



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월22일
(11) 등록번호 10-2231130
(24) 등록일자 2021년03월17일

(51) 국제특허분류(Int. Cl.)
H04B 10/70 (2013.01) H04L 25/02 (2006.01)
(52) CPC특허분류
H04B 10/70 (2013.01)
H04L 25/0202 (2013.01)
(21) 출원번호 10-2019-0159748
(22) 출원일자 2019년12월04일
심사청구일자 2019년12월04일
(56) 선행기술조사문헌
Junaid ur Rehman et al., "Holevo Capacity of Discrete Weyl Channels," Scientific Reports, 8:17457, pp. 1-10, (2018.11.29)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
신현동
경기도 수원시 영통구 청명로 132, 323동 501호(영통동, 벽산삼익아파트)
정영민
경기도 성남시 중원구 도촌북로 78, 501동 402호(도촌동, 휴먼시아섬마을5단지아파트)
유나이드 우르 레만
경기도 용인시 기흥구 덕영대로 1732 (서천동)
(74) 대리인
특허법인도담

전체 청구항 수 : 총 2 항

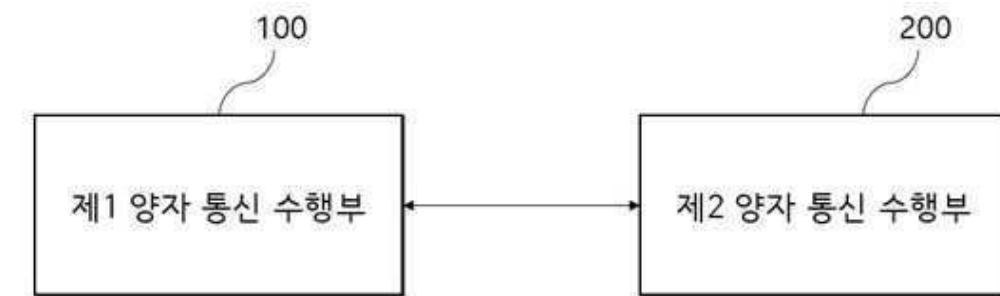
심사관 : 신상길

(54) 발명의 명칭 양자 채널 용량 추정 방법 및 이를 이용한 양자 통신 시스템

(57) 요약

본 기술은 양자 통신 및 양자 컴퓨팅에 관한 것으로, 본 기술에 따른 향상된 양자 채널 용량 추정 방법은, 양자 정보 및 일반 정보를 송수신하는 제1 양자 통신 수행부 및 제2 양자 통신 수행부를 포함하는 양자 통신 시스템의 양자 채널 용량 추정 방법에 있어서, 상기 제1 양자 통신 수행부는 미리 설정된 개수의 고유 기저를 준비하고, 상기 미리 설정된 개수의 양자 채널을 통해 상기 제2 양자 통신 수행부에 상기 고유 기저를 전송하는 단계, 상기 제2 양자 통신 수행부가 상기 고유 기저를 수신하면, 상기 고유 기저에 대해 투영 측정을 수행하는 단계 및 상기 측정 결과를 기초로 상기 양자 채널의 Holevo 용량의 하한을 연산하는 단계를 포함한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	2019R1A2C2007037
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	이공분야기초연구사업/중견연구자지원사업
연구과제명	양자네트워킹 핵심기술 연구
기 여 율	1/1
과제수행기관명	경희대학교 산학협력단
연구기간	2019.03.01 ~ 2024.02.28
공지예외적용	: 있음

명세서

청구범위

청구항 1

양자 정보 및 일반 정보를 송수신하는 제1 양자 통신 수행부 및 제2 양자 통신 수행부를 포함하는 양자 통신 시스템의 양자 채널 용량 추정 방법에 있어서,

상기 제1 양자 통신 수행부는 미리 설정된 개수의 고유 기저를 준비하고, 상기 미리 설정된 개수의 양자 채널을 통해 상기 제2 양자 통신 수행부에 상기 고유 기저를 전송하는 단계;

상기 제2 양자 통신 수행부가 상기 고유 기저를 수신하면, 상기 고유 기저에 대해 투영 측정을 수행하는 단계;

상기 측정 결과를 제1 레지스터에 저장하는 단계;

