2013년 8월 전자공학회 논문지 제 50 권 제 8 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 8, August 2013 http://dx.doi.org/10.5573/ieek.2013.50. 8.003

논문 2013-50-8-1

대칭용량 달성을 위한 극 퀀텀 채널 코딩

(Polar Quantum Channel Coding for Symmetric Capacity Achieving)

양 재 승*, 박 주 용**, 이 문 호***

(Jae Seung Yang, Ju Yong Park, and Moon Ho Lee©)

요 약

본 논문에서는 어떠한 이진 입력 이산 퀀텀채널(quantum channel)이 주어지더라도 대칭 용량을 달성할 수 있는 qubit(quantum bit)를 생성하기 위해, 극(polar) 큐텀 채널 코딩이라 부르는 퀀텀 채널의 결합과 분리 형태를 제시한다. 현재의 용량은 동등 확률을 갖는 임의의 qubit 입력에 따라서 결정된다. 퀀텀채널의 분극은 대칭채널이 1 에 근접하면 rate 1 로 아니면 rate 0 으로 전송하는 채널을 통해 퀀텀 데이터를 부분적으로 전송하는 퀀텀 오류정정 부호화에 아주 적합하다.

Abstract

We demonstrate a fashion of quantum channel combining and splitting, called polar quantum channel coding, to generate a quantum bit (qubit) sequence that achieves the symmetric capacity for any given binary input discrete quantum channels. The present capacity is achievable subject to input of arbitrary qubits with equal probability. The polarizing quantum channels can be well-conditioned for quantum error-correction coding, which transmits partially quantum data through some channels at rate one with the symmetric capacity near one but at rate zero through others.

Keywords : Quantum error-correction code, Polar quantum channel codes, Binary Erasure Channel

Ⅰ. 서 론

1948년 Shannon은 그의 제 1 정리에서 무기억 정보와 S(Source)가 주어졌을 때 S의 확대에 대하여 부호화를 함으로써 얼마라도 평균 부호 길이가 H(S)에 가까운 부호를 만들 수 있고 이원 대칭 채널(Binary Symmetric Channel:BSC)에서 길이가 무한대일 때 오류는 zero에 근접한다[1](부록에서 증명)고 밝혔다. 잡음 채널 코딩이론이나 소스(source) 코딩 이론과 같은 기존 정보이론의 결과는 정보원과 통신채널 모두가 무기억(memoryless)이라는 가정 하에서 얻어진 것이다. 무기억 퀀텀(quantum) 정보원의 경우는 서로 독립적인 신호들을 앞쪽으로 전송할 뿐이다. 이와 유사하게 채널에 연속적으로 가해지는 입력에 부가된 퀀텀잡음들이 서로 상관관계를 갖지 않는다면, 이때 퀀텀채널은 무기억이라고 할 수 있다. 그러한 퀀텀 기능들은 독립적이고 동일하게 분포된 랜덤 변수 시퀀스로 표시될 수 있다[2]. 그러나 실제로는 이러한 가정이 일반적으로 정당하다고 할 수 없으며, 특히 퀀텀 암호나 퀀텀 계산 네트워크에서 문제가 있다[3~5]. 최근 퀀텀 코딩의 주목적은

* 정회원, 대진대학교 컴퓨터공학과
(Department of Computer Engineering, Daejin University)
** 평생회원, 신경대학교 인터넷정보통신학과
(Department of Internet, Information & Communication, Shyngyeong University)
*** 평생회원, 전북대학교 전자정보공학부
(Division of Electronic Engineering, Chonbuk National University)
© Corresponding Author(E-mail: moonho@jbnu.ac.kr)
※ 본 연구는 한국연구재단 MEST 2013-035305의 지원으로 수행되었음.
접수일자:2012년10월17일, 수정완료일: 2013년7월23일

잡음이 있는 퀀텀 채널에 퀀텀 데이터가 전송될 때, 최대의 전송률로 세팅시키는 퀀텀 채널 용량에 근접할 코딩 기법을 디자인 하는 것이었다[6~9]. 기존의 경우와는 반대로 퀀텀 erasure 채널과 이진 대칭 퀀텀 채널(binary symmetric quantum channel)과 같은 특이한 채널을 위해, 실제 의미가 있는 퀀텀채널에 대한 그 값을 어떻게 효율적으로 계산하는지 아직도 알려져 있지 않다[2].

랜덤코딩이 채널용량에 근접하는 퀀텀코드가 존재한다는 것을 증명하기 위해 사용될지라도 이산 무기억 퀀텀채널에서 최적의 전송률을 달성하진 못 한다[10,11]. 그러한 퀀텀채널에서 전송률은 다행스럽게도 선형 퀀텀코드를 이용하여 설계하면 달성이 가능하다[12~14]. 그러나 이러한 코드들의 디코딩과정이 실제로 적용하기에는 다소 어려움이 있다. 따라서 코딩 복잡도가 낮은 qubit 시퀀스를 구성할 수 있을 뿐 아니라 증명이 가능하고 분명한 용량구조를 어떻게 만들어 낼 것인가 하는 것이 다소 어렵지만 달성해야할 목표가 되었다[15-19]. 본 논문에서는 이러한 목표를 달성하려는 시도로서 이진 이산 퀀텀채널의 높은 전송률을 달성할 수 있고 대칭용량이 가능한 퀀텀 극 부호 기법을 제시한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 복합 퀀텀 통신 시스템에서 사용되는 용어들에 대해 간략히 서술하며, Ⅲ장에서는 본 논문에서 가장 중점적으로 제시하는 내용으로서, 퀀텀채널의 결합과 분리라는 두 단계의 처리 과정으로 된 퀀텀채널을 제안한다. 서로 상관관계가 없는 퀀텀채널과 같은 부류를 위한, 퀀텀엔트로피의 고전적인 근사화 방법과 채널 분극으로부터 아이디어를 얻어 퀀텀채널 기법이 나오게 되었다. Ⅳ장은 퀀텀채널 분극을 통해 퀀텀 극 부호 설계에 대해 서술하며 Ⅴ장에서 모의실험을 제시하고, 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 이산 퀀텀채널(Discrete Quantum Channel)의 파라미터

단일 qubit $|u\rangle = p_0|0\rangle + p_1|1\rangle$ 은 2차원 Hilbert 공간 $H = \mathbb{C}^2$ 이다. 여기서 p_0 와 p_1 은 $|p_0|^2 + |p_1|^2 = 1$ 의 조건을 만족한다. 2^n 차원 공간 $H_n = H^{\otimes n}$ 에서 다중 qubit 상태 $|\psi\rangle$ 의 전송에 대해 생각해 보자. Hilbert 공간 H의 베이시스(basis)는 고정($\mathcal{B} = \{|0\rangle, |1\rangle\}$)한다. 퀀텀 오류 연산의 베이시스는 $\{E_{ij} = X^i Z^j\}$ 로 표시하며, 여기서 $X|i\rangle = |i+1 \bmod 2\rangle$ 이고 $Z|j\rangle = (-1)^j|j\rangle$, $\forall i, j \in \{0,1\}$ 이다. 이산 퀀텀채널 $\mathcal{E}$ 은 $A_u = \Sigma_{v \in F4} a_{u,v} E_v$ 형태의 임의의 연산집합으로 정의 되며, 여기서 복소수벡터 $a_u = (a_{u,v}, v \in F_4)$ 는 $F_4 = \{0,1,2,3\}$ 에서 확률분포로 정의된다. 이를 확인하기 위하여 $\mathcal{E}$ 의 합 연산을 행하는 A_u연산 집합이 다음과 같이 표현될 수 있다고 가정한다.

$$A_u = a_u I + \sum_{v}^{3} a_{u,v}\sigma_v \tag{1}$$

여기서 $\sigma_v \in \{\sigma_x, \sigma_z, \sigma_y\}$ 는 Pauli 행렬이다. 연산 A_u 즉, $\forall u \in F_4$ 는 완전조건 $\Sigma_u A_u^{\dagger} A_u = I$ 을 만족한다[2].

