[2] R. Mori and T. Tanaka “Performance and Construction of Polar codes on Symmetric Binary-Input Memoryless Channels”, IEEE ISIT, June 2009.
[3] R. Urbanke, S. Korada and E. Sasoglu, “Polar Codes : Characterization of Exponent, Bounds and Constructions”, IEEE ISIT, June 2009.
[4] E. Arikan, “On the rate of channel polarization”, IEEE ISIT, June 2009.
[5] S. Korada, E. Sasoglu, “A Class of Transformations that Polarize Binary-Input Memoryless Channels”, IEEE ISIT, June 2009.
[6] E. Arıkan, “Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels,” IEEE Trans. Inform. Theory, July, 2008.
[7] E. Arikan, “Channel Combining and Splitting for Cutoff Rate Improvement” IEEE Transactions on Information Theory, vol. 52, no. 2, February 2006.
[8] 이문호, E. Arikan, 「Polar Jacket code」 공동 세미나, Turkey Bilkent University, August 20, 2009.
[9] T. Richardson and R. Urbanke, Modern Coding Theory. Cambridge University Press, 2008.
[10] I. Land, J. Huber, Information Combining, ser. Foundations and Trends in Comm. and Information Theory. Delft, the Netherlands: NOW, vol. 3, Nov. 2006, available online at http://www.ee.technion.ac.il/people/sason/monograph.html.
[11] 이문호, 최은지, 양재승, 박주용, “Radix 4 Polar code의 부호 및 복호”, 전자공학회논문지, 제46권

TC편, 제10호, 14-27쪽, 2009년 10월.
[12] 이문호, 실용 정보이론, 복두출판사, 2003.
[13] R. Gallager, Low-density Parity-check Codes, Cambridge, MA: M.I.T. Press, 1963.
[14] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," in Proc. IEEE Int. Conf. Comm., vol. 2, pp. 1064-1070, May, 1993.
[15] D. J. C. MacKay and R. N. Neal, "Near Shannon limit performance of low-density parity-check codes," Electron. Lett., vol. 33, pp. 457-458, March 1997.
[16] I. Krikidis, "Analysis and Optimization issues for superposition modulation in cooperative networks," IEEE Trans. Vehicular Tech., Vol.58, No.9, pp. 4837 -4847, November 2009.
[17] H. Do and S. Chung, "Linear beamforming and superposition coding with common information for the gaussian MIMO broadcast channel," IEEE Trans. Commun., vol. 57, no. 8, pp. 2484-2494, August 2009.
[18] D. Kim, F. Khan, C. V. Rensburg, Z. Pi and S. Yoon, "Superposition of broadcast and unicast in wireless cellular systems," IEEE Comm. Magazine, IEEE. vol. 46, pp. 110-117, July, 2008.
[19] Moon Ho Lee, et al, "A Novel Channel Polarization on Binary Discrete Memoryless Channels", 12th IEEE International Conference on Communications, Singapore, November 17-20th, 2010.
[20] 김상효, 김영식, 장지웅, "채널 부호화의 새로운 패러다임 : 극부호화", 전자공학회논문지, 제37권, 제4호, 20-28쪽, 2010년 4월

부 록 I

※ 식 (26)를 이용한 순차 제거 반복 알고리즘 증명

먼저, log-likelihood ratio(LLR)값은

$$L(d)=\log_e\left[\frac{P(d=0)}{P(d=1)}\right]=\log_e\left[\frac{P(d=0)}{1-P(d=0)}\right] \quad (A.1)$$

식 (A.1)의 양변을 아래와 같이 나타낼 수 있다.

$$e^{L(d)}=\left[\frac{P(d=0)}{1-P(d=0)}\right] \quad (A.2)$$

$$e^{L(d)}-e^{L(d)}P(d=0)=P(d=0) \quad (A.3)$$

$$P(d=0)[1+e^{L(d)}]=e^{L(d)} \quad (A.4)$$

$$P(d=0)=\frac{e^{L(d)}}{1+e^{L(d)}} \quad (A.5)$$

$$P(d=1)=1-P(d=0)=1-\frac{e^{L(d)}}{1+e^{L(d)}}=\frac{1}{1+e^{L(d)}} \quad (A.6)$$

$$L(d_1\oplus d_2)$$

$$=\log_e\left[\frac{P(d_1=0)P(d_2=1)+[1-P(d_1=0)][1-P(d_2=1)]}{P(d_1=0)P(d_2=0)+[1-P(d_1=0)][1-P(d_2=0)]}\right]$$

