

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0112454

(43) 공개일자 2019년10월07일

(51) 국제특허분류(Int. Cl.)

G06N 99/00 (2019.01) B82Y 10/00 (2017.01)

(52) CPC특허분류

G06N 10/00 (2019.01)

B82Y 10/00 (2013.01)

(21) 출원번호 10-2018-0034468

(22) 출원일자 2018년03월26일

심사청구일자 2018년03월26일

(71) 출원인

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 분당구 양현로 507, 313동 305호(야탑동, 매화마을주공3단지아파트)

유알리만, 주나이드

경기도 용인시 기흥구 덕영대로 1732, 경희대학교 국제캠퍼스 전자정보관 559호

(74) 대리인

김홍석

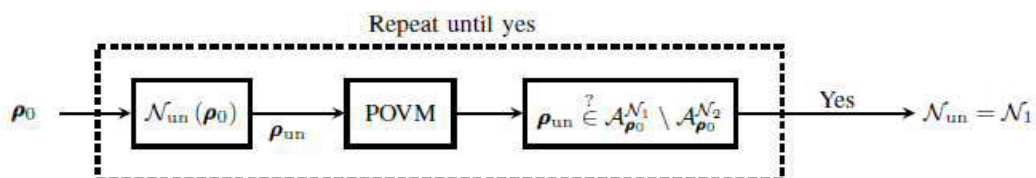
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 비대칭 양자 채널 구별 방법

(57) 요약

본 발명에 따른 비대칭(asymmetric) 양자 채널 구별 방법은, 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\mathcal{N}_{un}(\rho_0)$)를 측정하는 출력 상태 측정 과정; 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단하는 출력 상태 판단 과정; 및 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 채널 구별 과정을 포함하고, 양자 얽힘에 관한 명확한 정보 없이도 비대칭 양자 채널 구별 방법을 제공할 수 있다.

대표도 - 도4



이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1A2B2014462

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 개인연구지원사업(중견연구)

연구과제명 양자 초업힘을 이용한 하이브리드 양자통신 핵심기술연구

기 여 율 1/1

주관기관 경희대학교산학협력단

연구기간 2017.06.01 ~ 2018.05.31

명세서

청구범위

청구항 1

비대칭(asymmetric) 양자 채널 구별 방법에 있어서,

입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Mun}(\rho_0)$)를 측정하는 출력 상태 측정 과정;

상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단하는 출력 상태 판단 과정; 및

상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 채널 구별 과정을 포함하는, 비대칭 양자 채널 구별 방법.

청구항 2

제1 항에 있어서,

상기 출력 상태 판단 과정은,

제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{N_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{N_2}$ 에 기반하여, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 속하는지 여부를 판단하는 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 3

제2 항에 있어서,

상기 출력 상태가 상기 특정 출력 상태의 세트 내에 있지 않으면, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 것으로 판단될 때까지 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정을 반복하는 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 4

제3항에 있어서,

상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 속하는 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단하는 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 5

제4항에 있어서,

상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 있지 않으면,

상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단하고,

상기 확률 P2는

$$\begin{aligned}
 P_2 &= \mathbb{P} \{ \mathcal{N}_2 | \text{No UDQC in } N \text{ trials} \} \\
 &= \frac{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} | \mathcal{N}_2 \} \mathbb{P} \{ \mathcal{N}_2 \}}{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} \}} \\
 &= \frac{p_2}{p_1 (1 - \epsilon)^N + p_2}.
 \end{aligned}$$

로 결정되고,

ϵ 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)인 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 6

비대칭(asymmetric) 양자 채널 구별 방법에 있어서,

입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($Mun(\rho_0)$)를 측정하는 출력 상태 측정 과정;

상기 출력 상태에 기반하여, 상기 양자 채널이 ϵ -구별 가능(distinguishable) 기준에 따라 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한지 여부를 판단하는 출력 상태 판단 과정; 및

상기 양자 채널이 ϵ -구별 가능한 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 채널 구별 과정을 포함하는, 비대칭 양자 채널 구별 방법.

청구항 7

제6 항에 있어서,

상기 ϵ -구별 가능(distinguishable) 기준은,

$$\begin{aligned}
 \max \left\{ \max_{\rho \in \mathcal{P}_d} \mathbb{P} \left\{ \Pi^{\mathcal{N}_1}(\rho) \in \mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2} \right\}, \right. \\
 \left. \max_{\rho \in \mathcal{P}_d} \mathbb{P} \left\{ \Pi^{\mathcal{N}_2}(\rho) \in \mathcal{A}_{\rho}^{\mathcal{N}_2} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_1} \right\} \right\} \geq \epsilon
 \end{aligned}$$

이고,

$\mathcal{A}_{\rho}^{\mathcal{N}_1}$, $\mathcal{A}_{\rho}^{\mathcal{N}_2}$ 는 각각 제1 채널 및 제2 채널에 대해 가능한(achievable) 제1 출력 상태 및 제2 출력 상태이고, $\Pi^{\mathcal{N}_1}(\rho)$, $\Pi^{\mathcal{N}_2}(\rho)$ 는 각각 제1 채널 및 제2 채널의 출력에 대해 수행된 측정 결과이고, 최대화는 모든 밀도 연산자 및 측정 연산자에 대해 수행되는 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 8

제7 항에 있어서,

상기 출력 상태 판단 과정은,

제1 채널에 대해 가능한(achievable) 제1 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $\mathcal{A}_{\rho}^{\mathcal{N}_2}$ 에 기반하여, 상기 출력 상태가 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속할 확률이 특정 값 이상인지 여부를 판단하는 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 9

제8 항에 있어서,

상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속할 확률이 상기 특정 값보다 작으면, 상기 확률이 상기 특정 값 이상인 것으로 판단될 때까지 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정을 반복하고,

상기 확률이 상기 특정 값 이상인 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단하는 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 10

제9항에 있어서,

상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 확률이 상기 특정 값보다 작으면,

상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단하고,

상기 확률 P2는

$$\begin{aligned} P_2 &= \mathbb{P} \{ \mathcal{N}_2 | \text{No UDQC in } N \text{ trials} \} \\ &= \frac{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} | \mathcal{N}_2 \} \mathbb{P} \{ \mathcal{N}_2 \}}{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} \}} \\ &= \frac{p_2}{p_1 (1 - \epsilon)^N + p_2}. \end{aligned}$$

로 결정되고,

ϵ 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)인 것을 특징으로 하는, 비대칭 양자 채널 구별 방법.

청구항 11

비대칭(asymmetric) 양자 채널 구별을 수행하는 양자 시스템에서,

입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Mun}(\rho_0)$)를 수신하는 인터페이스부; 및

상기 출력 상태를 측정하고, 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단하고, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 제어부를 포함하는, 양자 시스템.

청구항 12

제11 항에 있어서,

상기 제어부는,

제1 채널에 대해 가능한(achievable) 제1 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $\mathcal{A}_{\rho}^{\mathcal{N}_2}$ 에 기반하여, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는지 여부를 판단하는 것을 특징으로 하는, 양자 시스템.

청구항 13

제12 항에 있어서,

상기 제어부는,

상기 출력 상태가 상기 특정 출력 상태의 세트 내에 있지 않으면, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 것으로 판단될 때까지 상기 출력 상태의 측정 및 상기 출력 상태의 판단을 반복하는 것을 특징으로 하는, 양자 시스템.

청구항 14

제3항에 있어서,

상기 제어부는,

상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단하는 것을 특징으로 하는, 양자 시스템.

청구항 15

제14항에 있어서,

상기 제어부는,

상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 있지 않으면,

상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단하고,

상기 확률 P2는

$$\begin{aligned} P_2 &= \mathbb{P}\{\mathcal{N}_2 | \text{No UDQC in } N \text{ trials}\} \\ &= \frac{\mathbb{P}\{\text{No UDQC in } N \text{ trials} | \mathcal{N}_2\} \mathbb{P}\{\mathcal{N}_2\}}{\mathbb{P}\{\text{No UDQC in } N \text{ trials}\}} \\ &= \frac{p_2}{p_1(1-\epsilon)^N + p_2}. \end{aligned}$$

로 결정되고,

ϵ 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)인 것을 특징으로 하는, 양자 시스템.

청구항 16

비대칭(asymmetric) 양자 채널 구별을 수행하는 양자 시스템에서,

입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Un}(\rho_0)$)를 수신하는 인터페이스부; 및

상기 출력 상태를 측정하고, 상기 출력 상태에 기반하여, 상기 양자 채널이 ϵ -구별 가능(distinguishable) 기준에 따라 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한지 여부를 판단하고, 상기 양자 채널이 ϵ -구별 가능한 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 제어부를 포함하는, 양자 시스템.