$\mathcal{E}: \mathcal{U} \mapsto \mathrm{T}$ 은 입력이 $\mathcal{U}$, 출력이 T인 이산 퀀텀채널을 나타내며, 이는 $|u\rangle \in \mathcal{U}$ 와 $|t\rangle \in \mathcal{T}$ 인 채널 전환확률 $\varepsilon(t|u)$을 의미한다. 입력 qubit $\mathcal{U}$ 는 항상 $\{|u_0\rangle, |u_1\rangle\}$ 내에 있으나, 출력 qubit $\mathcal{T}$ 와 전환확률 $\varepsilon(t|u)$은 특정한 제한이 없으며, 여기서 $|u_0\rangle$ 과 $|u_1\rangle$ 은 서로 직교상태 즉, $\langle u_0|u_1\rangle = 0$이다. 따라서 이 전환 확률은 기호 $\varepsilon^N : U^N \mapsto T^N$ 를 사용하여 N개의 동등하고 독립적인 채널의 조합을 나타내며, 전환확률은 다음과 같이 나타낸다.

$$\mathcal{E}^N(t|u) = \prod_{i=1}^{N} \mathcal{E}(t_i|u_i) \tag{2}$$

단일 qubit 채널 $\mathcal{E}$ 에 대해 전송률과 신뢰도를 측정하기 위해 두 개의 파라미터를 정의하게 되는데, 즉 식 (3)과 같은 대칭용량[20]과 식 (4)로 표시되는 Bhattacharyya 파라미터[21]이다.

$$\chi(\mathcal{E}) = \sum_{|t\rangle \in \mathrm{T}} \sum_{|u\rangle \in U} \frac{1}{2}\mathcal{E}(t|u) \log \frac{\mathcal{E}(t|u)}{\frac{1}{2}\mathcal{E}(t|u_0) + \frac{1}{2}\mathcal{E}(t|u_1)} \tag{3}$$

$$Z(\mathcal{E}) = \sum_{|t\rangle \in \mathrm{T}} \sqrt{\mathcal{E}(t|u_o)\mathcal{E}(t|u_1)} \tag{4}$$

파라미터 $\chi(\mathcal{E})$ 는 동등 확률을 갖는 입력 $\mathcal{U}$ 가 주어

진 퀀텀채널 $\mathcal{E}$ 에서 신뢰할만한 통신이 가능할 때의 전송률을 나타내고, 파라미터 $Z(\mathcal{E})$ 은 최대우도(maximum-likelihood) 결정 퀀텀 오류 확률의 최상위 한계를 의미한다.

보다 쉬운 이해를 위해, 지금부터 N qubit 상태 $|a_1 \cdots a_N\rangle$ 을 간략히 a_i^N 으로 나타낸다. a_i^j 표현은 $1 \le i \le j \le N$ 인 그의 sub-state $|a_i \cdots a_j\rangle$ 을 의미한다. $A = \{i_1, \ldots, i_A\} \subseteq 1, \ldots, N$가 주어지면 일반적인 sub-state $|a_{i_1} \cdots a_{i_A}\rangle$ 를 a_A 로 간략히 나타낸다. $\mathsf{a}_{1,o}^j$ 는 홀수 인덱스 $\{a_k : 1 \le k \le j, k = 2l-1, l \in \mathbb{Z}\}$ 을 갖는 sub-state를 나타내고, $\mathsf{a}_{1,e}^j$ 는 짝수 인덱스 $\{a_k : 1 \le k \le j, k = 2l, l \in \mathbb{Z}\}$ 을 갖는 sub-state를 나타낸다.

Ⅲ. 다중 Quantum 채널의 분극

퀀텀 채널 분극은 N개의 독립된 퀀텀채널 $\mathcal{E}$ 을 기반으로 N개의 연속되는 퀀텀채널 $\{\mathcal{E}_i^N : 1 \le i \le N\}$ 과 관계된 또 다른 집합을 만들어내는 작용이라 할 수 있다. N이 증가함에 따라 대칭용량 $\chi(\mathcal{E}_i^N)$ 은 인덱스 i가 거의 0 에 가까워질 만큼 작아지면 1로 향하거나 0으로 향한다는 의미에서 분극이 되는 효과를 보여준다. 이러한 연산은 퀀텀채널의 결합과 분리라는 두 가지 단계를 통해 수행된다.

3. 1. 퀀텀채널 결합 단계 (Quantum Channel Combining Phase)

이 단계에서는 N개의 동일한 독립 채널 $\mathcal{E}$ 들이 반복적인 방법으로 결합되며, $N = 2^n$ 인 다중레벨 결합 퀀텀채널 $\mathcal{E}^N$ 이 결합되고, 이때 n은 양의 정수이다. 즉, 첫 번째 레벨(기본 레벨)채널 $\mathcal{E}^1 = \mathcal{E}$ 부터 결합이 시작된다.

두 번째 레벨채널 $\mathcal{E}^2$ 에서는 두 개의 $\mathcal{E}$ 복사본이 다음과 같이 주어지는 전환확률을 가지고 서로 결합한다.

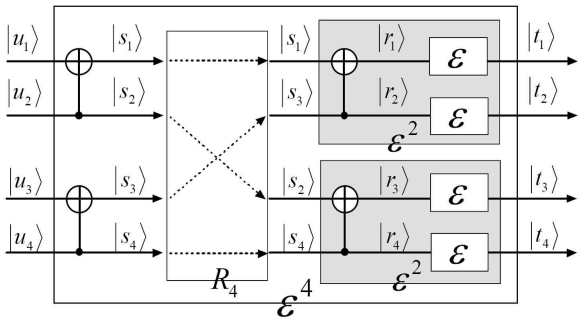

그림 1. 두 개의 하위레벨 ε 과 ε^2 퀀텀채널을 결합하여 처리한 ε^4 다중레벨 퀀텀채널의 처리과정

Fig. 1. The processing of the multi-level-combined channel ε^4 based on two lower-level combined quantum channels ε and ε^2.

$$\mathcal{E}^2\left(t_1^2 \middle| u_1^2\right) = \mathcal{E}\left(t_1 \middle| u_1 \oplus u_2\right)\mathcal{E}\left(t_2 \middle| u_2\right) \tag{5}$$

그림 1에 보인 바와 같이 $\mathcal{E}^2$ 의 입력으로부터 $\mathcal{E}$ 의 입력으로의 변환 연산 $|u_1^2\rangle \mapsto |r_1^2\rangle$ 은 CNOT 게이트 $C_{u2,u1}$ 에 의해 $|r_1^2\rangle = C_{u2,u1}|u_1^2\rangle = |u_1 \oplus u_2, u_2\rangle$ 와 같이 나타낼 수 있고, 여기서 $|u_1\rangle$ 은 target qubit이고 $|u_2\rangle$ 는 제어 qubit이다.