상기 제2 양자 통신 수행부는 상기 제1 레지스터의 엔트로피를 연산하고, 제2 레지스터에 저장하는 단계; 및

상기 엔트로피를 기초로 상기 양자 채널의 Holevo 용량의 하한을 연산하는 단계를 더 포함하고,

상기 투영 측정은

이산 베일 채널에서 상기 고유 기저의 관측 가능한 고전 랜덤 변수(classical random variable)를 측정하는 동작이고,

상기 엔트로피는,

이차 복잡도(d^2)를 갖는 폰 뉴어만 엔트로피 또는 선형 복잡도(d^{+1})를 갖는 섀넌 엔트로피(Shannon entropy)인 양자 채널 용량 추정 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

제1항에 있어서, 상기 양자 통신 시스템은,

이산 베일 연산자가 d 의 구별되는 고유값을 가지고, 상기 고유값의 고유 상태가 이산 베일 채널의 입력일 때, 상기 이산 베일 채널은 상기 이산 베일 연산자의 고유 기저와 대각화된 결과값을 출력하는 양자 채널 용량 추정 방법.

청구항 7

삭제

청구항 8

삭제

발명의 설명

기술 분야

- [0001] 본 발명은 양자 통신 및 양자 컴퓨팅에 관한 것이다. 보다 구체적으로, 양자 통신에 사용되는 양자 채널의 용량을 측정하기 위한 방법에 관한 것이다.

배경 기술

- [0003] 양자역학(quantum mechanics)은 분자, 원자, 전자, 소립자와 미시적인 계의 현상을 다루는 즉, 작은 크기를 갖는 계의 현상을 연구하는 물리학의 분야이다. 양자역학을 이해하기 위해 ‘양자’와 ‘역학’의 의미를 각각 살펴볼 수 있다. ‘양자’로 번역된 영어의 quantum은 양을 의미하는 quantity에서 온 말로, 무엇인가 띄엄띄엄 떨어진 양으로 있는 것을 가리키는 말이다. ‘역학’은 말 그대로는 ‘힘의 학문’이지만, 실제로는 ‘이러저러한 힘을 받는 물체가 어떤 운동을 하게 되는지 밝히는 물리학의 한 이론’이라고 할 수 있다. 간단히 말해 ‘힘과 운동’의 이론이다. 이렇듯 양자역학이란 띄엄띄엄 떨어진 양으로 있는 것이 이러저러한 힘을 받으면 어떤 운동을 하게 되는지 밝히는 이론이라고 할 수 있다.
- [0004] 양자 얽힘(quantum entanglement)은 양자 통신, 양자 암호 및 양자 계측학을 포함하는 양자 정보 처리의 재료(resource)이다. 양자역학에서, 양자 얽힘 또는 간단히 얽힘은 두 부분 계 사이에 존재할 수 있는 일련의 비고전적인 상관관계이다. 얽힘은 두 부분계가 공간적으로 서로 멀리 떨어져 있어도 존재할 수 있다. 예를 들어, 두 입자를 일정한 양자상태에 두어 두 입자의 스핀이 항상 반대가 되도록 할 수 있다. (예를 들어 두 스핀의 단일항 상태.) 양자역학에 따르면, 측정하기 전까지는 두 입자의 상태를 알 수 없다. 하지만 측정을 한다면, 그 순간 한 계의 상태가 결정되고 이는 즉시 그 계와 얽혀 있는 다른 계의 상태까지 결정하게 된다. 이는 마치 정보가 순식간에 한 계에서 다른 계로 이동한 것처럼 보일 수 있다.
- [0005] 양자 채널은 양자 정보 이론과 양자 통신 프로토콜의 핵심이라고 할 수 있다. 프로토콜의 성능과 실행 품질은 양자 채널의 용량에 크게 좌우될 수 있다. 현실적인 관점에서, 이용 가능한 양자 채널에 대한 정보를 모두 알 수는 없으므로 실제로 프로토콜을 효율적으로 구현하는 것은 매우 어렵다. 예를 들어, 양자 채널의 기본적인 임무 중 하나인, 멀리 떨어진 당사자간 정보 전송을 생각할 수 있다. 최대로 전송할 수 있는 정보는 채널의 용량에 의해 결정될 수 있다. 따라서, 일반적으로 채널 용량을 특성화하기 전에 해당 양자 채널에 대한 이해가 필요하다.
- [0006] 일반화된 파울리 채널 또는 이산 바일 채널(discrete Weyl channel)은 파울리 큐비트, 디페이징 및 디폴라이징 채널을 포함하는 광범위한 종류의 큐비트 채널을 구성한다. 중요성과 다양성을 고려할 때 이산 바일 채널을 특성화하기 위한 실험 설정을 고안하는 몇 가지 연구가 수행되었다.
- [0007] 예를 들어, 이분 최대 혼합 프로브가 이산 바일 채널의 파라미터 추정에 최적이라는 것이 알려져 있다. 그 후 디폴라이징 채널(이산 바일 채널의 특별한 경우)에 대해 연구되었고, 최적의 파라미터 추정 방법이 제안되었다. 다른 특화된 시나리오에서 일반화된 파울리 채널의 파라미터 추정의 실행 가능한 방법이 탐색된 바 있다.
- [0008] 앞서 언급한 모든 추정 방법은 d 차원 힐버트 공간에서 작동하는 양자 채널이 $d^2 \times d^2$ 프로세스 매트릭스로 표현되는 전통적인 프로세스 단층 촬영법(tomography)을 따랐다. 최근, 양자 채널의 전체 프로세스 단층 촬영을 수행하는 대신, 관심있는 영역만을 직접 추정하는 양자 채널 추정 방법의 제안이 있었다. 본 발명은 이러한 연구의 일환으로, 양자 채널 용량의 탐지 가능한 하한을 제공하는 것을 목적으로 한다.