$$=\log_e\left[\frac{\left(\frac{e^{L(d_1)}}{1+e^{L(d_1)}}\right)\left(\frac{1}{1+e^{L(d_2)}}\right)+\left(\frac{1}{1+e^{L(d_1)}}\right)\left(\frac{e^{L(d_2)}}{1+e^{L(d_2)}}\right)}{\left(\frac{e^{L(d_1)}}{1+e^{L(d_1)}}\right)\left(\frac{e^{L(d_2)}}{1+e^{L(d_2)}}\right)+\left(\frac{1}{1+e^{L(d_1)}}\right)\left(\frac{1}{1+e^{L(d_2)}}\right)}\right]$$

$$=\log_e\left[\frac{\left(\frac{e^{L(d_1)}+e^{L(d_2)}}{[1+e^{L(u_1)}][1+e^{L(u_2)}]}\right)}{\left(\frac{e^{L(d_1)}e^{L(d_2)}+1}{[1+e^{L(d_1)}][1+e^{L(d_2)}]}\right)}\right] \quad (A.7)$$

$$\therefore L(d_1\boxplus d_2)\triangleq L(d_1\oplus d_2)=\log_e\left[\frac{e^{L(d_1)}+e^{L(d_2)}}{1+e^{L(d_1)}e^{L(d_2)}}\right] \quad (A.8)$$

$$e^{L(d_1\oplus u_2)}=\frac{e^{L(d_1)}+e^{L(d_2)}}{1+e^{L(d_1)}e^{L(d_2)}} \quad (A.9)$$

$$\frac{1}{e^{L(d_1\oplus d_2)}}=\frac{1}{\frac{e^{L(d_1)}+e^{L(d_2)}}{1+e^{L(d_1)}\cdot e^{L(d_2)}}} \quad (A.10)$$

$$\Rightarrow (e^{L(d_1\oplus d_2)})^{-1}=\frac{1+e^{L(d_1)}\cdot e^{L(d_2)}}{e^{L(d_1)}+e^{L(d_2)}} \quad (A.11)$$

여기서, $e^{L(d_1)}$, $e^{L(d_2)}$, $e^{L(d_1\oplus d_2)^{-1}}$을 식 (A.12) ~ 식 (A.14)와 같다고 가정하면, 식 (A.11)을 식 (A.15)와 같이 유도할 수 있다.

$$e^{L(d_1)}=L_{N/2}^{(i)}(y_1^{N/2},\hat{u}_{1,o}^{2i-2}) \quad (A.12)$$

$$e^{L(d_2)}=L_{N/2}^{(i)}(y_{N/2+1}^{N},\hat{u}_{1,e}^{2i-2}) \quad (A.13)$$

$$(e^{L(d_1\oplus d_2)})^{-1}=L_{N/2}^{(2i-1)}(y_1^{N},\hat{u}_1^{2i-2}) \quad (A.14)$$

$$L_N^{(2i-1)}(y_1^{N},\hat{u}_1^{2i-2})=\frac{1+L_{N/2}^{(i)}(y_1^{N/2},\hat{u}_{1,o}^{2i-2}\oplus\hat{u}_{1,e}^{2i-2})\cdot L_{N/2}^{(i)}(y_{N/2+1}^{N}\hat{u}_{1,e}^{2i-2})}{L_{N/2}^{(i)}(y_1^{N/2},\hat{u}_{1,o}^{2i-2})+L_{N/2}^{(i)}(y_{N/2+1}^{N},\hat{u}_{1,e}^{2i-2})} \quad (A.15)$$

식 (A.15)을 기반으로 순차 제거 반복 복호를 할 수 있다.

부 록 Ⅱ

Bhattacharyya Bound Tree에 의한 Polar Reed Muller Code 설계 : 기존 Bhattacharyya Tree Bound는 전송 손실이 있다. 따라서 그림과 같이 새롭게 수정 제안 연구한다. 즉, Fraction 함으로써 무손실이 된다.