청구항 17

제6 항에 있어서,

상기 ϵ -구별 가능(distinguishable) 기준은,

$$\max \left\{ \max_{\rho \in \mathcal{P}_d} \mathbb{P} \left\{ \Pi^{\mathcal{N}_1}(\rho) \in \mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2} \right\}, \right. \\ \left. \max_{\rho \in \mathcal{P}_d} \mathbb{P} \left\{ \Pi^{\mathcal{N}_2}(\rho) \in \mathcal{A}_{\rho}^{\mathcal{N}_2} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_1} \right\} \right\} \geq \epsilon$$

이고,

$\mathcal{A}_{\rho}^{\mathcal{N}_1}$, $\mathcal{A}_{\rho}^{\mathcal{N}_2}$ 는 각각 제1 채널 및 제2 채널에 대해 가능한(achievable) 제1 출력 상태 및 제2 출력 상태이고, $\Pi^{\mathcal{N}_1}(\rho)$, $\Pi^{\mathcal{N}_2}(\rho)$ 는 각각 제1 채널 및 제2 채널의 출력에 대해 수행된 측정 결과이고, 최대화는 모든 밀도 연산자 및 측정 연산자에 대해 수행되는 것을 특징으로 하는, 양자 시스템.

청구항 18

제7 항에 있어서,
상기 제어부는,

제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{\mathcal{N}_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{\mathcal{N}_2}$ 에
기반하여, 상기 출력 상태가 특정 출력 상태 $A_{\rho}^{\mathcal{N}_1} \setminus A_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속할 확률이 특정 값 이상인지 여부를 판
단하는 것을 특징으로 하는, 양자 시스템.

청구항 19

제18 항에 있어서,
상기 제어부는,

상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속할 확률이 상기 특정 값보다 작으면, 상기 확률이 상기
특정 값 이상인 것으로 판단될 때까지 상기 출력 상태의 측정 및 상기 출력 상태의 판단을 반복하고,

상기 확률이 상기 특정 값 이상인 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성
공한 것으로 판단하는 것을 특징으로 하는, 양자 시스템.

청구항 20

제19항에 있어서,
상기 제어부는,

상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력
상태가 상기 특정 출력 상태 $A_{\rho}^{\mathcal{N}_1} \setminus A_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 있지 않으면,

상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지
채널이라고 판단하고,

상기 확률 P2는

$$\begin{aligned} P_2 &= \mathbb{P} \{ \mathcal{N}_2 | \text{No UDQC in } N \text{ trials} \} \\ &= \frac{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} | \mathcal{N}_2 \} \mathbb{P} \{ \mathcal{N}_2 \}}{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} \}} \\ &= \frac{p_2}{p_1 (1 - \epsilon)^N + p_2}. \end{aligned}$$

로 결정되고,

ϵ 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)인 것을 특징으로 하는, 양자 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 비대칭 양자 채널 구별 방법 및 이를 이용한 양자 시스템에 관한 것이다. 보다 상세하게는, 양자 채널들의 비대칭 비-모호(unambiguous) 구별 방법 및 양자 시스템에 관한 것이다.

배경 기술

[0002] 양자 채널은 양자 정보 이론 분야에서 중요한 역할을 한다. 하지만, 양자 채널은 측정 가능하지 않을 수 있고, 이론적 결과의 정확한 구현 및 반복을 위해 예측되고 근사적으로 모델링될 필요가 있다. 이와 관련하여, 이용되는 채널 모델에 대한 지식 없이 적절하게 실행될 수 없는 몇 가지 정보 이론 태스크가 있다. 예를 들어, 특정

채널 모델에 대하여 설계된 채널 코드는 다른 채널 모델에 대하여 열화된 성능을 제공하거나, 양자 키 분배 프로토콜은 일반적으로 이상이거나 또는 이레이저(erasure) 채널을 고려한다. 따라서, 근본적인 잡음 모델을 정확히 식별하고 이를 고려할 필요가 있다.

- [0003] 이와 관련하여, 이전에는 주어진 미지의 양자 채널에 대하여 적절한 채널 모델을 찾는 것에 대해 중점적으로 논의되었다. 이러한 문제는 세 가지 상이한 카테고리로 분류 가능하다.
- [0004] 첫 번째 카테고리는 미지의 채널 모델의 파라미터를 찾는 문제, 예컨대 파울리 큐비트 채널의 파라미터를 예측하는 절차가 제안되었다.
- [0005] 두 번째 카테고리는 양자 얽힘의 응용으로서 도입된 양자 채널 식별에 관한 것이다. 이후에, 양자 상태의 유니터리 변동의 식별 문제가 논의되었다. 이러한 문제는 일반적으로 파라미터 예측 문제로 논의되었다. 따라서, 이러한 채널 식별 문제는 일반적으로 양자 예측 분야의 발전으로부터 수혜를 받을 수 있다.
- [0006] 세 번째 카테고리는 채널 구분(discrimination)에 관한 것이다. 여기서, "구분"의 의미는 양자 상태 구분의 문제에서 사용되는 "구분"을 의미한다. 이와 관련하여, 채널 구분 문제는 알려진 채널들의 세트로부터 미지의 양자 채널을 구분하는 것에 관한 것이다. 하지만, 이러한 채널 구분은 유니터리 동작의 구분 등 특수한 상황에서만 도입되었다. 따라서, 알려진 채널들의 세트로부터 미지의 양자 채널을 구분하는 일반적인 방법에 대해서는 전혀 제시된 바가 없다는 문제점이 있었다.
- [0007] 특히, 상호 간에 비대칭 구조의 비대칭 양자 채널에서 비대칭 양자 채널 구별이 용이하지 않다는 문제점이 있었다. 또한, 양자 채널이 분명한 구분이 용이하지 않은 경우, 양자 채널을 구분하는 확률적인 방법에 대해 전혀 제시된 바가 없다는 문제점이 있었다.

발명의 내용

해결하려는 과제

- [0008] 따라서, 본 발명에서 해결하고자 하는 과제는, 비대칭 양자 채널 구별 방법을 제공하는 것을 목표로 한다.
- [0009] 또한, 본 발명에서 해결하고자 하는 과제는, 양자 채널이 분명한 구분이 용이하지 않은 경우, 양자 채널을 구분하는 확률적인 방법을 제공하는 것을 목표로 한다.

과제의 해결 수단

- [0010] 상기와 같은 과제를 해결하기 위한 본 발명에 따른 비대칭(asymmetric) 양자 채널 구별 방법은, 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Mun}(\rho_0)$)를 측정하는 출력 상태 측정 과정; 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단하는 출력 상태 판단 과정; 및 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 채널 구별 과정을 포함하고, 양자 얽힘에 관한 명확한 정보 없이도 비대칭 양자 채널 구별 방법을 제공할 수 있다.
- [0011] 일 실시 예에서, 상기 출력 상태 판단 과정은, 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $\mathcal{A}_{\rho}^{\mathcal{N}_2}$ 에 기반하여, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는지 여부를 판단할 수 있다.
- [0012] 일 실시 예에서, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 있지 않으면, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 것으로 판단될 때까지 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정을 반복할 수 있다.
- [0013] 일 실시 예에서, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.
- [0014] 일 실시 예에서, 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 있지 않으면, 상기 제2 채널이 상기

미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단할 수 있다. 이때, 상기 확률 P2는 수학적 13 및 수학적 14에 의해 결정되고, ε 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)일 수 있다.

[0015] 본 발명의 다른 양상에 따른 비대칭(asymmetric) 양자 채널 구별 방법은 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($Mun(\rho_0)$)를 측정하는 출력 상태 측정 과정; 상기 출력 상태에 기반하여, 상기 양자 채널이 ε -구별 가능(distinguishable) 기준에 따라 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한지 여부를 판단하는 출력 상태 판단 과정; 및 상기 양자 채널이 ε -구별 가능한 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 채널 구별 과정을 포함한다.

[0016] 일 실시 예에서, 상기 ε -구별 가능(distinguishable) 기준은, 수학적 10에 의해 결정되고, 수학적 10에서 $A_{\rho}^{N_1}$, $A_{\rho}^{N_2}$ 는 각각 제1 채널 및 제2 채널에 대해 가능한(achievable) 제1 출력 상태 및 제2 출력 상태이고, $\Pi^{N_1}(\rho)$, $\Pi^{N_2}(\rho)$ 는 각각 제1 채널 및 제2 채널의 출력에 대해 수행된 측정 결과이고, 최대화는 모든 밀도 연산자 및 측정 연산자에 대해 수행될 수 있다.