발명의 내용

해결하려는 과제

- [0010] 본 발명의 실시 예는, 양자 채널 용량 측정시, 양자 얽힘을 요하지 않고 요구되는 측정 구성(measurement configuration)을 줄임으로써, 보다 효율적이며 구현이 용이한 양자 통신 시스템을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0012] 본 기술은 양자 통신 및 양자 컴퓨팅에 관한 것으로, 본 기술에 따른 향상된 양자 채널 용량 추정 방법은, 양자 정보 및 일반 정보를 송수신하는 제1 양자 통신 수행부 및 제2 양자 통신 수행부를 포함하는 양자 통신 시스템의 양자 채널 용량 추정 방법에 있어서, 상기 제1 양자 통신 수행부는 미리 설정된 개수의 고유 기저를 준비하고, 상기 미리 설정된 개수의 양자 채널을 통해 상기 제2 양자 통신 수행부에 상기 고유 기저를 전송하는 단계, 상기 제2 양자 통신 수행부가 상기 고유 기저를 수신하면, 상기 고유 기저에 대해 투영 측정을 수행하는 단계 및 상기 측정 결과를 기초로 상기 양자 채널의 Holevo 용량의 하한을 연산하는 단계를 포함한다.

발명의 효과

[0014] 본 기술에 따르면, 양자 채널 용량 측정시 양자 얽힘을 필요로 하지 않고, 요구되는 측정 구성을 기존의 d^2 에서 $d+1$ 로 감소시킴으로써, 보다 효율적이며 구현이 용이한 양자 채널 용량 추정 방법이 제공된다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 실시 예에 따른 양자 통신 시스템을 설명하기 위한 도면이다.

도 2는 도 1의 양자 통신 시스템의 상세 구성을 설명하기 위한 도면이다.

도 3은 도 1의 양자 통신 시스템의 동작을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 명세서 또는 출원에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 내지 기능적 설명들은 단지 본 발명의 개념에 따른 실시 예를 설명하기 위한 목적으로 예시된 것으로, 본 발명의 개념에 따른 실시 예들은 다양한 형태로 실시될 수 있으며 본 발명의 개념에 따른 실시 예들은 다양한 형태로 실시될 수 있으며 본 명세서 또는 출원에 설명된 실시 예들에 한정되는 것으로 해석되어서는 아니 된다.

[0018] 본 발명의 개념에 따른 실시 예는 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있으므로 특정 실시 예들을 도면에 예시하고 본 명세서 또는 출원에 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예를 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0019] 제1 및/또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 이탈되지 않은 채, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0020] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0021] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 서술된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0022] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0023] 실시 예를 설명함에 있어서 본 발명이 속하는 기술 분야에 익히 알려져 있고 본 발명과 직접적으로 관련이 없는 기술 내용에 대해서는 설명을 생략한다. 이는 불필요한 설명을 생략함으로써 본 발명의 요지를 흐리지 않고 더욱 명확히 전달하기 위함이다.

[0024] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다. 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0025] 도 1은 본 발명의 실시 예에 따른 양자 통신 시스템을 설명하기 위한 도면이다.

[0026] 도 1을 참조하면, 본 발명의 실시 예에 따른 양자 통신 시스템은 제1 양자 통신 수행부(100) 및 제2 양자 통신 수행부(200)를 포함할 수 있다.