이와 유사한 방법으로 다음 레벨 채널 $\mathcal{E}^4$ 는 식 (6)과 같은 전환확률로, 반복적인 방법을 통해 2개의 독립적인 채널 $\mathcal{E}^2$ 과 결합될 수 있다.

$$\varepsilon^4\left(t_1^4 \middle| u_1^4\right) = \varepsilon^2\left(t_1^2 \middle| u_1 \oplus u_2, u_3 \oplus u_4\right) \cdot \varepsilon^2\left(t_3^4 \middle| u_2, u_4\right) \tag{6}$$

그림 1에서 매핑(mapping) R_4는 $|s_1 s_2 s_3 s_4\rangle$ 에서 $|s_1 s_3 s_2 s_4\rangle$ 로 매핑 시키는 치환 연산이다. $\mathcal{E}^4$ 의 입력으로 부터 입력 $\mathcal{E}$ 으로의 변환 연산 $|u_1^4\rangle \mapsto |r_1^4\rangle$ 은 다음과 같이 주어질 수 있다.

$$|r_1^4\rangle = R_4\left(C_{u2,u1} \otimes C_{u4,u3}\right)|t_1^4\rangle = R_4 G_4 |t_1^4\rangle \tag{7}$$

여기서 G_4는 식 (8)과 같은 2차 분극 행렬이고

$$G_4 = G_2^{\otimes 2} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{8}$$

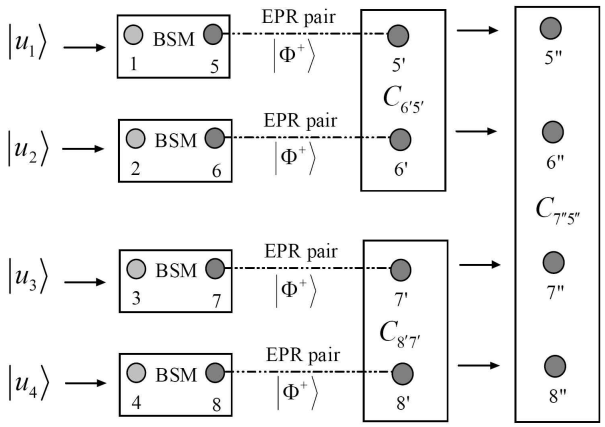

그림 2. 3 개의 CNOT 게이트를 사용한 4 qubit 입력으로 퀀텀 분극 과정의 퀀텀 회로

Fig. 2. Quantum circuit of the quantum polarizing processes with inputs of four qubits using three CNOT gates.

$\otimes$ 는 Keronecker 곱을 의미한다[22].

그림 2는 3 개의 CNOT 게이트를 사용한 4-qubit 입력의 퀀텀 분극 과정의 퀀텀 회로를 보여주고 있다. 2개의 target qubit $|u_j\rangle, j\in\{1,3\}$ 으로 구성되는 입력 qubit와 2개의 제어 qubit $|u_i\rangle$, $i\in\{2,4\}$ 은 임의로 선택이 가능하다. 8개의 광양자가 혼재된 클러스터 state $|\varpi\rangle$ 는 4 Bell state $|\Phi^+_{kk'}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, $\forall k\in\{5,6,7,8\}$ 로부터 생성되며, 여기서 $C_{(i+4)'(i+3)'}$ 은 광양자 $(i+4)'$&$(i+3)'$ 에서 실행될 것이고, $C_{7''5''}$ 은 생성된 광양자 $7''$ & $5''$ 에서 실행 되게 된다. 다시 말해서 $|\varpi\rangle=C_{7''5''}C_{8'7'}C_{6'5'}\otimes_{k=5}^{8}|\Phi^+\rangle_{kk'}$ 이 얻어져 퀀텀채널의 분극을 실현시키는데 이용된다. 그 다음 BSM(Bell state measurement)들이 4쌍의 광양자 $(k-4)\,k$ 에서 각각 실행된다. 표 1에 보인 BSM의 결과에 따라 Pauli 연산 $\{I,\sigma_x,\sigma_z,\sigma_y\}$ 은 $|\varpi\rangle$ 의 남아있는 qubit k'에 각각 적용되며, 결국 퀀텀 분극 과정에서 결합채널 ε^4 의 출력을 얻어내게 된다.

3. 2. 퀀텀채널 분리 단계 (Quantum Channel Splitting Phase)

이 단계에서는 $1\le i\le N$에 대해 앞에서 결합했던 n-qubit 퀀텀채널 ε^N 을 N개의 연속되는 채널 ε_i^N 의 set로 분리한다. 즉, 분리 연산은 다음과 같이 설정할 수 있다.

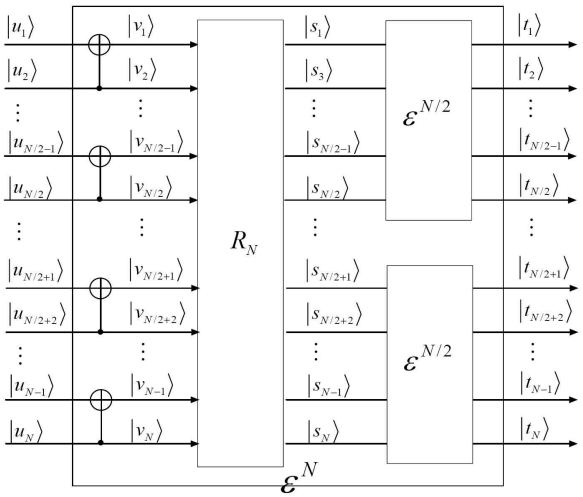

그림 3. 2개의 독립된 하위결합채널 $\varepsilon^{N/2}$ 을 기반으로 퀀텀채널의 분극과정에서 결합 퀀텀 채널 ε^N 의 반복 구조

Fig. 3. A recursive construction of the combined quantum channel ε^N in the process of the quantum channel polarization based on two independent low-combined channels $\varepsilon^{N/2}$.

$$\mathcal{E}_1^N:\mathcal{U}\mapsto \mathrm{T}^N\times\mathcal{U}^{i-1} \tag{9}$$

이때 전환확률은 다음과 같이 주어지며,

$$\mathcal{E}_i^N\left(t_1^N,u_1^{i-1}\middle|u_i\right)=\sum_{|u_{i+1}^N\rangle\in\mathcal{U}^{n-i}}\frac{1}{2^{N-1}}\mathcal{E}^N\left(t_1^N\middle|u_1^N\right) \tag{10}$$

여기서 $\left(t_1^N,u_1^{i-1}\right)$ 은 입력조건 $|u_i\rangle\in\mathcal{U}$ 에 대한 출력 $\mathcal{E}_i^N$ 을 나타낸다.

일예로, 주어진 채널 $\mathcal{E}$ 에 대해 2-레벨 결합 퀀텀 채널 $\mathcal{E}^2$ 은 $\{|u_1\rangle,|u_2\rangle\}=\{|0\rangle,|1\rangle\}$ 인 경우 두 개의 연속되는 채널 $\mathcal{E}_i^2$, $i\in\{1,2\}$ 로 분리된다. 식 (5)의 결합채널에 의해 다음과 같은 2개의 분리채널 $\mathcal{E}_1^2$ 과 $\mathcal{E}_2^2$ 을 각각 얻을 수 있다.

$$\begin{aligned}\varepsilon_1^2\left(t_1^2\middle|u_1\right)&=\sum_{u_2=0}^{1}\frac{1}{2}\varepsilon^2\left(t_1^2\middle|u_1^2\right)\\&=\sum_{u_2=0}^{1}\frac{1}{2}\varepsilon\left(t_1^2\middle|u_1\oplus u_2\right)\varepsilon\left(t_2\middle|u_2\right)\end{aligned} \tag{11}$$

$$\mathcal{E}_2^2(t_1^2, u_1|u_2) = \frac{1}{2}\mathcal{E}^2\left(t_1^2|u_1^2\right)$$
$$= \frac{1}{2}\mathcal{E}\left(t_1^2|u_1 \oplus u_2\right)\mathcal{E}\left(t_2|u_2\right) \quad (12)$$

일반적으로 임의의 수 $N=2^n$ 에 대해 식 (14),(15)와 같이 주어지는 연속적인 방법으로 하위레벨 분리 채널 $\mathcal{E}_i^N$, $1 \le i \le N$에 근거해 두 개의 분리채널 $\mathcal{E}_{2i-1}^{2N}$ 과 $\mathcal{E}_{2i}^{2N}$ 이 얻어 진다.