[0017] 일 실시 예에서, 상기 출력 상태 판단 과정은, 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{N_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{N_2}$ 에 기반하여, 상기 출력 상태가 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 속할 확률이 특정 값 이상인지 여부를 판단할 수 있다.

[0018] 일 실시 예에서, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속할 확률이 상기 특정 값보다 작으면, 상기 확률이 상기 특정 값 이상인 것으로 판단될 때까지 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정을 반복할 수 있다. 이때, 상기 확률이 상기 특정 값 이상인 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.

[0019] 일 실시 예에서, 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 확률이 상기 특정 값보다 작으면, 상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단할 수 있다. 이때, 상기 확률 P2는 수학적 13 및 수학적 14에 의해 결정되고, ε 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)일 수 있다.

[0020] 본 발명의 또 다른 양상에 따른 비대칭(asymmetric) 양자 채널 구별을 수행하는 양자 시스템은, 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($Mun(\rho_0)$)를 수신하는 인터페이스부; 및 상기 출력 상태를 측정하고, 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단하고, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 제어부를 포함한다.

[0021] 일 실시 예에서, 상기 제어부는, 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{N_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{N_2}$ 에 기반하여, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 속하는지 여부를 판단할 수 있다.

[0022] 일 실시 예에서, 상기 제어부는, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 있지 않으면, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 것으로 판단될 때까지 상기 출력 상태의 측정 및 상기 출력 상태의 판단을 반복할 수 있다.

[0023] 일 실시 예에서, 상기 제어부는, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 속하는 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.

[0024] 일 실시 예에서, 상기 제어부는, 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 있지 않으면, 상기 제2

채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단할 수 있다. 이때, 상기 확률 P2는 수학적 식 13 및 수학적 식 14에 의해 결정되고, ε 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)일 수 있다.

[0025] 본 발명의 또 다른 양상에 따른 비대칭(asymmetric) 양자 채널 구별을 수행하는 양자 시스템은, 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Nun}(\rho_0)$)를 수신하는 인터페이스부; 및 상기 출력 상태를 측정하고, 상기 출력 상태에 기반하여, 상기 양자 채널이 ε -구별 가능(distinguishable) 기준에 따라 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한지 여부를 판단하고, 상기 양자 채널이 ε -구별 가능한 경우, 상기 양자 채널 구별이 성공한 것으로 판단하는 제어부를 포함한다.

[0026] 일 실시 예에서, 상기 ε -구별 가능(distinguishable) 기준은, 수학적 식 10에 의해 결정되고, 수학적 식 10에서 $A_{\rho}^{N_1}$, $A_{\rho}^{N_2}$ 는 각각 제1 채널 및 제2 채널에 대해 가능한(achievable) 제1 출력 상태 및 제2 출력 상태이고, $\Pi^{N_1}(\rho)$, $\Pi^{N_2}(\rho)$ 는 각각 제1 채널 및 제2 채널의 출력에 대해 수행된 측정 결과이고, 최대화는 모든 밀도 연산자 및 측정 연산자에 대해 수행될 수 있다.

[0027] 일 실시 예에서, 상기 제어부는, 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{N_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{N_2}$ 에 기반하여, 상기 출력 상태가 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 속할 확률이 특정 값 이상인지 여부를 판단할 수 있다.

[0028] 일 실시 예에서, 상기 제어부는, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속할 확률이 상기 특정 값보다 작으면, 상기 확률이 상기 특정 값 이상인 것으로 판단될 때까지 상기 출력 상태의 측정 및 상기 출력 상태의 판단을 반복하고, 상기 확률이 상기 특정 값 이상인 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.

[0029] 일 실시 예에서, 상기 제어부는, 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 있지 않으면, 상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단할 수 있다. 이때, 상기 확률 P2는 수학적 식 13 및 수학적 식 14에 의해 결정되고, ε 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p_1 및 p_2 는 사전 확률(priori probabilities)일 수 있다.

발명의 효과

[0030] 본 발명에 따른 방법은, 양자 얽힘에 관한 명확한 정보 없이도 비대칭 양자 채널 구별 방법을 제공할 수 있다는 장점이 있다.

[0031] 또한, 본 발명에 따른 방법은, 양자 채널이 분명한 구분이 용이하지 않은 경우, 출력 상태 측정 및 출력 상태 판단의 반복을 통해 양자 채널을 구분하는 확률적인 방법을 제공할 수 있다는 장점이 있다.

도면의 간단한 설명

[0032] 도 1은 본 발명에 따른 비대칭 양자 채널 구별 방법을 수행하는 양자 시스템을 도시한다.

도 2는 본 발명에 따른 서버 시스템들의 상세 구성을 도시한다.

도 3은 본 발명과 관련하여 양자 채널의 예측 방법을 수행하기 위한 일 예시를 나타낸다.

도 4는 본 발명에 따른 채널 구별(discrimination)과 연관된 절차를 수행하는 상세한 구성을 나타낸다.

도 5는 본 발명에 따른 채널 사용 N에 대한 메트릭 확률을 나타낸 것이다.

도 6은 본 발명의 일 실시 예에 따른 비대칭(asymmetric) 양자 채널 구별 방법의 흐름도를 나타낸다.

도 7은 본 발명의 다른 실시 예에 따른 비대칭(asymmetric) 양자 채널 구별 방법의 흐름도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0033] 상술한 본 발명의 특징 및 효과는 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시 예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 개시형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 명세서에서 사용한 용어는 단지 특정한 실시 예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다.
- [0034] 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용한다.
- [0035] 제1, 제2등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.
- [0036] 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. "및/또는"이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.
- [0037] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미가 있다.
- [0038] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않아야 한다.
- [0039] 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈", "블록" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.
- [0040] 이하, 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 당해 분야에 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 설명한다. 하기에서 본 발명의 실시 예를 설명함에 있어, 관련된 공지의 기능 또는 공지의 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다.
- [0041] 이하, 본 발명에 따른 비대칭(asymmetric) 양자 채널 구별 방법 및 장치에 대해 살펴보기로 하자.
- [0042] 도 1은 본 발명에 따른 비대칭 양자 채널 구별 방법을 수행하는 양자 시스템을 도시한다. 도 1에 도시된 바와 같이, 양자 시스템은 복수의 서브 시스템을 포함하고, 편의상 제1 서브 시스템(100)과 제2 서브 시스템(200)이 포함된 것으로 표현할 수 있다. 하지만, 상기 제1 및 제2 서브 시스템(100, 200)에만 한정되는 것이 아니라, 임의의 개수의 서브 시스템 간에도 적용될 수 있다. 한편, 상기 제1 및 제2 서브 시스템(100, 200)은 임의의 양자 기기일 수 있고, 하나의 양자 기기 내의 서로 다른 컴포넌트일 수 있다.
- [0043] 한편, 도 2는 본 발명에 따른 서브 시스템들의 상세 구성을 도시한다. 도 2에 도시된 바와 같이, 제1 서브 시스템(100)은 제어부(110), 인터페이스부(120), 및 메모리(130)를 포함한다. 또한, 제2 서브 시스템(200)은 제어부(210), 인터페이스부(220), 및 메모리(230)를 포함한다. 여기서, 인터페이스부(120, 220)는 양자 채널(quantum channel)을 이용하는 양자 인터페이스부일 수 있다. 또한, 인터페이스부(120, 220)는 일반 채널(classical channel)을 이용하는 일반 인터페이스부를 포함할 수 있다. 한편, 메모리(130, 230)는 양자 정보를 저장하는 양자 메모리일 수 있다. 또한, 메모리(130, 230)는 일반 정보를 저장하는 일반 메모리를 포함할 수 있다.
- [0044] 먼저, 도 1을 참조하여, 본 발명에 따른 비대칭 양자 채널 구별 방법에 대하여 살펴보면 다음과 같다. 제1 서브 시스템(100)은 양자 채널을 통해 정보를 전송하고, 제2 서브 시스템(200)은 양자 채널 구별을 통해 전송된 정보를 수신할 수 있다. 한편, 제2 서브 시스템(200)이 양자 채널을 통해 정보를 전송하고, 제1 서브 시스템(100)은 양자 채널 구별을 통해 전송된 정보를 수신할 수도 있다.
- [0045] 다음으로, 도 2를 참조하여, 본 발명에 따른 비대칭 양자 채널 구별 방법에 대해 살펴보기로 하자. 이와 관련하여, 제1 서브 시스템(100)의 상세 구성을 참조하여 설명되지만, 이에 한정되지 않고, 제2 서브 시스템(200)의 컴포넌트에서 이러한 동작을 수행하는 것도 가능하다.
- [0046] 인터페이스부(120)는 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Min}(\rho_0)$)를 수신한다. 한편, 제어부(110)는

출력 상태를 측정하고, 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단할 수 있다. 이때, 제어부(110)는 출력 상태가 특정 출력 상태의 세트 내에 속하는 경우, 양자 채널 구별이 성공한 것으로 판단할 수 있다.