[0027] 제1 양자 통신 수행부(100) 및 제2 양자 통신 수행부(200)는 각각 사용자 Alice와 Bob이 사용하는 양자 통신 수행부일 수 있다. Alice는 송신자로서 양자 채널(quantum channel)을 통해 양자 정보를, 고전 채널(Classical channel)을 통해 일반 정보를 Bob에게 전송할 수 있다. 제1 양자 통신 수행부(100)는 송신 기기로, 제2 양자 통신 수행부(200)는 수신 기기로 표시하였지만, 실시 예에 따라 그 역도 성립할 수 있다. 또한, 제1 양자 통신 수행부(100)가 송신 또는 수신 기기로 동작함에 따라, 제2 양자 통신 수행부(200)는 이에 대응하여 수신 또는 송신 기기로 동작할 수 있다.

[0028] 제1 양자 통신 수행부(100)와 제2 양자 통신 수행부(200)는 양자 암호 통신을 통해 암호화된 양자 정보 및 일반 정보를 교환할 수 있다.

[0029] 본 발명의 실시 예에서, 양자 통신 시스템은 이산 베일 채널의 채널 용량을 하한을 제공할 수 있다. 양자 채널의 고전적인(classical) 채널 용량은 채널에 대한 임의의 입력으로 달성할 수 있는 고전적인 통신의 최대 속도일 수 있다.

[0030] 양자 채널의 채널 용량에 대한 하한은 Holevo 용량으로 주어질 수 있다. Holevo 용량은 양자의 분리 가능한 입력 상태에 의해 달성될 수 있다. 본 발명의 양자 채널 용량 측정 방법을 설명하기 위해, 먼저 이산 베일 채널, Holevo 용량 및 이산 베일 연산자에 대해 설명하기로 한다.

[0031] 이산 베일 채널이란 파울리 큐빗 채널을 임의의 d 차원으로 일반화한 채널일 수 있다. 입력 상태 ρ 에 대한 이산 베일 채널의 동작은 아래와 같다.

$$\mathcal{N}_{\text{dwc}}(\rho) = \sum_{n=0}^{d-1} \sum_{m=0}^{d-1} p_{n,m} W_{n,m} \rho W_{n,m}^{\dagger}$$

[0032]

[0033] d 차원의 입력 상태 ρ 에서 이산 베일 채널은 실제로 매우 넓은 종류의 단위 양자 채널을 특성화할 수 있다. 이산 베일 채널의 동작에는 큐빗 디폴라이징(depolarizing), 2-파울리, 파울리 비트 플립, 디페이징(dephasing) 채널이 포함될 수 있다.

[0034] Holevo 용량은 특정 양자 채널에 대해, 인코더가 다양한 용도에서 얽힘 입력을 사용할 수 없는 고전 통신의 최대 달성 가능한 점근율로 정의될 수 있다. Holevo 용량을 χ , 양자 채널을 $\mathcal{N}$ 라고 할 때, Holevo 용량은 아래와 같다.

$$\chi(\mathcal{N}) = \sup [S\left(\sum_i p_i \mathcal{N}(\rho_i)\right) - \sum_i p_i S(\mathcal{N}(\rho_i))]$$

[0035]

[0036] 이때, 상한(supremum)은 모든 입력 상태 ρ_i 와 모든 입력 상태들의 확률 p_i 에 대해 적용되며, S 는 폰뉴어만 엔트로피일 수 있다.

[0037] 이산 베일 연산자는 파울리 연산자(d=2)의 비 에르미트 큐빗(d>2)의 일반화일 수 있다. d 차원 힐베르트 공간에서 d^2 이산 베일 연산자는 다음과 같이 정의될 수 있다. 이때, $\mathbb{Q}_d = \{0, 1, \dots, d-1\}$, $\omega = e^{\frac{2\pi i}{d}}$ 이며, $\oplus$

는 모듈로 d 연산일 수 있다. $|i\rangle$ 는 d 차원 힐버트 공간에서 i 번째 기저 상태일 수 있다.

$$W_{n,m} = \sum_{i=0}^{d-1} \omega^{in} |i\rangle\langle i \oplus m|, \quad n, m \in \mathbb{Q}_d,$$

[0038]

[0039] d 차원의 연산자로의 파울리 연산자의 일반화를 통해 이산 베일 채널을 정의할 수 있으며, 이는 결국 파울리 큐비트 채널을 $\mathcal{H}_d$ 로 일반화할 수 있다. 2 차원 공간에서 $W_{0,1}$, $W_{1,0}$, $W_{1,1}$ 는 각각 비트 플립, 위상 플립 및 비트 플립, 위상 플립의 결합을 나타낼 수 있다.

