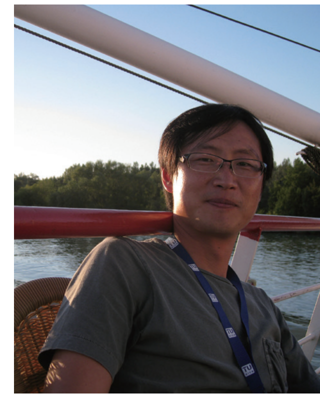
On MMS in Quantum Information Theory

양자정보이론에서의 최대혼합상태에 관하여



글_정갑균·고등과학원 계산과학부 연구원

양자정보이론에서의 최대혼합상태(Maximally Mixed State: MMS)를 고려하기 위하여, 우리는 먼저 양자상태의 수학적 정의를 살펴보자. 차원이 d인 힐버트 공간에 A라는 매트릭스가 주어져 있다고 할 때,

$$\mathrm{Tr}(A)=1,\ A^{\dagger}=A\geq 0 \qquad (1)$$

를 만족하는 연산자 A를 양자상태(quantum state)라고 정의한다. 여기서 rk(A)=1인 상태를 순수상태(pure state)라 말하고, rk(A)〉1인 상태를 혼합상태(mixed state)라 정의한다. 특히 조건 (1)을 만족하면서 풀랭크(full rank)를 만족하는 연산자를 최대혼합상태라 부르며 그 형태는 $A_d=\frac{1}{d}\times I_d$로 표현된다. 여기서 I_d는 $d\times d$ 단위행렬이다. 이런 연산자 A_d를 당연하게 여길 수 있지만 물리적 의미 입장에서는 쉬운 문제가 아니게 된다. 특히 공간의 차원이 무한대이거나 연속변수(continuous–variable: CV) 경우는 알려진 것이 많지 않다.

차원이 고정된 힐버트 공간 $H(\mathbf{C}^d)$상에서의 최대혼합상태 A_d는 다음과 같은 일반적인 성질을 가진다. 우선 대각행렬이며 $\mathrm{Tr}(A_d)=1$, 유일하게(unique) 정해진다. 기하적으로는 힐버트 공간 $H(\mathbf{C}^d)$를 블락볼(Bloch sphere) 표현으로 대응시켜 생각할 경우, 최대혼합상태는 블락볼의 원점에 해당된다. 최대혼합상태의 가장 중요한 성질 중의 하나는 바로 폰노이만(von Neumann) 엔트로피(S)를 최대화하는 상태인 것이다[1]. 구체적으로는, 주어진 $A_d\in H(\mathbf{C}^d)$에 대하여

$$S(A_d)\equiv -\mathrm{Tr}(A_d\log A_d)=\log d \qquad (2)$$

이며, 순수상태의 경우 $S(A)=0$을 항상 만족한다.

그렇다면 최대혼합상태를 만드는 구체적인 방법은 무엇인가? 답은 바로 양자채널의 일종인 양자랜덤화채널(random unitary channel)의 일반적인 개념을 고안하는 것이다. 즉, 임의의 양자상태 A에 대하여 그리고 충분히 작은 양(positive)의 에 대하여, 만약

$$\|\boldsymbol{R}(A)-A_d\|_p\leq \frac{e}{\sqrt[p]{d^{p-1}}} \qquad (3)$$

을 만족하는 양자채널 $\boldsymbol{R}$이 존재한다면, 우리는 그 채널을 양자랜덤화채널이라고 부른다[2]. 여기서 $\|\cdot\|_p$는 쉐튼노름(Schatten p–norm)을 의미한다. 이런 채널을 이용하면 새로운 형태의 비밀양자채널을 구성할 수 있을 뿐 아니라 양자네트워크(quantum network) 상에서의 응용도 가능해진다[3,4]. 지금부터는 앞서 언급한 MMS의 아주 중요한 응용을 살펴보고자 한다. 이산변수의 탁월한 응용 예는 양자채널의 고전용량(classical capacity)에 관한 가산성 위배(additivity violation)에

1) 여기서 S_{min}은 최소출력엔트로피(minimum–output entropy)이며, 쇼어(P. W. Shor)에 의하여 양자채널의 고전용량(classical capacity)과 대응관계가 있다는 사실이 알려져 있다.