[0047] 또는, 제어부(110)는 출력 상태를 측정하고, 상기 출력 상태에 기반하여, 상기 양자 채널이 ε -구별 가능(distinguishable) 기준에 따라 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한지 여부를 판단할 수 있다. 이때, 제어부(110)는 양자 채널이 ε -구별 가능한 경우, 상기 양자 채널 구별이 성공한 것으로 판단할 수 있다.

[0048] 한편, 메모리(130, 230)에서 양자 정보 또는 일반 정보를 저장하도록 구성된다. 전송된 바와 같이, 메모리(130, 230)는 양자 메모리 또는 일반 메모리로 지칭될 수 있다.

[0049] 다음으로, 본 발명에 따른 비대칭(asymmetric) 양자 채널 구별과 관련하여, 아래에서 상세히 살펴보기로 하자.

[0050] 먼저, 양자 채널들의 구별 가능성(distinguishability)에 대해 살펴보면 다음과 같다. 유한 차원의 힐버트 공간 H 를 고려하면, 양자 상태 $\rho \in H$ 에 속하고, ρ 는 단위 트레이스를 갖는 포지티브 연산자에 해당한다. 즉, $\rho \geq 0$ 이고, $\text{tr}(\rho) = 1$ 이다. 이때, D_d 로 표시되는 d -차원 힐버트 공간을 통해 모든 밀도 행렬들의 세트가 표시될 수 있다. 또한, 순수 양자 상태를 표시하기 위해 C^d (차원 d 의 복소 벡터 공간)의 단위 벡터가 또한 사용될 수 있다. 양자 채널 $N(\rho)$ 는 H_A 의 엘리먼트들로 H_B 의 엘리먼트로 변환하는 완전 포지티브 트레이스 보존 (CTTP: Completely Positive Trace Preserving) 맵(map)이다. 윗 첨자(superscript)에 의해 H_A 및 H_B 에 관한 연산자 (및 상태)를 구별할 수 있다. 즉, $\hat{I}^A \otimes \mathcal{N}^B(\rho^A \otimes \sigma^B)$ 는 H_B 에 N , 및 H_A 에 단위 연산을 적용한 것이다. 양자 채널을 크라우스(Kraus) 연산자 M_i 를 이용하여 아래의 수학적 식 1과 같이 표현할 수 있다.

수학적 식 1

$$\mathcal{N}(\rho) = \sum_i M_i \rho M_i^\dagger$$

[0051]

여기서, 크라우스 연산자는 $\sum_i M_i^\dagger M_i = I$ 의 관계를 만족한다.

[0052]

A. 문제 정의

[0053]

[0054] 양자 채널 N 을 다음과 같이 고려할 수 있다. 즉, 양자 잡음의 정확한 특성은 알려지지 않았지만, 양자 채널 N 이 k 개의 상이한 가능한 채널들, 즉 $\{N_1, \dots, N_k\}$ 의 세트에 속하는 것이 보장된다고 가정할 수 있다. 본 발명에 따른 목표는 주어진 양자 채널 N 중에서 특정 액션을 가장 잘 설명하는 가능한 채널 N_i 를 식별하는 것이다. 이와 관련하여, 이러한 채널 특성이 비대칭인 경우를 특히 고려하기로 한다. 이와 관련하여, 비대칭(asymmetric)인 경우, 즉 N_1 이 N_2 로부터 완벽하게 구별 가능하지만, N_2 가 N_1 로부터 완벽하게 구별 가능하지 않은 경우, N_1 및 N_2 를 결정할 필요가 있다. 이때, $i = 1, 2, \dots, k$ 에 대하여 채널 N_i 가 잡음 특성에 의해 정의되지만 심각도(severity)에 의해 정의되지는 않음을 주목하자. 예를 들어, 임의의 값일 수 있지만, 비-축퇴(non-degenerate)에 해당하는 ε 에 대하여 N_i 는 아래의 수학적 식 2와 같이 양자 이레이저(eraser) 채널이 될 수 있다.

수학적 식 2

$$\mathcal{N}_\varepsilon(\rho) = (1 - \varepsilon)\rho + \varepsilon|\varepsilon\rangle\langle\varepsilon|$$

[0055]

[0056] 여기서, $|\varepsilon\rangle \perp \mathcal{H}$ 은 이레이저 신호이다.

[0057] 한편, 양자 채널의 예측 방법에 대해 상세하면 살펴보면 다음과 같다.

[0058] B. 양자 채널 모델

[0059] 이와 관련하여, 도 3은 본 발명과 관련하여 양자 채널의 예측 방법을 수행하기 위한 일 예시를 나타낸다. 도 2 및 도 3을 참조하면, 제어부(120, 220)가 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태(Mun)을 판단한다. 도 3에 도시된 바와 같이, 제어부(120, 220)는 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($Mun(\rho_0)$)를 수신하고, POVM (Positive-Operator Valued Measurement)를 수행한다. 다음으로, 제어부(120, 220)는 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단 (또는 예측)할 수 있다. 이때, 특정 출력 상태의 세트 내에 속하는지 여부를 판단 (또는 예측)하기 위해 모든 상태 변수를 이용하여 예측할 수 있다.

[0060] 전술한 첫 번째 접근법은 양자 채널의 파라미터 예측에 관한 것으로, 수학적 3에 의해 표현 가능하다.

수학적 3

$$\mathcal{N}_\theta(\rho) = \sum_i p_i(\theta) M_i \rho M_i^\dagger$$

[0061]

[0062] 여기서, 채널 크라우스 연산자 M_i 는 알려져 있고, 채널 파라미터 p_i 는 θ 에 의해 추정 가능하다. 예를 들어, 이러한 클래스는 수학적 4와 같이 큐비트 비-편파(depolarizing) 채널의 비-편파 파라미터를 예측하는 문제를 포함한다.

수학적 4

$$\mathcal{N}_\theta(\rho) = \frac{1-\theta}{d} I_d + \theta \rho$$

[0063]

[0064] 두 번째 접근법은 수학적 5와 같이 표현 가능하다.

수학적 5

$$\mathcal{N}_\theta(\rho) = \sum_i M_i(\theta) \rho M_i^\dagger(\theta)$$

[0065]

[0066] 여기서, 크라우스 연산자의 전체 구조는 실수 형태의, 연속 파라미터 θ 에 달려있다.

[0067] 이러한 두 가지 접근법을 살펴보면, 첫 번째 접근법이 두 번째 접근법의 특수한 (그리고 단순한) 경우로 간주될 수 있다. 한편, 두 가지 접근법들은 $\mathbb{E}\{(\theta_{\text{actual}} - \theta_{\text{est}})^2\}$ 의 제곱 평균 에러를 최소화하는 파라미터 θ 를 예측한다.

[0068] 이러한 두 가지 시나리오는 UDQC의 문제와는 근본적으로 상이하다. 이와 관련하여, 주어진 세트 k 개의 가능한 구조로부터 채널의 구조를 모호성 없이(unambiguously) 식별할 수 있다. 한편, k 개의 가능한 구조는 수학적 6으로 표현 가능하다.

수학식 6

$$\mathcal{N}_{\text{un}} \in \{\mathcal{N}_1, \dots, \mathcal{N}_k\}$$

[0069]

[0070]

[0071]

한편, 수학식 5의 가능한 구조의 세트 중에서 어떤 엘리먼트가 실제로 제공되는지를 판별하는 것이 중요하다.

이와 관련하여, 도 4는 본 발명에 따른 채널 구별(discrimination)과 연관된 절차를 수행하는 상세한 구성을 나타낸다. 도 2 및 도 4를 참조하면, 제어부(120, 220)가 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\mathcal{M}_{\text{un}}$)을 판단한다. 도 4 도시된 바와 같이, 제어부(120, 220)는 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\mathcal{M}_{\text{un}}(\rho_0)$)를 수신하고, POVM (Positive-Operator Valued Measurement)를 수행한다. 다음으로, 제어부(120, 220)는 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단 (또는 예측)할 수 있다. 이때, 특정 출력 상태의 세트 내에 속하는지 여부를 판단 (또는 예측)하기 위해 모든 상태 변수를 이용하여 예측하는 것이 아니라 일부 출력 상태만을 이용할 수 있다. 구체적으로, 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{\mathcal{N}_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{\mathcal{N}_2}$ 에 기반하여, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{\mathcal{N}_1} \setminus A_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는지 여부를 판단할 수 있다.