$$\mathcal{E}_{2i-1}^{2N}\left(t_1^{2N}, u_1^{2i-2}|u_{2i-1}\right) = \sum_{u_{2i}=0}^{1}\frac{1}{2}\mathcal{E}_i^N\left(t_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2}|u_{2i+1} \oplus u_{2i}\right)$$
$$\cdot\mathcal{E}_i^N\left(t_{2N+1}^{2N}, u_{1,e}^{2i-2}|u_{2i}\right) \quad (13)$$

$$\mathcal{E}_{2i}^{2N}\left(t_1^{2N}, u_1^{2i-2}|u_{2i}\right) = \frac{1}{2}\mathcal{E}_i^N\left(t_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2}|u_{2i+1} \oplus u_{2i}\right)$$
$$\cdot\mathcal{E}_i^N\left(t_{2N+1}^{2N}, u_{1,e}^{2i-2}|u_{2i}\right) \quad (14)$$

$\left|t_1^N\right\rangle$과 이전의 $\left|u_1^{i-1}\right\rangle$을 관찰한 후 i-번째 결정 요소가 i-번째 입력 $|u_i\rangle$을 평가하는 연속적인 제거 디코더에 대해, 분리채널 $\mathcal{E}_i^N$은 i-번째 결정입력 $|u_i\rangle$에 의해 결정된 효율적인 퀀텀채널이라는 것을 알 필요가 있다. 분리채널 $\mathcal{E}_i^N$의 분극 효과에 대해 말하자면 다음과 같은 대칭용량에 대한 흥미 있는 결과를 얻을 수 있다.

모든 채널 $\mathcal{E}$ 과 모든 고정된 $\delta \in (0,1)$에 대해, $N=2^n$이 ∞를 향해 감에 따라 $\chi(\mathcal{E}_i^N) \in (1-\delta, 1]$, $\chi(\mathcal{E}_i^N) \mapsto \chi(\mathcal{E})$인 $\{i \in \mathcal{A} \subseteq \{1,2,\ldots,N\}\}$의 인덱스가 일부 있고, $\chi(\mathcal{E}_j^N) \in [0,\delta]$, $\chi(\mathcal{E}_i^N) \mapsto \chi(\mathcal{E})$인 $\{j \in \mathrm{B} \subseteq \{1,2,\ldots,N\}\}$의 또 다른 인덱스가 있다. 즉, $N=2^n$이 ∞를 향해 감에 따라 대칭용량 $\chi(\mathcal{E}_i^N)$과 $\chi(\mathcal{E}_j^N)$은 각각 $\chi(\mathcal{E})$ 과 $1-\chi(\mathcal{E})$을 향해 가도록 하는 $i \in \mathcal{A}$, $j \in B$ 인덱스들이 있음을 의미한다.

$\chi(\mathcal{E}_i^N)$의 값이 i의 중간영역에서 엉뚱한 행위를 한다는 것을 발견하게 된다. 이와 같은 행위를 하는 것은 다음과 같은 의미를 가지고 있다. 즉, $\chi(\mathcal{E}) > r > 0$ 인 어떠한 이산 채널이든 집합$\mathcal{A}_N \subset \{1,\ldots,N\}$의 시퀀스가 있어서 $N=2^n$이 ∞를 향해 감에 따라 모든 $i \in \mathcal{A}_N$의 최대우도 결정 퀀텀 오류 확률 $Z(\mathcal{E}_i^N)$의 최상위 한계가 0을 향한다는 의미이다.

Ⅳ. Polar Quantum 코드의 구성

이 장에서는 이산 퀀텀채널의 분극 효과를 이용한 대칭용량을 달성할 수 있는 극 퀀텀 코드 구성법을 제시한다. 극 퀀텀 부호를 구성하게 된 동기는 각 좌표채널을 개별적으로 얻고, $N=2^n$ 이 ∞를 향해 감에 따라 $Z(\mathcal{E}_i^N)$ 값이 0 에 접근하는 채널을 통해 데이터를 전송하는 부호화 시스템을 만들려는 것이다.

$N=2^n$ 값이 주어지면 입력은 다음과 같은 방법으로 부호화 될 수 있다.

$$\left|\mathrm{r}_1^N\right\rangle = G_N\left|\mathrm{u}_1^N\right\rangle \quad (15)$$

여기서 G_N 은 N차 생성행렬이다. $\{1,\ldots,N\}$의 임의의 subset에 대해 식 (15)는 다음과 같이 다시 쓸 수 있다.

$$\left|\mathrm{r}_1^N\right\rangle = G_N(\mathcal{A})\left|\mathrm{u}_{\mathcal{A}}\right\rangle \oplus G_N\left(\mathcal{A}^C\right)\left|\mathrm{u}_{\mathcal{A}^C}\right\rangle \quad (16)$$

여기서 $G_N(\mathcal{A})$은 $\mathcal{A}$의 인덱스 행에 의해 형성된 G_N의 sub-matrix를 나타내고, 반면 $\mathcal{A}^c$는 $\mathcal{A} \cap \mathcal{A}^C = \phi$와 $\mathcal{A} \cup \mathcal{A}^C = \{1,\ldots,N\}$이 되도록 $\{1,\ldots,N\}$의 subset이다.

극 퀀텀 코드를 만들어내기 위해서 파라미터 $\mathcal{A}$와 $\left|u_{\mathcal{A}^c}\right\rangle$는 고정 되나 $\left|u_{\mathcal{A}}\right\rangle$는 자유변수로 남게 되고, state $\left|u_{\mathcal{A}}\right\rangle$로부터 state $\left|r_1^N\right\rangle$로 매핑이 되고나면, 이것은 실제로 coset 퀀텀코드가 된다. 즉, 고정된 퀀텀 state $G_N(\mathcal{A}^c)\left|u_{\mathcal{A}^c}\right\rangle$에 의해 결정된 생성행렬이 $G_N(\mathcal{A})$인 선형 퀀텀 블록 코드의 coset이다. 이러한 부류의 퀀텀 코드는 집단인 G_N-coset 퀀텀코드로 간주되게 된다. 개별적인 G_N-coset 퀀텀코드는 $\left((N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C})\right)$와 같이 표시되며, 여기서 K는 $\mathcal{A}$의 사이즈에 의해 정해지는 코딩 dimension이다. 집합 $\mathcal{A}$는 데이터 qubit로 $\left|u_{\mathcal{A}^c}\right\rangle$는 frozen qubit로 간주된다.

퀀텀 디코더를 연속적으로 제거시키기 위해서는 G_N-coset 퀀텀코드 $\left((N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C})\right)$을 고려해볼 수 있다.

N-qubit state $|u_1^N\rangle$가 출력이 $|t_1^N\rangle$인 $\mathcal{E}^N$으로 전송될 $|r_1^N\rangle$로 코딩되는 것을 가정하면, $\mathcal{A}$과 $|u_{\mathcal{A}^c}\rangle$ 및 $|t_1^N\rangle$에 대한 정보에 따라 $|u_1^N\rangle$에서 훌륭한 추정 state $|\tilde{u}_1^N\rangle$을 만들어내는 것이 디코더의 할 일이다.

연속적인 제거 퀀텀 디코더에 대해 코딩 결과가 주어지게 된다. $1 \le i \le N$의 경우 퀀텀 디코더를 이용해 식 (18)과 같이 주어지는 그의 결정상태 $|\tilde{u}_1^N\rangle$가 만들어진다.

$$|\tilde{u}_i\rangle = \begin{cases} |u_i\rangle, & \text{if } i \in \mathcal{A}^C \\ \left|h_i\left(\mathrm{t}_1^N, \tilde{\mathrm{u}}_1^{i-1}\right)\right\rangle, & \text{if } i \in \mathcal{A} \end{cases} \quad (17)$$

여기서 $|h_i\rangle$는 다음과 같이 계산되는 결정 qubit이다.

$$\left|h_i\left(\mathrm{t}_1^N, \tilde{\mathrm{u}}_1^{i-1}\right)\right\rangle = \begin{cases} |0\rangle, & \text{if } \dfrac{\varepsilon_1^N\left(\mathrm{t}_1^N, \mathrm{u}_1^{i-1}|0\right)}{\varepsilon_1^N\left(\mathrm{t}_1^N, \mathrm{u}_1^{i-1}|1\right)} \ge 1 \\ |1\rangle, & \text{otherwise} \end{cases} \quad (18)$$

이것은 퀀텀 오류의 필요충분조건이 $|\tilde{\mathrm{u}}_{\mathcal{A}}\rangle \neq |\mathrm{u}_{\mathcal{A}}\rangle$, $\forall i \in \mathcal{A}$이라는 것이다.