관한 결과이다[5]. 양자랜덤화채널($\boldsymbol{R}$)과 그것의 복소공액인 채널($\bar{\boldsymbol{R}}$)이 있다고 가정하면

$$S_{\min}(\boldsymbol{R} \otimes \bar{\boldsymbol{R}}) < S_{\min}(\boldsymbol{R}) + S_{\min}(\bar{\boldsymbol{R}}) \qquad (4)$$

과 같은 부등호가 성립한다는 것이다[1]. 고전정보이론에서는 항상 고전용량이 등호인 관계가 성립되지만 양자채널의 용량은 가산성이 성립되지 않으며 이는 양자채널이 고전채널보다 뛰어나다(strong)고 이해할 수 있다. 여전히 양자채널의 용량(capacity)과 가산성에 관한 연구는 풀어야 할 숙제가 많다.

재미있는 것은 이와 같은 최대혼합상태가 최대얽힘상태(Maximally Entangled State: MES)[2]와 직접적인 대응관계를 가진다는 사실이다. 차원 확장과 관련되는 수학적인 순수화(purification) 기법을 사용하면 다음의 결과를 얻게된다.

$$\pi(A_d) = \alpha_{d^2} \qquad (5)$$

여기서 $\pi(A_d) = \alpha_{d^2}$는 각각 순수화 함수, MMS, MES를 나타낸다. 차원이 2인 경우의 예를 살펴보자.

$A_d = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$ 라고 하면, 순수화된 상태

$$\pi(A_d) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix} \qquad (6)$$

을 얻으며 ($\mathrm{rk}(\pi(A_d)) = 1$) 이 결과는 네 종류의 최대얽힘상태인 벨 상태(Bell's state) 혹은 EPR 상태들 중의 하나가 됨을 알 수 있다. 즉 최대혼합상태의 순수화는 최대얽힘상태를 주고, 반대로 최대얽힘상태의 부분자취(partial trace)는 최대혼합상태에 대응됨을 알 수 있다. 이 예는 임의의 차원에 대하여도 성립한다. 폰노이만 엔트로피 관점에서 최대의 엔트로피 상태(MMS)가 최소의 엔트로피를 갖는 상태(MES)와 직접적인 대응 관계를 가진다는 사실에 놀라게 된다.

이와 같은 상황은 연속변수(CV)의 공간에서도 생각해 볼 수 있다. 여기서의 CV 공간은 물리적으로는 위상공간(phase space)이며 수학적으로는 심플렉틱 공간(symplectic space)을 의미한다. 이 공간에서 위그너 분포함수(Wigner W−distribution function)를 고려하면 양자상태가 가우시안(Gaussian) 형태를 갖게 되어 앞서 언급한 연속변수를 가우시안이라 부르게 된다. 그러면 가우시안 최대혼합상태(Gaussian Maximally Mixed State: GMMS)는 어떤 것인가? 이런 GMMS에 대한 접근은 브레들러(Bradler)에 의해 처음 제시되었고[6] $\boldsymbol{I}_b$라 불리게 된다. 여기서

$$\boldsymbol{I}_b = \frac{1}{b^2}\sum_{n=0}^{\infty}\left(1 - \sum_{k=0}^{b^{2k}} e^{-b^2}\right)|n><n| \qquad (7)$$