[0072]

이와 관련하여, 양자 채널의 대칭 구별가능성(symmetric distinguishability)가 고려될 수 있다. 스펙트럴 분해 $\rho = \sum_k p_k |\psi_k\rangle \langle \psi_k|$ 를 갖는 상태 ρ 에 대하여 상태 ρ 의 지원은 $\text{supp}(\rho) = \text{span}\{|\psi_k\rangle : p_k > 0\}$ 이다. $\text{supp}(\rho_0) \cap \text{supp}(\rho_1) = \{0\}$ 이면 두 개의 양자 상태 ρ_1 및 ρ_2 는 비-결합(disjoint)이다. 또한, 일부 입력 $|\psi^{RQ}\rangle$ 에 대한 출력 상태 $(I^R \otimes \mathcal{N}_1^Q)(|\psi^{RQ}\rangle)$ 및 $(I^R \otimes \mathcal{N}_2^Q)(|\psi^{RQ}\rangle)$ 가 비-결합이면 두 양자 연산자 $\mathcal{M}_1$ 및 $\mathcal{M}_2$ 는 비-결합이다.

[0073]

반면에, 얽힌 입력 상태가 이용 가능하지 않은 경우, 엄격 조건을 완화하는 경우를 고려하면 다음과 같다. 이와 관련하여, 얽힘 없이 완전한 구분가능성이 일반적으로 가능하지 않더라도 하나의 채널을 다른 채널과 적어도 구별하기 위해 위의 theorem의 엄격 조건을 완화하는 것을 고려할 수 있다. 일단 기반 구조가 식별되면, 양자 채널의 파라미터 예측 방법이 식별된 구조의 파라미터들을 예측하는데 사용된다.

[0074]

C. 비대칭 구별가능성 프레임워크 (Asymmetric Distinguishability Framework)

[0075]

적어도 일 방향 구분가능성이 가능한 구별가능성 프레임워크를 도입할 수 있다. 이와 관련하여, 두 개의 가능한 채널의 경우에 구별가능성을 고려할 수 있다.

[0076]

먼저, 비대칭 특성의 문제를 고려한다. 미지의 주어진 채널 $\mathcal{N}_{\text{un}}$ 과 알려진 세트의 가능한 채널 모델들을 고려한다. 가능한 채널 모델들로 $\mathcal{M}_1$ 및 $\mathcal{M}_2$ 를 고려할 수 있다. 비대칭 구별 가능성은 기반 미지 채널이 실제로 $\mathcal{M}_1$ 이지만, $\mathcal{M}_2$ 는 그렇지 않은 경우, 채널 모델을 모호하지 않게 발견하는 것이다. 기결정된 최대 개수의 단계 내에서 비-모호성 구별이 실패한다면, 채널의 특성에 관한 확률적 예측을 여전히 수행할 수 있다.

[0077]

Definition 1 (달성 가능한 출력 상태): 고정 입력 상태 ρ_0 에 대하여, 채널 $\mathcal{M}$ 에 대해 달성 가능한 출력 상태는 수학식 7로 표현 가능하다.

수학식 7

$$\mathcal{A}_{\rho_0}^{\mathcal{N}} := \{\rho : \text{tr}(\rho \mathcal{N}(\rho_0)) > 0, \rho \in \mathcal{D}_d\}$$

[0078]

[0079] Theorem 1 (비대칭 비-모호 구별 가능한 채널) 두 개의 채널들 $\mathcal{N}_1$ 및 $\mathcal{N}_2$ 가 수학식 8을 만족하는 상태 ρ_0 가 존재하면 비대칭 비-모호 구별 가능하다.

수학식 8

$$\mathcal{A}_{\rho_0}^{\mathcal{N}_1} \cup \mathcal{A}_{\rho_0}^{\mathcal{N}_2} \neq \mathcal{A}_{\rho_0}^{\mathcal{N}_1} \cap \mathcal{A}_{\rho_0}^{\mathcal{N}_2}$$

[0080]

[0081] Proof: 수학식 8의 부등호 조건으로 인해, $\sigma \in \mathcal{A}_{\rho_0}^{\mathcal{N}_1}$ 가 되지만 $\sigma \notin \mathcal{A}_{\rho_0}^{\mathcal{N}_2}$ 가 되게 하는 상태 σ 가 존재하도록 직접 변환된다. σ 의 지원에 관한 프로젝터를 이용하여 미지 상태 $\mathcal{N}_{\text{un}}(\rho_0)$ 의 출력을 계속 측정한다. 측정 결과를 통해 결과가 σ 의 지원에 관한 것을 지시할 때마다, 채널은 분명히 $\mathcal{N}_1$ 이고 $\mathcal{N}_2$ 는 아닐 것이다.

[0082] 반면에, 두 개의 채널 $\mathcal{N}_1$ 및 $\mathcal{N}_2$ 를 고려하면, $\mathcal{N}_1$ 은 $\mathcal{N}_2$ 와 특정 단계 내에 비-모호하게 구별 가능하다. 채널 특성을 관측하는 유일한 방법은 채널의 출력 상태에 관한 효과를 통해 가능하다. 따라서, $\mathcal{N}_1$ 의 출력 ρ_1 및 $\mathcal{N}_2$ 의 출력 ρ_2 는 비-모호하게 구별 가능하다. 임의의 두 상태 ρ_1 및 ρ_2 에 대하여, 비-모호하게 구별 가능하기 위해, 이들은 선형적으로 독립적이어야 한다. 이는 $\sigma \in \mathcal{A}_{\rho_0}^{\mathcal{N}_1}$ 및 $\sigma \notin \mathcal{A}_{\rho_0}^{\mathcal{N}_2}$ 가 되도록 하는 σ 가 존재하는 것을 보장하고, 따라서 수학식 8이 성립한다.

[0083] 위의 theorem에서의 설명은 세트 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 또는 $\mathcal{A}_{\rho}^{\mathcal{N}_2} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_1}$ 가 empty 하지 않도록 전환될 수 있다. 상기 theorem에 대한 다음의 corollary를 얻을 수 있다.

[0084] Corollary 1 : $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 가 non-empty 하면 $\mathcal{N}_1$ 은 $\mathcal{N}_2$ 와 구별 가능하고, $\mathcal{A}_{\rho}^{\mathcal{N}_2} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_1}$ 가 non-empty하면 $\mathcal{N}_2$ 는 $\mathcal{N}_1$ 과 구별 가능하다고 할 수 있다.

[0085] 대칭 UDQC가 가능하다면, 비대칭 UDQC의 조건은 자동으로 만족한다고 할 수 있다. 이러한 관점에서, 대칭 UDQC가 비대칭 UDQC의 특수한 경우로 간주될 수 있다.

[0086] 일반적으로 구별 가능 절차는 채널의 1회 사용 이상을 요구한다. 하지만, 일부 세트의 채널은 한 번의 채널 사용으로 구별 가능할 수 있다. 이러한 한 번의 채널 사용으로 구별 가능한 채널을 원-샷 구별 가능 채널이라고 지칭할 수 있다.

[0087] Theorem 2 (원-샷 구별 가능 채널): 두 채널 $\mathcal{N}_1$ 및 $\mathcal{N}_2$ 는 수학식 9를 만족하도록 상태 $\sigma_1 \in \mathcal{A}_{\rho_0}^{\mathcal{N}_1}$ 및 $\sigma_2 \in \mathcal{A}_{\rho_0}^{\mathcal{N}_2}$ 가 존재하는 경우에만 원-샷 구별 가능하다.

수학식 9

$$\text{tr}(\sigma_1 \sigma_2) = 0$$

[0088]

[0089] 여기서, $\text{tr}(\sigma_1 \mathcal{N}_1(\rho_0)) = 1$ 및 $\text{tr}(\sigma_2 \mathcal{N}_2(\rho_0)) = 1$ 의 관계가 성립한다.

[0090] *Proof:* 두 양자 채널의 원-샷 구별 가능 채널의 필요 충분조건은 동일 입력에 대한 두 채널의 출력 상태의 원-샷 구별 가능성의 필요 충분조건으로부터 유추 가능하다. 위의 theorem의 설명에서의 조건은 원-샷 구별 가능성이 되는 두 개의 채널의 출력에 관한 필요 충분조건이다.