코드 $((N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C}))$의 성능을 분석하기 위해 그 다음에 해야 할 일은 블록 퀀텀 에러의 확률 P_e를 정의하는 것이다. 만약에 각 state $|u_{\mathcal{A}}\rangle$가 2^{-K}의 확률로 전송되고 앞에서 언급한 디코더를 통해 디코딩 된다면, P_e의 확률은 다음과 같이 계산될 수 있다.

$$P_e\left(N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C}\right) = \sum_{\mathrm{u}_{\mathcal{A}}} \frac{1}{2^K} \sum_{\mathrm{t}_1^N : |\mathrm{u}_1^N(\mathrm{t}_1^N)\rangle \neq |\mathrm{u}_1^N\rangle} \mathcal{E}^N\left(\mathrm{t}_1^N|\mathrm{u}_1^N\right) \quad (19)$$

$\mathrm{u}_{\mathcal{A}^C}$의 모든 선택에 대해 확률 $P_e(N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C})$의 평균값은 식 (21)과 같이 주어질 수 있다.

$$P_e(N,K,\mathcal{A}) = \sum_{\mathrm{u}_{\mathcal{A}^C}} \frac{1}{2^{N-k}} P_e(N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C}) \quad (20)$$

따라서 이 확률의 upper-bound 가 달성된다.

퀀텀채널 $\mathcal{E}$과 $((N,K,\mathcal{A}))$의 선택에 대해 다음과 같은 frozen qubit $|u_{\mathcal{A}^c}\rangle$가 있다.

$$P_e(N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C}) \le \sum_{i\in\mathcal{A}} Z\left(\mathcal{E}_1^N\right) \quad (21)$$

$\Sigma_{i\in\mathcal{A}} Z\left(\mathcal{E}_j^N\right)$을 최소화 시키기 위해 $\{1,\ldots,N\}$의 모든 K subset 중에서 $\mathcal{A}$의 선택을 의미한다. 이 아이디어의 기인하여 극 퀀텀 코드의 정의를 내리게 된다.

정의 1 (Polar Quantum Code) : 주어진 채널 $\mathcal{E}$에 대해 파라미터가 $P_e(N,K,\mathcal{A},\mathrm{u}_{\mathcal{A}^C})$인 G_N-coset 코드를, 만약 set $\mathcal{A}$와 관련된 K-qubit 퀀텀 데이터 state가 $i \in \mathcal{A}$와 $j \in \mathcal{A}^c$에 대해 각각 $Z\left(\mathcal{E}_1^N\right) \le Z\left(\mathcal{E}_j^N\right)$이 될 수 있도록 $\{1,\ldots,N\}$의 K-element set으로 선택될 수 있다면, 극 퀀텀 코드라 부른다.

실제로 극 퀀텀 코드의 생성은, 다중레벨 결합 채널 $\mathcal{E}^N$과 그의 해당 분리 채널 $\mathcal{E}_i^N$을 이용하여 채널을 특별하게 설계하는 것이다. 한 이산 퀀텀 채널을 위한 극 퀀텀 코드는 다른 이산 채널에 대해서는 polar case가 아닐 수도 있으며, 여기서 현재의 polar 퀀텀 코드는 주어진 채널 $\mathcal{E}$에 대해 대칭용량 $\chi(\mathcal{E})$을 달성하게 된다. 이것은 polar 퀀텀 코드가 잡음이 없는 채널이나 순수 잡음채널로 접근함을 의미하며, 즉, 무 잡음이 되는 일련의 채널은 N이 무한대로 접근함에 따라 $\chi(\mathcal{E})$에 수렴 한다는 뜻이다.

극 퀀텀 코드와 퀀텀 에러 정정 코드의 관계를 보기 위해, 퀀텀 채널 분극을 통해 퀀텀 에러 정정 코드의 구조를 제시한다. 퀀텀 오류 정정 코드로서 자격을 받게 되면, 안정화기 $\mathcal{H} = (H_x|H_z)$로서 최고의 평가를 받을 수 있는 성질을 갖춘 것으로 볼 수 있다[10-12]. 안정화기 $\mathcal{H}$는 $H_x \cdot G_Z^T + H_z \cdot G_x^T = 0 \mod 2$를 만족하는 생성행렬 $\mathcal{G} = (G_x|G_z)$와 연계되어 있다. 퀀텀 에러 정정 코드가 만족해야할 안정화기의 그 다음 단계 성질은 $H_x \cdot H_z^T + H_z \cdot H_x^T = 0 \mod 2$을 만족하는 것이다. 기존 코드 쌍을 이용하여 부호화 하면 다음과 같은 생성행렬이 얻어진다.

$$\mathcal{G} = \left(G_x|G_z\right) = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \\ D & E(D) \end{bmatrix} \quad (22)$$

여기서 G_1 과 G_2 는 각각 두 개의 기존 코드를 생성시킬 수 있다. $E(D)$는 행렬 D의 행을 rotation시키는 역할을 한다. 에러 정정 코드를 만들기 위해 생성행렬을 $G_1 = G_2 = G_N(\mathcal{B})$ 와 같이 취하면, 행렬 $G_N(\mathcal{B})$ (예: G_N 의 sub-matrix)은 distance가 2^{t+1} 인 코드를 만들어 낸다. 결합행렬 $\left(G_1^T, D^T\right)^T$ 은 distance가 2^t 인 코드를 만들어 낸다. $E(D)=0$을 취하면 이 코드는 최소거리(minimum distance)가 2^t 이 된다. 사실, 제안된 퀀텀코드가 $2^t + 2^{t-1}$ 의 최소거리를 갖도록 적당한 rotation 연산 $E(D)$를 설계할 수 있다.

이제 퀀텀 채널 분극 기법을 통해 퀀텀 에러 정정 코드를 제안한다. 예를 들어 $N=8$ 인 $G_8 = G_2^{\otimes 3}$ 의 경우, $Z_{1,1} = 1/2$ 으로 시작한 $k = 1, 2, 2^2, 2^3$ 에 대해 반복적인 방법으로 벡터 $Z(8) = \left(Z_{8,1}, Z_{8,2}, \ldots, Z_{8,8}\right)$ 의 퀀텀 채널 분극에 따라 신뢰도를 계산할 수 있다.

$$Z_{2k,j} = \begin{cases} 2Z_{2k,j} - Z_{k,j}^2, & \text{for } 1 \le j \le k \\ Z_{k,j-k}^2, & \text{for } k+1 \le j \le 2k \end{cases} \quad (23)$$

따라서 모든 $1 \le j < k \le 8$ 에 대해 inequality $z_{8,i_j} < z_{8,i_k}$ 가 실현될 수 있도록 set $(1,\ldots,8)$ 의 치환 $\pi_N = (i_1, \ldots, i_8)$ 을 실행한다.

(N,K) polar 퀀텀 코드의 생성행렬 $\mathcal{G}_p(N,K)$ 는 인덱스가 $\{i_1,\ldots,i_K\} \subseteq \{1,\ldots,N\}$ 인 행으로 이루어진 sub-matirx로부터 구성된다. 이 구성의 계산상의 복잡도를 계산해보면 $O(N \log N)$ 와 같다.