[0040] 본 발명의 실시 예에 따른 양자 통신 시스템은 이산 베일 채널의 대각화된 결과값을 출력할 수 있다. 구체적으로, 이산 베일 연산자 $W_{n,m}$ 가 d 의 구별되는 고유값을 가지고, 이들의 고유 상태 $|i_{n,m}\rangle$ 가 이산 베일 채널의 입력이라고 가정할 수 있다. 이때, 이산 베일 채널은 이산 베일 연산자의 고유 기저와 대각화된 결과값을 출력할 수 있다.

[0041] 이때, 고유값 $P_k^{n,m}$ 는 아래 수학적식과 같이 주어지며, $p_{a,b}$ 는 이산 베일 채널의 특성을 나타내는 파라미터일 수 있다.

수학적식 1

$$P_k^{n,m} = \sum_{\substack{a,b \in \mathbb{Q}_d: \\ k = -nb \oplus ma}} p_{a,b}$$

[0042]

[0043] 이러한 특성을 이용하여 본 발명의 양자 통신 시스템은 이산 베일 채널의 Holevo 용량의 하한을 제공할 수 있다. 이산 베일 채널의 Holevo 용량의 하한은 $\chi(\mathcal{N}_{\text{dwc}}) \geq \chi_{\text{lb}}(\mathcal{N}_{\text{dwc}})$ 로 표현되며, 구체적으로 하한은 수학적식 2 일 수 있다.

수학적식 2

$$\chi_{\text{lb}}(\mathcal{N}_{\text{dwc}}) = \log_2 d - \min_{|\psi\rangle \in \mathcal{B}(\mathcal{S}^i)} S(\mathcal{N}(|\psi\rangle\langle\psi|)).$$

[0044]

[0045] 이때, $\mathcal{B}(\mathcal{S}^i)$ 는 $d+1$ 이산 베일 연산자 $\mathcal{S} = \{W_{1,0}, W_{0,1}, W_{1,1}, W_{2,1}, \dots, W_{d-1,1}\}$ 의 i 번째 고유 벡터의 집합일 수 있다.

[0046] 수학적식 2의 하한은, 파울리 큐비트 채널, 임의의 차원에 대한 디폴라이징(depolarizing) 채널 및 디페이징 채널에 대해 성립할 수 있다.

[0047] 또한, 수학적식 1로부터, $|\psi\rangle \in \mathcal{B}(\mathcal{S}^i)$ 일 때 채널 출력 상태 $\mathcal{N}(|\psi\rangle\langle\psi|)$ 는 이산 베일 연산자의 고유 기저와 수직이므로, 양자 통신 시스템은 투영 측정(projective measurement)을 채널 출력 상태에 대해 반복적으로 수행하여 채널 출력 상태의 폰 뉴어만 엔트로피 $S(\mathcal{N}(|\psi\rangle\langle\psi|))$ 의 추정치를 획득할 수 있다.

[0048] 엔트로피는 이차 복잡도(d^2)를 갖는 폰 뉴어만 엔트로피 또는 선형 복잡도(d^{+1})를 갖는 섀넌 엔트로피(Shannon entropy)일 수 있다. 다만, 본 발명의 실시 예에서, 이차 복잡도(d^2)를 갖는 폰 뉴어만 엔트로피 추정에 관한 문제를, 선형 복잡도(d^{+1})를 갖는 섀넌 엔트로피(Shannon entropy)의 추정에 관한 문제로 변환

함으로써 더 적은 측정 구성을 요하는 양자 채널 용량 추정 방법의 구현이 가능하다.

[0049] 획득한 채널 출력 상태의 폰 뉴어만 엔트로피의 추정치로부터, 물리적으로 사용 가능하지만 채널의 특성을 나타내는 파라미터를 알 수 없는 이산 베일 채널의 Holevo 용량에 대한 추정치를 획득할 수 있다.

[0050] 위 과정은 아래 수학식 3으로 수학적으로 표현될 수 있다. 최종적으로 획득된 이산 베일 채널의 Holevo 용량의 하한으로부터 양자 채널의 최대 사용 가능한 용량을 보다 정확하게 추측할 수 있다.