수학식 10

$$\max_{\Pi} \left\{ \max_{\rho \in \mathcal{D}_d} \mathbb{P} \left\{ \Pi^{\mathcal{N}_1(\rho)} \in \mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2} \right\}, \right. \\ \left. \max_{\rho \in \mathcal{D}_d} \mathbb{P} \left\{ \Pi^{\mathcal{N}_2(\rho)} \in \mathcal{A}_{\rho}^{\mathcal{N}_2} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_1} \right\} \right\} \geq \epsilon$$

[0091]

[0092] 여기서, 최대화는 모든 밀도 연산자 및 측정 연산자에 대해 수행되고, $\Pi^{\mathcal{N}_1(\rho)}$ 는 측정 연산자 Π 를 이용한 채널 출력 $\mathcal{N}_1(\rho)$ 에 대하여 수행된 측정된 값이다.

[0093] 이러한 정의는 채널 구분 절차의 예상된 성능을 자연스럽게 유도하는 것을 가능하게 한다. 채널 구분 절차는 가능한 채널 모델 특성에 관계없이, 파라미터 ϵ 에 관한 결과에 기반할 수 있다. 파라미터 ϵ 은 채널이 한 번만 사용되는 경우에만 채널 출력에 대해 수행된 결과의 확률에 대응한다. 일반성이 유지되는 범위에서, $\mathcal{N}_1$ 에 대한 비대칭성을 가정할 수 있다. 즉, 미지 채널이 $\mathcal{N}_1$ 이면 UDQC가 수행될 수 있고,

$$\max_{\rho \in \mathcal{D}_d} \mathbb{P} \left\{ \Pi^{\mathcal{N}_1(\rho)} \in \mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2} \right\} \geq \epsilon$$

를 만족한다.

[0094] 아래의 두 가지 고유 특징의 관점에서 제안된 방식의 성능에 대하여 검토할 수 있다.

[0095] 1) 미지 채널이 $\mathcal{N}_1$ 인 경우, N번의 시도 내에 UDQC가 성공할 확률(P1)

[0096] 2) N번의 시도 내에 UDQC가 성공하지 못한 경우, 미지 채널이 $\mathcal{N}_2$ 일 확률 (P2)

[0097] 단일 시도 내에 UDQC 성공 확률이 ϵ 이기 때문에, N번의 시도에서 성공 확률은 수학식 11 및 12와 같다.

수학식 11

$$P_1 = \mathbb{P} \{ \text{Success in } N \text{ trials} \}$$

[0098]

수학식 12

$$= 1 - (1 - \epsilon)^N$$

[0099]

[0100] 한편, $\epsilon > 0$ 이기 때문에, N이 증가함에 따라 N번의 시도에서 성공 확률은 1에 수렴한다.

[0101] 두 번째 정량화에 대한 베이지안(Bayesian) 접근법을 고려하면 다음과 같다. 이와 관련하여, 채널 $\mathcal{N}_1$ 및 $\mathcal{N}_2$ 가 사전(prior) 확률 p_1 및 p_2 를 갖는다고 가정하면, 미지 채널이 $\mathcal{N}_2$ 일 확률 (P2)은 수학식 13 및 14와 같다.

수학식 13

$$P_2 = \mathbb{P} \{ \mathcal{N}_2 | \text{No UDQC in } N \text{ trials} \}$$

$$= \frac{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} | \mathcal{N}_2 \} \mathbb{P} \{ \mathcal{N}_2 \}}{\mathbb{P} \{ \text{No UDQC in } N \text{ trials} \}}$$

수학식 14

$$= \frac{p_2}{p_1 (1 - \epsilon)^N + p_2}$$

전술한 확률 메트릭 P1 및 P2는 각각 ϵ 및 사전 확률에 기반한다. 알려진 채널들의 쌍에 대하여, 일단 채널의 사전 확률이 알려지고 ϵ 의 값이 결정되면, P1 및 P2의 관점에서 제안 방식의 예상 성능을 판단할 수 있다. 두 메트릭 값이 1에 빠르게 수렴할수록, 제안된 UDQC 방식의 성능이 더 양호함을 나타낸다.

도 5는 본 발명에 따른 채널 사용 N에 대한 메트릭 확률을 나타낸 것이다. i) $\epsilon = 0.01, p_1 = 0.8$, ii) $\epsilon = 0.3, p_1 = 0.2$, iii) $\epsilon = 0.1, p_1 = 0.5$ 에 대하여, 채널 사용 N에 대한 메트릭 확률은 다음과 같다. 모든 세트의 파라미터에 대하여, P1 및 P2는 채널 사용 횟수가 증가함에 따라 단조 증가한다. 또한, ϵ 의 값이 클수록, 두 메트릭 값은 1에 빨리 수렴한다. 이에 따라 더 적은 횟수의 시도에 의해 UDQC가 성공할 수 있다. 반면에, 이러한 결과가 관측되지 않으면 채널이 N_0 라고 확신할 수 있다.

III. Examples

표 1은 본 발명에 따른 큐빗 채널들을 나열한다. 한편, 표 2는 본 발명에 따른 큐빗 채널들의 구분 가능성 및 최적 입력과 UDQC 성공 확률 ϵ 을 나열한 것이다.

표 1

Channel	Definition
Identity	$\mathcal{N}_I(\rho) = \rho$
Bit flip	$\mathcal{N}_{bf}(\rho) = (1 - p_{bf})\rho + p_{bf}X\rho X^\dagger$
Phase flip	$\mathcal{N}_{pf}(\rho) = (1 - p_{pf})\rho + p_{pf}Z\rho Z^\dagger$
Depolarizing	$\mathcal{N}_{de}(\rho) = (1 - p_{de})\rho + p_{de}\pi$
Quantum erasure	$\mathcal{N}_\epsilon(\rho) = (1 - p_\epsilon)\rho + p_\epsilon \epsilon\rangle\langle\epsilon $

표 2

$\mathcal{N}_1$	$\mathcal{N}_2$	Distinguishable	Optimal Input	ϵ
$\mathcal{N}_{\text{bf}}(\rho)$	$\mathcal{N}_1(\rho)$	$\mathcal{N}_1$	$ 0\rangle\langle 0 $	p_{bf}
$\mathcal{N}_{\text{pf}}(\rho)$	$\mathcal{N}_1(\rho)$	$\mathcal{N}_1$	$ +\rangle\langle + $	p_{pf}
$\mathcal{N}_{\text{de}}(\rho)$	$\mathcal{N}_1(\rho)$	$\mathcal{N}_1$	Any $ \psi\rangle\langle\psi $	p_{de}
$\mathcal{N}_\varepsilon(\rho)$	$\mathcal{N}_1(\rho)$	$\mathcal{N}_1$	Any $ \psi\rangle\langle\psi $	p_ε
$\mathcal{N}_{\text{bf}}(\rho)$	$\mathcal{N}_{\text{pf}}(\rho)$	$\mathcal{N}_1, \mathcal{N}_2$	$ 0\rangle\langle 0 , +\rangle\langle + $	$p_{\text{bf}}, p_{\text{pf}}$
$\mathcal{N}_{\text{bf}}(\rho)$	$\mathcal{N}_{\text{de}}(\rho)$	$\mathcal{N}_2$	$ +\rangle\langle + $	$p_{\text{de}}/2$
$\mathcal{N}_{\text{bf}}(\rho)$	$\mathcal{N}_\varepsilon(\rho)$	$\mathcal{N}_1, \mathcal{N}_2$	$ 0\rangle\langle 0 $	$\max\{p_{\text{BF}}, p_\varepsilon\}$
$\mathcal{N}_{\text{pf}}(\rho)$	$\mathcal{N}_{\text{de}}(\rho)$	$\mathcal{N}_2$	$ 0\rangle\langle 0 $	$p_{\text{de}}/2$
$\mathcal{N}_{\text{pf}}(\rho)$	$\mathcal{N}_\varepsilon(\rho)$	$\mathcal{N}_1, \mathcal{N}_2$	$ +\rangle\langle + $	$\max\{p_{\text{pf}}, p_\varepsilon\}$
$\mathcal{N}_{\text{de}}(\rho)$	$\mathcal{N}_\varepsilon(\rho)$	$\mathcal{N}_1, \mathcal{N}_2$	Any $ \psi\rangle\langle\psi $	$\max\{p_{\text{de}}, p_\varepsilon\}$

[0109]

[0110] 채널 정의에서, X , Z 는 파울리 X , 파울리 Z 연산자이고, $\pi = I/d$ 는 힐버트 공간을 통한 최대 혼합 상태이다.