즉, 주어진 행렬 G_8 에 대해 식 (24)와 같은 결과를 얻는다.

$$Z_8 = (0.996, 0.684, 0.809, 0.121, 0.879, 0.191, 0.316, 0.004) \quad (24)$$

즉 $\pi_8 = (8,4,6,7,2,3,5,1)$ 을 얻을 수 있는데 식 (24)는 행렬 $G_8 = O_2^{\otimes 3}$ 을 통해 얻어지고, $\pi_8 = (8,4,6,7,2,3,5,1)$ 를 생성한다. 그림 4는 $G_8 = O_2^{\otimes 3}$ 과 일반식인 $G_{2^n} = O_2^{\otimes n}$ Bhattacharyya 바운드를 보이고 있다.

한편 퀀텀 polar 코드 $((8,7))$ 은 다음과 같은 생성행렬을 얻을 수 있다.

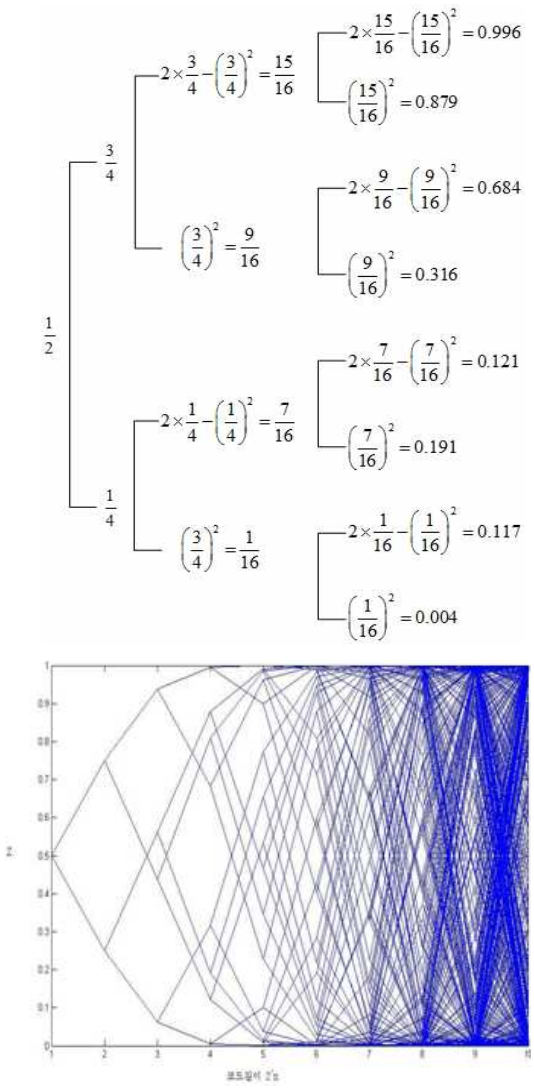

그림 4. $G_8 = O_2^{\otimes 3}$ 연산과 $G_{2^n} = O_2^{\otimes n}$ 의 Bhattacharyya 바운드

Fig. 4. $G_8 = O_2^{\otimes 3}$ calculation and Bhattacharyya bound on $G_{2^n} = O_2^{\otimes n}$.

$$\mathcal{G}_P(8,7) = \left[\begin{array}{c|c} 11110000 & 00000000 \\ 11001100 & 00000000 \\ 10101010 & 00000000 \\ 11111111 & 00000000 \\ 00000000 & 11110000 \\ 00000000 & 11001100 \\ 00000000 & 10101010 \\ 00000000 & 11111111 \\ 11000000 & 10100000 \\ 10100000 & 10010000 \\ 10010000 & 01100000 \end{array}\right] \quad (25)$$

퀀텀 안정화기 부호의 구조[11]에 따라서 퀀텀코드는 식 (26)과 같은 연접행렬로 다시 표현될 수 있다.

$$\mathcal{H}(8,7)=\left[\begin{array}{c|c} 11111111 & 00000000 \\ 00000000 & 11111111 \\ 11110000 & 11001100 \\ 11001100 & 10101010 \\ 10101010 & 11110000 \end{array}\right]=[H_x\,|\,H_z] \qquad (26)$$

식 (26)은 $H_xH_z^T+H_zH_x^T=0 \mod 2$ 를 만족한다[24]. 이 코드는 최소거리가 5 이다. 그림 5는 퀀텀채널 분리단계에서 반복적인 퀀텀채널에 대한 트리과정을 보이고 있다.

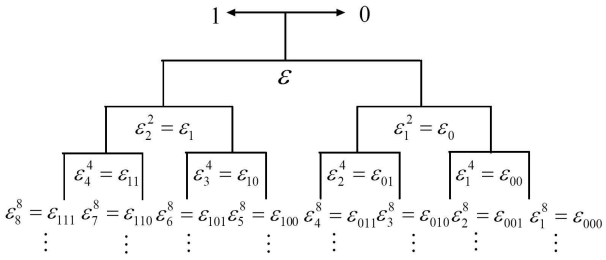

그림 5. 퀀텀채널 분리단계에서 반복적인 퀀텀채널에 대한 트리과정

Fig. 5. The tree process for the recursive quantum channel polarization in quantum channel splitting phase.

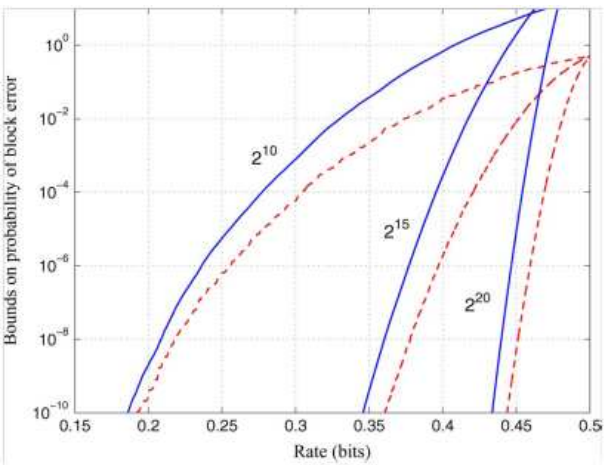

그림 6(a). 블록 길이와 전송율에 대한 블록 오류율[20]

Fig. 6(a). Block error rate for rate with various block lengths[20]

V. 모의실험

그림 6(a)는 Arikan Polar 블록코드의 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.

그림 6(b)는 Binary Erasure Channel 에서의 Rate[bit/ch.use]과 블록 길이 N과의 관계를 나타낸다. 즉 N=2000일 경우 대략 R=0.467이 된다.

VI. 결 론

본 논문에서는 퀀텀채널의 결합과 분리단계를 통해 주어진 모든 이진 입력 이산 퀀텀채널에 대한 대칭용량을 달성하기 위해서 퀀텀채널 분극이라 불리는 코딩방법을 제시했다. 이 방법은 대단히 효율적으로 퀀텀 데이터를 전송할 수 있는 퀀텀 polar 코드를 구성할 퀀텀 코딩 기법을 제공한다. 이 기법은 모든 이진입력 이산 퀀텀채널에 대해 대칭용량을 달성 할 수 있다. 이 코딩방법은 비록 이진 입력 이산 채널을 위해 제안 되었지만, 약간의 수정을 가하면 비이진(non-binary) 입력 이산 퀀텀채널과 같은 다양한 분야에 쉽게 적용할 수 있다. 이러한 문제를 풀기위한 첫 출발점은, 대칭용량을

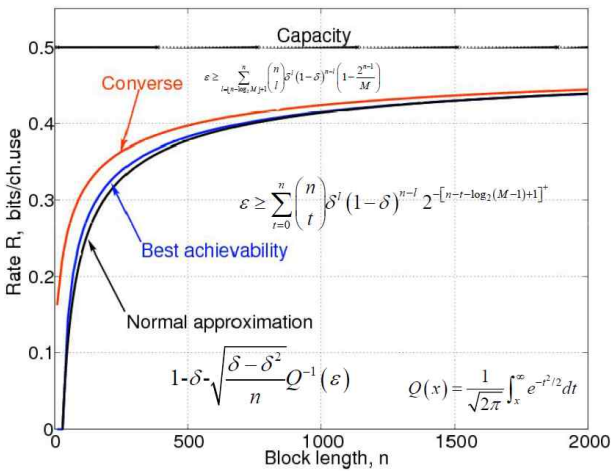

그림 6(b). Binary Erasure Channel에서의 Rate[bit/ch.use]과 블록 길이 N과의 관계

Fig. 6(b). Rate[bit/ch.use] VS. Block length N in Binary Erasure Channel.