수학식 3

$$\begin{aligned}\chi(\mathcal{N}_{\text{dwc}}) &= \log_2(d) - \min_{|\psi\rangle \in \mathcal{B}(\mathcal{H})} S(\mathcal{N}_{\text{dwc}}(|\psi\rangle\langle\psi|)) \\ &\geq \log_2(d) - \min_{|\psi\rangle \in \mathcal{B}_W \setminus \mathcal{B}_{0,0}} S(\mathcal{N}_{\text{dwc}}(|\psi\rangle\langle\psi|)) \\ &\geq \log_2(d) - \min_{|\psi\rangle \in \mathcal{B}_S} S(\mathcal{N}_{\text{dwc}}(|\psi\rangle\langle\psi|)) \\ &= \log_2(d) - \underbrace{\min_{|\psi\rangle \in \mathcal{B}_S^i} S(\mathcal{N}_{\text{dwc}}(|\psi\rangle\langle\psi|))}_{\chi_{\text{lb}}(\mathcal{N}_{\text{dwc}})}\end{aligned}$$

[0051]

[0052] 종래에는 양자 채널의 특성을 알 수 없는 경우, 채널 용량을 계산하기 위해, 용량을 계산하기 전에 전체 프로세스 단층 촬영(tomography)을 수행해야 했다. 프로세스 단층 촬영에는 일반적으로 d^2 측정 구성(measurement configuration)이 필요할 수 있다.

[0053] 본 발명의 실시 예에 따른 양자 채널 용량 추정 방법은 d+1 측정 구성만을 필요로 하며, 별도의 양자 얽힘을 요하지 않는다. d+1의 측정 구성은 입력 상태와 측정 설정의 합일 수 있다. 개별 큐비트에 대한 투영 측정(projective measurement)만으로 채널 용량의 Holevo 용량의 하한값을 알 수 있으므로 채널 용량 추정의 리소스를 줄일 수 있고 구현하기 용이한 효과가 있다.

[0054] 도 2는 본 발명의 실시 예에 따른 양자 통신 시스템의 상세 구성을 설명하기 위한 도면이다.

[0055] 도 2를 참조하면, 제1 양자 통신 수행부(100)는 제어부(110), 송수신부(120) 및 메모리(130)를 포함할 수 있다. 또한, 제2 양자 통신 수행부(200)는 제어부(210), 송수신부(220) 및 메모리(230)를 포함할 수 있다.

[0056] 송수신부(120, 220)은 양자 채널(quantum channel)을 이용하는 양자 송수신부 일 수 있다. 또한, 송수신부(120, 220)은 고전 채널(classical channel)을 이용하는 일반 송수신부를 포함할 수 있다.

[0057] 송수신부(120, 220)은 양자 채널(quantum channel)을 이용하는 양자 송수신부 일 수 있다. 또한, 송수신부(120, 220)은 고전 채널(classical channel)을 이용하는 일반 송수신부를 포함할 수 있다. 제1 양자 통신 수행부(100) 및 제2 양자 통신 수행부(200)는 송수신부(120, 220)을 통해 양자 정보 및 일반 정보를 송수신할 수 있다. 양자 정보는 양자 채널을 통해, 일반 정보는 고전 채널을 통해 각각 송수신될 수 있다.

[0058] 메모리(130, 230)는 양자 정보를 저장하는 양자 메모리일 수 있다. 또한, 메모리(130, 230)는 일반 정보를 저장하는 일반 메모리를 포함할 수 있다. 메모리(130, 230)에서 양자 정보 또는 일반 정보를 저장하도록 구성된다. 전술된 바와 같이, 메모리(130, 230)는 양자 메모리 또는 일반 메모리로 지칭될 수 있다.

[0059] 도 3은 도 1의 양자 통신 시스템의 동작을 설명하기 위한 순서도이다.

[0060] 도 3을 참조하면, S301 단계에서, 제1 양자 통신 수행부는 미리 설정된 개수의 고유 기저를 준비하고, 상기 미리 설정된 개수의 채널을 통해 제2 양자 통신 수행부에 전송할 수 있다.

[0061] 실시 예에서, 이산 베일 연산자 $W_{n,m}$ 의 고유 벡터에 의해 형성된 고유 기저는 $\mathcal{B}_{n,m}$ 일 수 있다. 아래 수학식 4로부터, n, m의 두 변수는 k라는 단일 변수로 표현될 수 있다.

수학식 4

$$W_k = \begin{cases} W_{1,0} & \text{for } k = 0, \\ W_{k-1,1} & \text{for } k = 1, 2, \dots, d. \end{cases}$$

[0062]

[0063]

이산 베일 연산자의 힐버트 공간의 차원이 d , 사용되는 채널의 개수를 N 이면, 미리 설정된 개수는 $N/(d+1)$ 일 수 있다. 서로 다른 입력 상태는 상기 미리 설정된 개수만큼 채널에 입력될 수 있다.