[0111] 미지 채널이 $\mathcal{N}_{\text{bf}}$ 또는 $\mathcal{N}_{\text{pf}}$ 가 되도록 보장하는 경우를 고려하면 다음과 같다. 이때, 미지 채널의 최적 입력과 ε 값을 찾을 수 있다. ε 값과 함께 다른 가능한 채널 쌍과 이들의 구분 가능 상태에 대한 설명은 표 1에 나열된 바와 같다.

[0112] 필요 충분조건에 따라, 미지 채널이 $\mathcal{N}_{\text{bf}}$ 또는 $\mathcal{N}_{\text{pf}}$ 중 하나이면, 이들은 비-결합이기 때문에 얽힘을 사용하지 않고는 UDQC가 가능하지 않다. 하지만, 제안된 방식은 이러한 구분을 가능하게 한다. 또한, 이는 전송된 양 방향으로 구분 가능한 채널들의 쌍에 불과하다. 따라서, 이들 두 개 중 임의의 하나가 미지 채널이라고 가정할 수 있다. 명확성을 위해, 미지 채널이 $\mathcal{N}_{\text{bf}}$ 이고 채널에 상태 $|0\rangle$ 이 입력 된다고 가정한다. 출력에서, $\{|0\rangle, |1\rangle\}$ 기저로 프로젝트 형태의 측정을 수행할 수 있다. 이때, 아래의 수학적 식 15 내지 18이 성립한다.

수학적 식 15

[0113]

$$\text{tr}(|0\rangle\langle 0| \mathcal{N}_{\text{bf}}(|0\rangle\langle 0|)) = 1 - p_{\text{bf}}$$

수학적 식 16

[0114]

$$\text{tr}(|1\rangle\langle 1| \mathcal{N}_{\text{bf}}(|0\rangle\langle 0|)) = p_{\text{bf}}$$

수학적 식 17

[0115]

$$\text{tr}(|0\rangle\langle 0| \mathcal{N}_{\text{pf}}(|0\rangle\langle 0|)) = 1$$

수학식 18

$$\text{tr}(|1\rangle\langle 1|\mathcal{N}_{\text{pf}}(|0\rangle\langle 0|)) = 0$$

[0116]

[0117]

따라서, 채널 출력이 $|1\rangle$ 상태라고 관측되면, 미지 채널은 $\mathcal{N}_{\text{bf}}$ 이지만 $\mathcal{N}_{\text{pf}}$ 는 아님을 알 수 있다. 또한, 수학식 16에서, $\epsilon = p_{\text{bf}}$ 이다. 또한, 미지 채널이 $\mathcal{N}_{\text{pf}}$ 라고 가정하면, 상태 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ 를 입력하여 UDQC를 수행할 수 있고, $\epsilon = p_{\text{bf}}$ 를 얻게 된다. 채널 파라미터가 알려지지 않은 것으로 가정했기 때문에, 각 채널 사용에 대해 미지 채널을 $\mathcal{N}_{\text{bf}}$ 및 $\mathcal{N}_{\text{pf}}$ 로 교대로 변경한다면 일부 이점 (더 적은 채널 사용 등)을 추가로 얻을 수 있다. 이 경우, $\epsilon = p_{\text{bf}} + p_{\text{pf}}/2$ 는 $\epsilon = \min\{p_{\text{bf}}, p_{\text{pf}}\}$ 인 경우보다 더 나은 성능을 보장한다. 한편, 제안된 비대칭 UDQC 절차는 일반 채널 클래스의 특수한 경우뿐만 아니라, 일반 채널 클래스 (예컨대, 파울리 채널, 하다마드 채널, 유니터리 채널 등)의 경우로 확장 가능하다.

[0118]

이상에서는, 비대칭 UDQC에 대하여 살펴보았다. 이와 관련하여, 비대칭 UDQC에 대한 완화된 필요 충분조건이 유도되었다. 제안된 절차에 따른 수식화와 결과는 일반적이고, 고려되는 채널 세트의 두 가지 파라미터에 의존한다. 두 가지 파라미터에 대한 이러한 의존성으로 인해, 일단 가능한 채널 세트가 주어지면 비대칭 UDQC 절차의 (채널 사용에 관한) 예상 성능을 계산하는 것이 가능하다.

[0119]

한편, 도 2를 참조하여, 제1 및 제2 서브 시스템(100, 200)에 의해 수행되는 비대칭 UDQC(양자 채널의 비-모호 구분) 절차에 대해 살펴보면 다음과 같다. 전술한 바와 같이, 이러한 비대칭(asymmetric) 양자 채널 구별이 제1 서브 시스템(100)에 의해 수행되는 것으로 기재되었으나, 이에 한정되는 것은 아니다. 비대칭 양자 채널 구별은 제2 서브 시스템(200)에 의해서 수행 가능하다. 또는, 제1 및 제2 서브 시스템(100, 200)을 관리하는 임의의 양자 시스템에 의해서도 수행 가능하다. 아래에서는, 편의상 제1 서브 시스템(100)에 의해 수행되는 것으로 기재한다.

[0120]

인터페이스부(120)는 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Min}(\rho_0)$)를 수신한다. 한편, 제어부(110)는 출력 상태를 측정하고, 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단할 수 있다. 이때, 제어부(110)는 출력 상태가 특정 출력 상태의 세트 내에 속하는 경우, 양자 채널 구별이 성공한 것으로 판단할 수 있다.

[0121]

이때, 제어부(110)는 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $\mathcal{A}_{\rho}^{\mathcal{N}_2}$ 에 기반하여, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는지 여부를 판단할 수 있다.

[0122]

이와 관련하여, 제어부(110)는 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 있지 않으면, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 것으로 판단될 때까지 상기 출력 상태의 측정 및 상기 출력 상태의 판단을 반복할 수 있다.

[0123]

한편, 제어부(110)는 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.

[0124]

또한, 제어부(110)는 상기 출력 상태 측정 및 상기 출력 상태 판단의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 있는지를 판단한다. 이때, 상기 출력 상태가 상기 특정 출력 상태 $\mathcal{A}_{\rho}^{\mathcal{N}_1} \setminus \mathcal{A}_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 있지 않고, 상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단한다. 한편, 상기 확률 P2는 수학식 13 및 수학식 14에 의해 결정되고, ϵ 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p1 및 p2

는 사전 확률(priori probabilities)이다.

[0125] 본 발명의 다른 양상에 의하면, 제어부(110)는 출력 상태를 측정하고, 상기 출력 상태에 기반하여, 상기 양자 채널이 ε -구별 가능(distinguishable) 기준에 따라 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한지 여부를 판단할 수 있다. 이때, 제어부(110)는 양자 채널이 ε -구별 가능한 경우, 상기 양자 채널 구별이 성공한 것으로 판단할 수 있다.

[0126] 이때, 상기 ε -구별 가능(distinguishable) 기준은, 수학적 식 10에 의해 결정되고, 수학적 식 10에서 $A_{\rho}^{N_1}$, $A_{\rho}^{N_2}$ 는 각각 제1 채널 및 제2 채널에 대해 가능한(achievable) 제1 출력 상태 및 제2 출력 상태이다. 또한, $\Pi^{N_1}(\rho)$, $\Pi^{N_2}(\rho)$ 는 각각 제1 채널 및 제2 채널의 출력에 대해 수행된 측정 결과이고, 최대화는 모든 밀도 연산자 및 측정 연산자에 대해 수행될 수 있다.

[0127] 한편, 제어부(110)는 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{N_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{N_2}$ 에 기반하여, 상기 출력 상태가 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 속할 확률이 특정 값 이상인지 여부를 판단할 수 있다.

[0128] 이때, 제어부(110)는 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속할 확률이 상기 특정 값보다 작으면, 상기 확률이 상기 특정 값 이상인 것으로 판단될 때까지 상기 출력 상태의 측정 및 상기 출력 상태의 판단을 반복한다. 또한, 제어부(110)는 상기 확률이 상기 특정 값 이상인 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.

[0129] 한편, 제어부(110)는 상기 출력 상태 측정 과정 및 상기 출력 상태 판단 과정의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 있는지를 판단한다. 이때, 제어부(110)는 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 있지 않고, 상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면, 상기 제2 채널을 상기 미지 채널이라고 판단한다.

[0130] 또한, 제어부(110)는 상기 출력 상태 측정 및 상기 출력 상태 판단의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 있는지를 판단한다. 이때, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{N_1} \setminus A_{\rho}^{N_2}$ 의 세트 내에 있지 않고, 상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단한다. 한편, 상기 확률 P2는 수학적 식 13 및 수학적 식 14에 의해 결정되고, ε 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p1 및 p2는 사전 확률(priori probabilities)이다.