Bhattacharyya bound는 Fraction 기법

무손실 Upper Bound 증명

Lemma: if w=11……1 00…….0 이면, d=11……1, and ℓ-d=00……0

$$X_w = (2^{2^d}-1)^{2^{l-d}}$$

다음과 같은 가정을 할 수 있다.

$$X_{w_0} = (2^{2^c}-1)^{2^{n-c+1}}$$
$$> (2^{2^{c-1}}-1)*2^{2^{n-c+1}}\left[2^{2^n+1}-(2^{2^{c-1}}-1)^{2n-c+1}\right]$$

$$(2^{2^{c-1}}+1)^{2^{n-c+1}} > 2^{2^n+1}-(2^{2^{c-1}}-1)^{2^{n-c+1}}$$
$$(2^{2^{c-1}}+1)^{2^{n-c+1}}+(2^{2^{c-1}}-1)^{2^{n-c+1}}$$
$$> 2*2^{2^n} = 2*2^{2^{n-c+1}\cdot 2^{c-1}} = 2*(2^{2^{c-1}})^{2^{n-c+1}}$$

$$\left(\frac{2^{2^{c-1}}+1}{2^{2^{c-1}}}\right)^{2^{n-c+1}}+\left(\frac{2^{2^{c-1}}-1}{2^{2^{c-1}}}\right)^{2^{n-c+1}} > 2$$

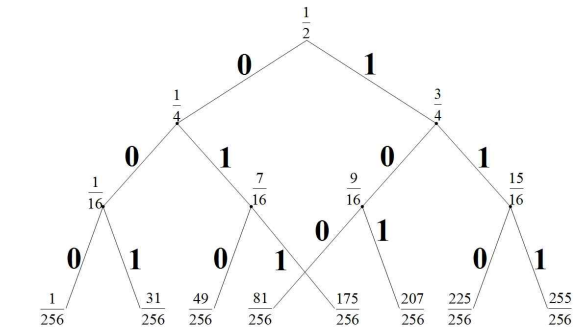
$$\left(1+\frac{1}{2^{2^{c-1}}}\right)^{2^{n-c+1}}+\left(1-\frac{1}{2^{2^{c-1}}}\right)^{2^{n-c+1}} > 2$$

위 식 양변을 $(2^{2^{c-1}}-1)^{2^{n-c+1}}$으로 나누면, $\varepsilon > 0$일 때, 위 식을 다음과 같이 쓸 수 있다.

$$\therefore\ (1+a)^{2k}+(1-a)^{2k}$$
$$= 1+\binom{2k}{1}a+\ldots+a^{2k}+1-\binom{2k}{1}a+\ldots+a^{2k} = 2+\varepsilon$$

부 록 Ⅲ

Bhattacharyya Bound Tree는 다음 그림과 같고, 이에 대한 이진 전개는 다음 표와 같다.



$l=0$	$l=1$	$l=2$	$l=3$	$l=4$
* $X_*=1$	1 $X_1=3$	11 $X_{11}=15$	111 $X_{111}=255$	1111 $X_{1111}=65535$
	0 $X_0=1$	10 $X_{10}=9$	110 $X_{110}=255$	1110 $X_{1110}=65025$
		01 $X_{01}=7$	101 $X_{101}=207$	1101 $X_{1101}=64575$
		00 $X_{00}=1$	011 $X_{011}=175$	1011 $X_{1011}=63135$
			100 $X_{100}=81$	0111 $X_{0111}=58975$
			010 $X_{010}=49$	1100 $X_{1100}=50625$
			001 $X_{001}=39$	1010 $X_{1010}=42849$
			000 $X_{000}=1$	1001 $X_{1001}=34911$
				0110 $X_{0110}=30625$
				0101 $X_{0101}=22687$
				0011 $X_{0011}=14911$
				1000 $X_{1000}=6561$
				0100 $X_{0100}=2401$
				0010 $X_{0010}=961$
				0001 $X_{0001}=511$
				0000 $X_{0000}=1$

"0" means squaring, i.e., X^2
"1"means $2X-X^2$

• Bhattacharyya bound 증명 :

같은 값을 갖는 두 개의 확률 변수 H_0, H_1에 대한 최소 오류 확률은 다음과 같다.

$$H_0 : Z \sim f_{Z|0},\ H_1 : Z \sim f_{Z|1}$$

$$P = \frac{1}{2}\int \min\{f_{Z|0}(z), f_{Z|1}(z)\}dz \quad (C.1)$$
$$= \frac{1}{2}-\frac{1}{4}\int |f_{Z|0}(z)-f_{Z|1}(z)|dz \quad (C.2)$$

$$P \le \frac{1}{2}\int \sqrt{f_{Z|0}(z)f_{Z|1}(z)}\,dz \quad (C.3)$$

식 (C.1)은 Bhattacharyya bound를 의미한다. 두 개의 확률 변수 H_0, H_1가 같은 값을 가지기에 최대 우도 결정 규칙에 의해 최소 오류 확률이 결정된다. 그러므로 다음과 같이 식 (C.1)를 유도할 수 있다.