달성하고자 하는 방법의 연구에 뿌리를 두었고, 또한 채널용량에 근접하는 대칭용량을 달성하는데 최대로 기여할 수 있는 실질적인 코딩 방법이 존재하느냐를 탐구하는데 초점을 두었다. 이에 대한 구체적이고 수학적인 증명은 차후 논문에서 다룬다.

부 록

1. 2원 대칭 통신로(Binary Symmetric Channel)에서 통신로 부호화

A. 블록 코드 길이 N 의 길이가 무한한 경우

2원 대칭 통신로의 통신로 용량은 입력심볼 0과 1이 같은 확률로 발생하는 확률로 발생하는 정보원으로 실현된다.

따라서, 0과 1을 랜덤하게 발생시켜서 길이 N 인 M 개의 계열을 만들고, 이것을 정보원 심볼 $s_1, s_2 \cdots, s_M$ 에 대응시킨다.

여기서 $s_1, s_2 \cdots, s_M$ 은 같은 확률로 발생하고 있는 것으로 한다.

이것은 부호의 전송속도 R이

$$R = \frac{\log_2 N}{N} \ [\text{bit/symbol}] \tag{A-1}$$

(i) 통신로의 비트 오율을 p라고 하면, N 이 크게 될 때 거의 N_p 개의 에러가 생긴다.(엄밀히 말하면 "에러의 수가 $N(p-\varepsilon)$ 와 $N(p+\varepsilon)$ 의 바깥에 있는 확률은 무시할 수 있을 정도로 적다"고 해야만 한다.) 여기서 N_p 는 정수라고 가정한다. 어떤 계열을 중심으로 해서

0개의 에러로 도달 가능한 계열의 수	1 개
1개의 에러로 도달 가능한 계열의 수	N 개
2개의 에러로 도달 가능한 계열의 수	${}_N C_2$ 개
N_p 개의 에러로 도달 가능한 계열의수	${}_N C_{N_p}$ 개

이므로 길이 N 인 부호어는 수신단에서 식 (A-2)와 같이 주어지는 Z 개의 계열 범위로 분산된다.

$$Z = 1 + N + {}_N C_2 + \ldots + {}_N C_{N_p} \tag{A-2}$$

이때 Z 는 다음과 같이 표시될 수 있고

$$Z = 1 + N + \frac{N(N-1)}{2} + \cdots + \frac{N!}{(N_p)!(N-N_p)!} \tag{A-3}$$

N 이 충분히 크게 될 때 식 (A-4)라고 쓸 수 있다.

$$\frac{N!}{(N_p)!(N-N_p)!} < Z < N_p \frac{N!}{(N_p)!(N-N_p)!} \tag{A-4}$$

여기서 p 는 충분히 0에 가까운 수라고 가정하고 있다.

여기에 스티어링의 공식(Stirling's formular) $x! \approx x^x$ 를 이용하면 식 (A-5)와 같이 나타낼 수 있다.

$$\frac{N^N}{(N_p)^{N_p}(N-N_p)^{N-N_p}} < Z < N_p \frac{N^N}{(N_p)^{N_p}(N-N_p)^{N-N_p}} \tag{A-5}$$

여기서 우변 N_p 배의 항은 다른 항이 N^N 에 비례해서 증가하기 때문에 무시할 수 있어 다음과 같은 결과를 얻을 수 있다.

$$\begin{aligned} Z &\approx \frac{N^N}{(N_p)^{N_p}(N-N_p)^{N-N_p}} \\ &= \frac{1}{p^{N_p}(1-N_p)^{N(1-p)}} = 2^{\log_2 p^{N_p}(1-N_p)^{N(1-p)}} \\ &= 2^{N(p\log_2\frac{1}{p}+(1-p)\log_2\frac{1}{1-p})} \\ &= 2^{NH(p)} \end{aligned} \tag{A-6}$$

즉, 비트 오율 p 인 BSC에서 길이 N 인 부호어가 수신측에서 분산되는 범위는 $2^{NH(p)}$ 정도인 것을 알 수 있다.

(ii) 다음에서 이 중에 진짜원인 이외의 계열이 부호어로서 존재할 확률을 계산해 보면, 길이 N 인 2원 계열의 총수는 2^N 이다. 따라서 이 중에서 M 개의 부호어를 랜덤하게 선택하였으므로 진짜원인 이외의 M-1개의 부호어가 이 중에서 하나라도 선택될 확률은 높아야 식 (A-7)과 같다.

$$\frac{(M-1)}{2^N}2^{NH(p)} \tag{A-7}$$

M 이 충분히 크다고 하면 다음과 같다.

$$P_E = \frac{M}{2^N}2^{NH(p)} \tag{A-8}$$

(iii) 위의 식 (A-8)에서 $M=2^{NR}$ 을 대입하여 정리하면 다음과 같은 결과를 얻을 수 있고

$$P_E = 2^{N(R-(1-H(p)))} \tag{A-9}$$

따라서 $R<1-H(p)$ 이라면, $N\to\infty$ 일 때 $P_E\to 0$ 가 증명되었다.

다음에 정리의 후반을 증명한다. 지금 P_E 가 임의의 작은 적당한 부호가 존재하고, 이 부호의 부호어 수는 $M=2^{NR}$ 이다. 단, $R>C$ 이었다고 한다.

이때, 수신측에서는 2^N 개의 계열이 $M=2^{NR}$ 개의 영역으로 분할되어 있어, 수신계열의 각각의 영역의 어느 영역에 속할 것인가에 따라서, 송신 부호어를 판정하도록 되어 있다고 한다. 여기서 설명한 부호화와 복호화는 극히 일반적인 것이고, 이 이상의 일반적인 부호화 및 복호법은 존재하지 않으므로 이와같은 방법에서도 $R>C$ 가 실현되지 않는 것을 보이면 된다.

그런데 수신측에서 이 M 개 판정영역이 같은 크기였다고 하면, 각각에 $\frac{2^N}{M}$ 개의 계열이 포함된다. 같은 크기가 아니면, 계열의 총수가 $\frac{2^N}{M}$ 보다 작은 것이 있다.

그런데, 어떤 부호어를 내보냈을 때, 그 부호어는 수신측에서는 $2^{NH(p)}$ 개의 계열로 분산된다고 생각할 수 있다. 이것이 지금 생각하고 있는 복호 영역에 전부 들어가지 않으면 안되므로, 각 영역의 계열 총수는 적어도 $2^{NH(p)}$ 보다 커야만 한다. 즉, 다음 식과 같은 조건을 만족해야 한다.

$$\frac{2^N}{M} > 2^{NH(p)} \tag{A-10}$$

그런데, $M=2^{NR}$, $R>C$ 라고 하면, 이 식이 성립하지 않는 것이 명백하다.

B. 블록 코드 길이 N 의 길이가 유한한 경우

2013 IEEE International Symposium Information Theory on ISIT 2013 Istanbul, Turkey. 7 July 2013, Tutorial Session에서 MIT의 Y.Polyanskiy와 Princeton 대의 S.Verdu 교수 강의가 있었다. Information Theory 연구의 관심사이다. 선형 블록 코드, 터보코드, LDPC 코드, Polar 코드 등 모두가 블록 길이가 유한한 경우이다. ISIT 2013 학술대회에서 삼성 산디에고 연구실의 발표에서 내부코드는 Polar 코드, 외부코드는 Reed Solomon 코드를 사용한 연접코드에서도 샤논정리에 근접한 $2^{-N^{1-\varepsilon}}$ 임을 밝혔다.