이고, 숫자기저(number basis) $|n>$에 대한 표현이 된다. 중요한 것은 위상공간이 무한대로 펼쳐지므로 원점으로부터의 반경에 대한 제한($r \leq b$)을 고려하게 되며, 형태자체는 평평하다(flat). 이산변수의 유일한 경우와는 달리 가우시안의 경우에는 다른 후보를 생각해 볼 수 있는데, 그것은 바로 열평형(thermal equilibrium)과 관련되는 열적상태(thermal state) A_{th}이며, 평균 광자에너지(mean−photon energy) $\bar{n}$를 고정할 경우,

$$A_{th}(\bar{n}) = \sum_{n=0}^{\infty}\frac{\bar{n}^n}{(\bar{n}+1)^{n=1}}|n><n| \qquad (8)$$

으로 주어진다. 순수화 방법(π)이 동원될 경우 $\pi(A_{th}(\bar{n}))$는 양자광학에서 잘 아려진 2−모드 압

착진공상태(two–mode squeezed vacuum state)가 되며 이는 가우시안 최대얽힘상태를 주게 된다. 아쉽게도 식 (7)에 주어진 I_b에 대한 $\pi(I_b)$ 형태는 알려진 바가 없고, 우리는 단지 또 다른 가우시안 최대얽힘상태가 될 것이라는 예측만 있을 뿐이다.

다음으로 가우시안 최대혼합상태의 응용에 대한 연구를 간략하게 소개하고자 한다. 브레들러의 가우시안 비밀양자채널(Gaussian private quantum channel)은 양자정보를 I_b와 근접한 상태로 변환하기 때문에 제 3자의 도청이나 정보 손실을 원천 봉쇄할 수 있다. 여기서 사용된 방법은 결맞음 상태의 혼합 만을 사용한 반면, 저자를 포함한 본 연구진이 제한한 방법은 결맞음에 압착연산(squeezing operation)을 추가여 비밀양자채널을 구성하여도 양자정보를 안전하게 전송할 수 있다는 결과를 얻었다[7]. 가우시안 연산은 결맞음 연산(displacement operation)과 압착연산이 포함될 때를 의미하므로 우리의 결과는 보다 일반적인 상황에서 적용이 가능하다.

마지막으로 앞으로의 연구를 소개하며 본 기고를 마치고자 한다. 양자채널의 고전용량위배에 관한 결과는 양자랜덤화채널의 존재성에 관한 수학적 증명이며, 물리적 실험을 향한 어떤 시도도 이루어져 있지 않다. 이에 본 연구진은 양자채널의 실제적인 가산성 위배를 보일 수 있는 양자광학회로(quantum optical circuit)을 구성하는 이론적 제안을 시도하고 있다[8]. 앞서 소개한 순수화 기법을 이용한 MMS와 MES의 대응관계와 가우시안에서의 GMMS를 정확하게 이해하고 적용할 경우를 상정한다면 본 연구가 그리 요원한 것은 아닐 것이다.

참고문헌

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2000).

[2] K. Jeong, Randomizing quantum states to Schatten p–norm for all p≥1, AIP Conference Proceedings 1633, 171 (2014).

[3] K. Jeong and Jaewan Kim, Secure sequential transmission of quantum information, Quantum Info. Process. Open Access, DOI: 10.1007/s11128–015–1054–5 (2015).

[4] Dong Pyo Chi and Kabgyun Jeong, Approximate Quantum State Sharings via Pair of Private Quantum Channels, J. Quant. Info. Sci. 4, 64 (2014).

[5] M. B. Hastings, Superadditivity of communication capacity using entangled inputs, Nature Phys. 5, 255 (2009).

[6] K. Bradler, Continuous–variable private quantum channel, Phys. Rev. A 72, 042313 (2005).

[7] K. Jeong, Jaewan Kim, and Su–Yong Lee, Gaussian private quantum channel with squeezed coherent states, submitted (2015).

[8] K. Jeong, Jaewan Kim, Kisik Kim, and Su–Yong Lee, Gaussian maximally mixed states and additivity violation of the classical capacity on quantum channels, In preparation (2015).

2) 최대얽힘상태는 양자역학 혹은 양자정보이론의 핵심 요소이며 고전역학이 해결하지 못한 많은 풀이를 제시하는 핵심 열쇠의 역할을 수행한다.