$$P = \frac{1}{2}\int_{\{z:f_{Z|0}(z)\le f_{Z|1}(z)\}} f_{Z|0}(z)dz + \frac{1}{2}\int_{\{z:f_{Z|1}(z)< f_{Z|0}(z)\}} f_{Z|1}(z)dz$$
$$= \frac{1}{2}\int \min\{f_{Z|0}(z), f_{Z|1}(z)\}dz$$

더 나아가,

$$\begin{aligned}
&\frac{1}{2}\int |f_{Z|0}(z)-f_{Z|1}(z)|dz \\
&=\frac{1}{2}\int_{\{z:f_{Z0}(z)>f_{Z1}(z)\}}(f_{Z|0}(z)-f_{Z|1}(z))dz \\
&\quad+\frac{1}{2}\int_{\{z:f_{Z1}(z)\geq f_{Z0}(z)\}}(f_{Z|1}(z)-f_{Z|0}(z))dz \\
&=\left[\frac{1}{2}\int_{\{z:f_{Z0}(z)>f_{Z1}(z)\}}f_{Z|0}(z)dz+\frac{1}{2}\int_{\{z:f_{Z1}(z)\geq f_{Z0}(z)\}}f_{Z|1}(z)dz\right] \\
&\quad-\left[\frac{1}{2}\int_{\{z:f_{Z0}(z)>f_{Z1}(z)\}}f_{Z|1}(z)dz+\frac{1}{2}\int_{\{z:f_{Z1}(z)\geq f_{Z0}(z)\}}f_{Z|0}(z)dz\right] \\
&=(1-P)-P \\
&=1-2P
\end{aligned}$$

이를 다시 정리하면, 식 (C.2)를 얻는다.

$f_{Z|0}(z),f_{Z|1}(z)\geq 0, \min\{f_{Z|0}(z),f_{Z|1}(z)\}\leq f_{Z|0}(z),f_{Z|1}(z)$이므로, 부등식 (C.3)은 쉽게 증명할 수 있다. 따라서,

$$\min\{f_{Z|0}(z),f_{Z|1}(z)\}\leq \sqrt{f_{Z|0}(z)f_{Z|1}(z)}$$

부 록 Ⅳ

Arikan Generator matrix

$$Q_2=\begin{pmatrix}1&0\\1&1\end{pmatrix}, Q_2^2=\begin{pmatrix}1&0\\1&1\end{pmatrix}\times\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I_2=\left(Q_2^T\right)^2$$

$$Q_2Q_2^T+Q_2^TQ_2=\begin{pmatrix}1&0\\1&1\end{pmatrix}\times\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}1&1\\0&1\end{pmatrix}\times\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

$$=\begin{pmatrix}1&1\\1&0\end{pmatrix}+\begin{pmatrix}0&1\\1&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I_2(In\ GF(2))$$

$$\left(Q_2Q_2^T\right)+\left(Q_2^TQ_2\right)=\begin{pmatrix}1&1\\1&0\end{pmatrix}\times\begin{pmatrix}0&1\\1&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I_2$$

저 자 소 개

이 문 호(평생회원)-교신저자
1984년 전남대학교 전기공학과 박사
1985년～1986년 미국 미네소타대학포스트닥터
1990년 동경대학 정보통신공학과 박사
1980년 10월～2010 2월 전북대학교 전기전자컴퓨터공학부 교수
2010년 2월～현재 WCU-2 연구책임교수
<주관심분야 : 무선이동통신>

박 주 용(정회원)
1982년 전북대학교 전자공학과 학사
1994년 전북대학교 전자공학과 박사
1991년 3월～2006년 2월 서남대학교 전자공학과부 교수
2007년 3월～현재 신경대학교 인터넷정보통신학과 부교수
<주관심분야 : 무선이동통신>

이 준(학생회원)
2009년 중국 중남대 전자공학과 학사
2009년～현재 전북대학교 전자공학부 석사과정
<주관심분야 : STBC(시공간 블록부호), MIMO, OFDM, 무선통신, LDPC code, Turbo code>