[0064]

즉, 제1 양자 통신 수행부는 $N/(d+1)$ 개의 고유 기저를, N 개의 채널에 $N/(d+1)$ 번 제2 양자 통신부에 전송할 수 있다.

[0065]

S303 단계에서, 제2 양자 통신 수행부가 j 번째 고유 기저를 수신하면, 제2 양자 통신 수행부는 j 번째 고유 기저에 대해 투영 측정(projective measurement)을 수행할 수 있다.

[0066]

S305 단계에서, 제2 양자 통신 수행부는 측정 결과를 제1 레지스터의 j 번째 자리에 저장하고, S307 단계에서 제1 레지스터의 엔트로피를 연산하고 제2 레지스터에 저장할 수 있다. S303 단계 내지 S307 단계는 다음과 같은 과정에 따라 수행될 수 있다.

[0067]

투영 측정은 이산 베일 채널에서 고유 기저의 관측 가능한 고전 랜덤 변수(classical random variable, X_k)를 측정하는 동작일 수 있다. 전술한 수학식 1은 투영 측정에 의해 획득된 고전 랜덤 변수의 엔트로피를 추정함으로써, 이산 베일 채널의 폰 뉴어만 엔트로피를 추정하는 수단을 제공할 수 있다.

[0068]

구체적으로, 본 발명의 실시 예에 따른 양자 통신 시스템은 이산 베일 채널의 대각화된 결과값을 출력할 수 있다(수학식 1). 이산 베일 연산자 $W_{n,m}$ 가 d 의 구별되는 고유값을 가지고, 이들의 고유 상태 $|i_{n,m}\rangle$ 가 이산 베일 채널의 입력이라고 가정할 수 있다.

[0069]

이때, 이산 베일 채널은 이산 베일 연산자의 고유 기저와 대각화된 결과값을 출력할 수 있다. 고유값 $P_k^{n,m}$ 는 아래 수학식1과 같이 주어지며, $P_{a,b}$ 는 이산 베일 채널의 특성을 나타내는 파라미터일 수 있다. 이러한 특성을 이용하여 본 발명의 양자 통신 시스템은 이산 베일 채널의 Holevo 용량의 하한을 제공할 수 있다.

[0070]

위 과정을 통해 이차 복잡도(d^2)를 갖는 폰 뉴어만 엔트로피 추정에 관한 문제를, 선형 복잡도($d+1$)를 갖는 섀넌 엔트로피(Shannon entropy)의 추정에 관한 문제로 변환할 수 있다.

[0071]

S309 단계에서, 투영 측정의 결과를 기초로 양자 채널의 Holevo 용량의 하한을 연산할 수 있다. 구체적으로, 제2 양자 통신 수행부는 투영 측정 결과를 기초로 엔트로피를 연산하고, 연산된 엔트로피를 기초로 Holevo 용량의 하한을 연산할 수 있다.

[0072]

본 발명의 양자 통신 시스템은 이산 베일 채널의 Holevo 용량의 하한을 제공할 수 있다. 이산 베일 채널의 Holevo 용량의 하한은 $\chi(\mathcal{N}_{\text{dwc}}) \geq \chi_{\text{lb}}(\mathcal{N}_{\text{dwc}})$ 로 표현되며, 구체적으로 하한은 전술한 수학식 2일 수 있다.

[0073]

$$\chi_{\text{lb}}(\mathcal{N}_{\text{dwc}}) = \log_2 d - \min_{|\psi\rangle \in \mathcal{B}(\mathcal{S}^i)} S(\mathcal{N}(|\psi\rangle\langle\psi|)).$$

[0074]

이때, $\mathcal{B}(\mathcal{S}^i)$ 는 $d+1$ 이산 베일 연산자 $\mathcal{S} = \{W_{1,0}, W_{0,1}, W_{1,1}, W_{2,1}, \dots, W_{d-1,1}\}$ 의 i 번째 고유 벡터의 집합일 수 있다.

[0075]

전술한 수학식 1로부터, $|\psi\rangle \in \mathcal{B}(\mathcal{S}^i)$ 일 때 채널 출력 상태 $\mathcal{N}(|\psi\rangle\langle\psi|)$ 는 이산 베일 연산자의 고유 기저와 수직이므로, 양자 통신 시스템은 투영 측정(projective measurement)을 채널 출력 상태에 대해 반복적으로 수행하여 채널 출력 상태의 폰 뉴어만 엔트로피 $S(\mathcal{N}(|\psi\rangle\langle\psi|))$ 의 추정치를 획득할 수 있다.