즉, 어떠한 $\varepsilon>0$ 에서 충분히 큰 수 n 에 대하여, 제안한 외부 코드율 R_0 를 가진 RS Polar 연접 코드의 오류율은 다음 식으로 상한 바운드가 결정된다[23].

$$\varepsilon \le 2^{-(\frac{n^{0.5-\varepsilon}(1-R_0)}{2}-1)m} \tag{B-1}$$

bounded-distance 복호에서, 외부 코드의 오류정정반경 범위는 $\tau=[(1-R_0)m/2]$ 일 때,

$$\varepsilon = \sum_{i=\tau+1}^{m}\binom{m}{i}P_e^i(1-P_e)^{m-i} \le \binom{m}{\tau+1}P_e^{\tau+1} \tag{B-2}$$

이 식은 다음과 같이 다시 나타낼 수 있다.

$$\begin{aligned}\varepsilon &\le \binom{m}{\tau+1}2^{-n^{0.5-\varepsilon}(\tau+1)} < \binom{m}{\tau+1}2^{-n^{0.5-\varepsilon}m(1-R_0)/2}\\ &< 2^m 2^{-n^{0.5-\varepsilon}m(1-R_0)/2}\\ &= 2^{-(n^{0.5-\varepsilon}m(1-R_0)/2-1)m}\\ &= 2^{-(\frac{n^{0.5-\varepsilon}(1-R_0)}{2}-1)m}\end{aligned} \tag{B-3}$$

한 가지 흥미로운 것은 그림 6(b)의 BEC(Binary Erasure Channel)에서 converse 바운드와 식 (B-1)의 RS Polar 코드의 바운드 ε 과 거의 같다.

REFERENCES

[1] Shannon, C.E, "A Mathematical Theory of Communication," *Bell Syst. Tech. J* 27, pp. 379-423, 1948.

[2] Nielsen, M., Chuang, I., *Quantum Computation and Quantum Information*,. Cambridge University Press, Cambridge, 2000.
[3] Deng, F.G., Long, G.L., "Secure Direct Communication with a Quantum One-Time Pad," *Phys. Rev. A* 69(5), 052319, 2004.
[4] Zeng, G., Keitel, C.H., "Arbitrated Quantum-Signature Scheme," *Phys. Rev.* A 65(4), 042312(1-6), 2002.
[5] Zeng, G., Reply to "Comment on 'Arbitrated Quantum-Signature Scheme'," *Phys. Rev.* A 78(1), 016301(1-5), 2008.
[6] Guo, Y., Lee, M.H., Zeng, G., "Quantum Codes Based on Fast Pauli Block Transforms in the Finite Field. Quan," *Infor. Proc.* 8(4), pp.361-378, 2009.
[7] Guo, Y., Lee, M.H., "Fast Quantum Codes Based on Pauli Block Jacket Matrices. Quant," *Infor. Proc* 9(5), pp.663-666, 2010.
[8] Devetak, I., "The Private Classical Capacity and Quantum Capacity of a Quantum Channel," *IEEE Trans. Inf. Theory* 51(1), pp.44-55, 2005.
[9] Jiang, L., He, G., Xiong, J., Zeng G.H., "Quantum Anonymous Voting for Continuous Variables," *Phys. Rev.* A 85(4), 042309(1-6), 2012.
[10] Calderbank, A.R., Rains, E.M., Shor, P.W., et al., "Quantum Error Correction and Orthogonal Geometry," *Phys. Rev. Lett.* 78(3), pp.405-408, 1997.
[11] Li, Y., Dumer, I., Pryadko, L.P., "Clustered Error Correction of Codeword-Stabilized Quantum Codes," *Phys. Rev. Lett.* 104(19), 190501(1-4), 2010.
[12] MacKay, D.J.C., Mitchison, G.J., McFadden, P. L., "Sparse-Graph Codes for Quantum Error Correction," IEEE Trans.Infor. Theory 50(10), pp.2315-2330, 2004.
[13] Aggarwal, V., Calderbank, A.R., "Boolean Functions, Projection Operators, and Quantum Error Correcting Codes," *IEEE Trans. Infor.* Theory 54(4), pp.1700-1707, 2008.
[14] Ocko, S.A., Chen, X., Zeng, B., et al., "Quantum Codes Give Counterexamples to the Unique Preimage Conjecture of the N-Representability Problem," *Phys. Rev. Lett.* 106(11), 110501(1-4), 2011.
[15] Chen, J., Ji, Z., Wei, Z., et al., "Correlations in Excited States of Local Hamiltonians," *Phys. Rev.* A 85(4), 040303(1-4), 2012.
[16] Grassl, M., Shor, P., Smith, G., et al., "Generalized Concatenated Quantum Codes," *Phys. Rev.* A 79(5), 050306(1-4), 2009.
[17] Bombin, H., Martin-Delgado, M.A., "Topological Quantum Distillation," *Phys. Rev. Lett.* 97(18), 180501(1-4), 2006.
[18] Viyuela, O., Rivas, A., Martin-Delgado, M.A, "Generalized Toric Codes Coupled to Thermal Baths," *New J. Phys.* 14, pp.33-44, 2012.
[19] Wilde, M.M., Guha, S., Tan, S.H., et al., "Explicit Capacity-Achieving Receivers for Optical Communication and Quantum Reading," *ISIT 2012*, Boston, MA, USA, 2012.
[20] Arikan, E., "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Trans. Infor. Theory* 55(7), pp.3051-3073, 2009.
[21] Bhattacharyya, A., "A Measure of Divergence Between Two Statistical Populations Defined by Their Probability Distributions," *Bull. Calcutta Math Soc.* 35, pp.99-110, 1943.
[22] Mark M. Wilde, Saikat Guha, "Polar Codes for Classical-Quantum Channels," *IEEE Trans. on Information Theory*, vol. 59, pp. 1175-1187, Feb. 2013.
[23] H. Mahdavifar, M. El-Khamy, J. Lee, I. Kang "On the Construction and Decoding of Concatenated Polar Codes" *IEEE ISIT 2013,* IEEE Int. Symposium on Information Theory, pp.73, Turkey, 2013. 7.7-7.12.
[24] M. H. Lee, J*acket Matrices: Construction and Its Applications for Fast Cooperative Wireless signal Processing*, LAP LAMBERT, Germany, 2012.

저 자 소 개

양 재 승(정회원)

1988년 연세대학교 금속공학과 학사
1995년 연세대학교 산업정보 석사
2010년 전북대학교 정보보호공학 박사
1989년~1999년 한국UNISYS 차장
2000년~2010년 제이에스 정보 이사
2011년 3월~현재 대진대학교 컴퓨터공학과 시간강사
<주관심분야 : Polar Code, 정보보안>

이 문 호(평생회원)-교신저자

1984년 전남대학교 전기공학과 박사, 통신기술사
1985년~1986년 미국 미네소타 대학 전기과 포스트닥터
1990년 일본동경대학 정보통신 공학과박사
1970년~1980년 남양MBC 송신소장
1980년 10월~2010년 2월 전북대학교 전자공학부 교수
2010년 2월~현재 WCU-2 연구책임교수
<주관심분야 : 무선이동통신>

박 주 용(평생회원)

1982년 전북대학교 전자공학과 석사
1994년 전북대학교 전자공학과 박사
1991년 3월~2007년 2월 서남대학교 전자공학부 부교수
2007년 3월~현재 신경대학교 인터넷정보통신학과 부교수
<주관심분야 : 무선이동통신>