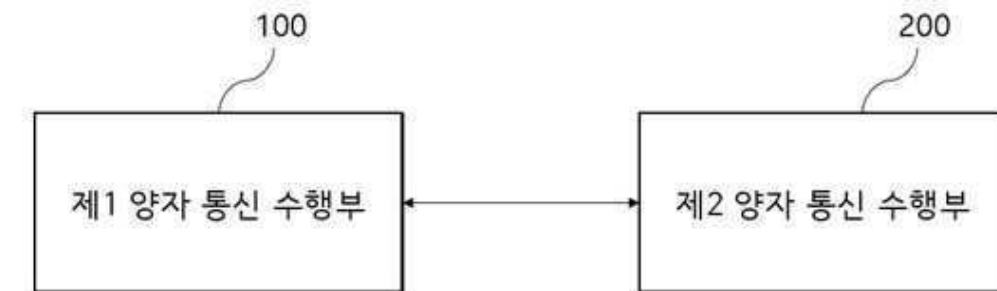
- [0076] 획득한 채널 출력 상태의 폰 뉴어만 엔트로피의 추정치로부터, 물리적으로 사용 가능하지만 채널의 특성을 나타내는 파라미터를 알 수 없는 이산 베일 채널의 Holevo 용량에 대한 추정치를 획득할 수 있다.
- [0077] 종래에는 양자 채널의 특성을 알 수 없는 경우 채널 용량을 계산하기 위해 용량을 계산하기 전에 전체 프로세스 단층 촬영(tomography)을 수행해야 했다. 프로세스 단층 촬영에는 일반적으로 d^2 측정 구성(measurement configuration)이 필요할 수 있다.
- [0078] 본 발명의 실시 예에 따른 양자 채널 용량 추정 방법은 $d+1$ 측정 구성만을 필요로 하며, 별도의 양자 얽힘을 요하지 않는다. $d+1$ 의 측정 구성은 입력 상태와 측정 설정의 합일 수 있다. 개별 큐비트에 대한 투영 측정(projective measurement)만으로 채널 용량의 Holevo 용량의 하한값을 알 수 있으므로 채널 용량 추정의 리소스를 줄일 수 있고 구현하기 용이한 효과가 있다.
- [0079] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능 뿐만 아니라 각각의 구성 요소들은 별도의 소프트웨어 모듈로도 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 메모리에 저장되고, 제어부(controller) 또는 프로세서(processor)에 의해 실행될 수 있다.
- [0080] 본 명세서와 도면에 게시된 본 발명의 실시 예들은 본 발명의 기술 내용을 쉽게 설명하고 본 발명의 이해를 돕기 위해 특정 예를 제시한 것뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 게시된 실시 예들 이외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다.

부호의 설명

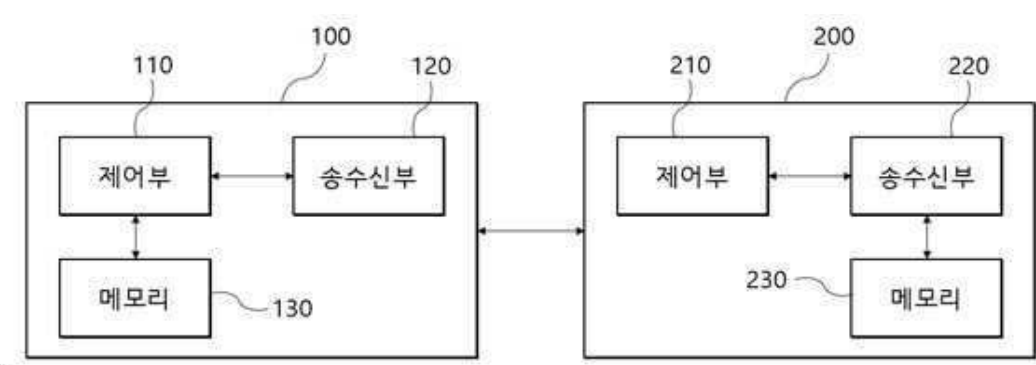
- [0082] 100: 제1 양자 통신 수행부
200: 제2 양자 통신 수행부
110, 210: 제어부
120, 220: 송수신부
130, 230: 메모리

도면

도면1



도면2



도면3