[0131] 이상에서는, 본 발명에 따른 비대칭(asymmetric) 양자 채널 구별을 수행하는 양자 시스템에 대해 살펴보았다. 아래에서는, 본 발명의 또 다른 양상에 따른 비대칭(asymmetric) 양자 채널 구별 방법에 대해 살펴본다. 이와 관련하여, 양자 채널 구별을 수행하는 양자 시스템에서 설명된 내용과 양자 채널 구별 방법의 내용은 상호 결합하여 이용될 수 있다.

[0132] 이와 관련하여, 도 6은 본 발명의 일 실시 예에 따른 비대칭(asymmetric) 양자 채널 구별 방법의 흐름도를 나타낸다. 도 6을 참조하면, 양자 채널 구별 방법은 출력 상태 측정 과정(S110), 출력 상태 판단 과정(S120) 및 채널 구별 과정(S130)을 포함한다.

[0133] 출력 상태 측정 과정(S110)에서, 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($\text{Mun}(\rho_0)$)를 측정한다. 출력 상태 판단 과정(S120)에서, 상기 출력 상태가 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한 특정 출력 상태의 세트 내에 속하는지 여부를 판단한다. 채널 구별 과정(S130)에서, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 경우, 상기 양자 채널 구별이 성공한 것으로 판단한다.

[0134] 한편, 출력 상태 측정 과정(S110)에서, 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{N_1}$ 및 제2 채널에

대해 가능한 제2 출력 상태인 $A_{\rho}^{\mathcal{N}_2}$ 에 기반하여, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{\mathcal{N}_1} \setminus A_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는지 여부를 판단할 수 있다.

[0135] 이때, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 있지 않으면, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속하는 것으로 판단될 때까지 상기 출력 상태 측정 과정(S110) 및 상기 출력 상태 판단 과정(S120)을 반복할 수 있다.

[0136] 한편, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{\mathcal{N}_1} \setminus A_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속하는 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.

[0137] 한편, 상기 출력 상태 측정 과정(S110) 및 상기 출력 상태 판단 과정(S120)의 반복과 연관된 채널 사용이 N번 이상이고, 상기 출력 상태가 상기 특정 출력 상태 $A_{\rho}^{\mathcal{N}_1} \setminus A_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 있지 않으면, 상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단할 수 있다. 이때, 상기 확률 P2는 수학적 식 13 및 수학적 식 14에 의해 결정되고, ε 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p1 및 p2는 사전 확률(priori probabilities)이다.

[0138] 한편, 본 발명의 다른 실시 예에 따른 비대칭(asymmetric) 양자 채널 구별 방법에 대해 살펴보면 다음과 같다. 이와 관련하여, 도 7은 본 발명의 다른 실시 예에 따른 비대칭(asymmetric) 양자 채널 구별 방법의 흐름도를 나타낸다. 도 7을 참조하면, 양자 채널 구별 방법은 출력 상태 측정 과정(S110), 출력 상태 판단 과정(S120') 및 채널 구별 과정(S130')을 포함한다.

[0139] 출력 상태 측정 과정(S110)에서, 입력 상태(ρ_0)를 갖는 양자 채널의 출력 상태($Mun(\rho_0)$)를 측정한다. 출력 상태 판단 과정(S120')에서, 상기 출력 상태에 기반하여, 상기 양자 채널이 ε -구별 가능(distinguishable) 기준에 따라 양자 채널 구별(UDQC: Unambiguous Discrimination of Quantum Channel)이 가능한지 여부를 판단한다. 채널 구별 과정(S130')에서, 상기 양자 채널이 ε -구별 가능한 경우, 상기 양자 채널 구별이 성공한 것으로 판단한다.

[0140] 상기 ε -구별 가능(distinguishable) 기준은, 수학적 식 10에 의해 결정되고, 수학적 식 10에서 $A_{\rho}^{\mathcal{N}_1}$, $A_{\rho}^{\mathcal{N}_2}$ 는 각각 제1 채널 및 제2 채널에 대해 가능한(achievable) 제1 출력 상태 및 제2 출력 상태이다. 또한, $\Pi^{\mathcal{N}_1}(\rho)$, $\Pi^{\mathcal{N}_2}(\rho)$ 는 각각 제1 채널 및 제2 채널의 출력에 대해 수행된 측정 결과이고, 최대화는 모든 밀도 연산자 및 측정 연산자에 대해 수행될 수 있다.

[0141] 상기 출력 상태 판단 과정(S120')에서, 제1 채널에 대해 가능한(achievable) 제1 출력 상태 $A_{\rho}^{\mathcal{N}_1}$ 및 제2 채널에 대해 가능한 제2 출력 상태인 $A_{\rho}^{\mathcal{N}_2}$ 에 기반하여, 상기 출력 상태가 특정 출력 상태 $A_{\rho}^{\mathcal{N}_1} \setminus A_{\rho}^{\mathcal{N}_2}$ 의 세트 내에 속할 확률이 특정 값 이상인지 여부를 판단할 수 있다.

[0142] 한편, 상기 출력 상태가 상기 특정 출력 상태의 세트 내에 속할 확률이 상기 특정 값보다 작으면, 상기 확률이 상기 특정 값 이상인 것으로 판단될 때까지 상기 출력 상태 측정 과정(S110) 및 상기 출력 상태 판단 과정(S120')을 반복할 수 있다. 이때, 상기 확률이 상기 특정 값 이상인 것으로 판단되면, 미지(unknown) 채널이 상기 제1 채널이고, 상기 UDQC가 성공한 것으로 판단할 수 있다.

[0143] 한편, 상기 출력 상태 측정 과정(S110) 및 상기 출력 상태 판단 과정(S120')의 반복과 연관된 채널 사용이 N번 이상이고, 상기 확률이 상기 특정 값보다 작으면, 상기 제2 채널이 상기 미지 채널이라고 판단할 수 있는 확률 P2가 특정 값 이상이면 상기 제2 채널을 상기 미지 채널이라고 판단할 수 있다. 이때, 상기 확률 P2는 수학적 식 13 및 수학적 식 14에 의해 결정되고, ε 은 상기 채널 사용이 1회인 경우의 상기 UDQC의 성공 확률이고, p1 및 p2는 사전 확률(priori probabilities)이다.

[0144] 이상에서는, 본 발명에 따른 비대칭 양자 채널 구별 방법 및 이를 수행하는 양자 시스템에 대해 살펴보았다.

[0145] 본 발명의 적어도 일 실시 예에 따르면, 양자 얽힘에 관한 명확한 정보 없이도 비대칭 양자 채널 구별 방법을

제공할 수 있다는 장점이 있다.

[0146] 또한, 본 발명의 적어도 일 실시 예에 따르면, 양자 채널이 분명한 구분이 용이하지 않은 경우, 출력 상태 측정 및 출력 상태 판단의 반복을 통해 양자 채널을 구분하는 확률적인 방법을 제공할 수 있다는 장점이 있다.

[0147] 본 발명에 따른 비대칭(asymmetric) 양자 채널 구별 방법 및 이를 수행하는 양자 시스템은 미지의 양자 채널 식별 등에 활용 가능하다. 이러한 양자 채널 식별 방법은 양자 얽힘 상태를 이용하지 않고 미지의 주어진 양자 채널의 식별을 위한 양자 기기 등에 활용되어 기술 사업화가 가능하다.

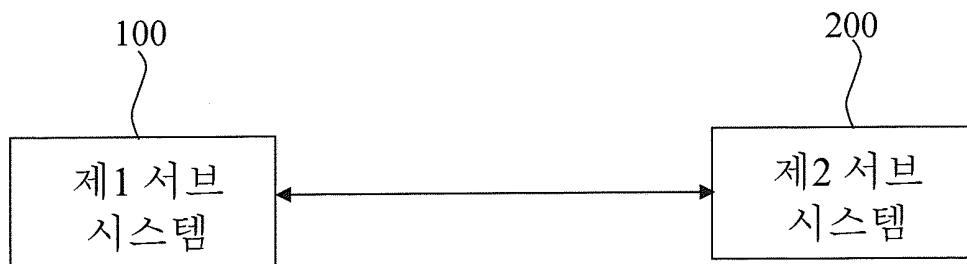
[0148] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능뿐만 아니라 각각의 구성 요소들은 별도의 소프트웨어 모듈로도 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 메모리에 저장되고, 제어부(controller) 또는 프로세서(processor)에 의해 실행될 수 있다.

부호의 설명

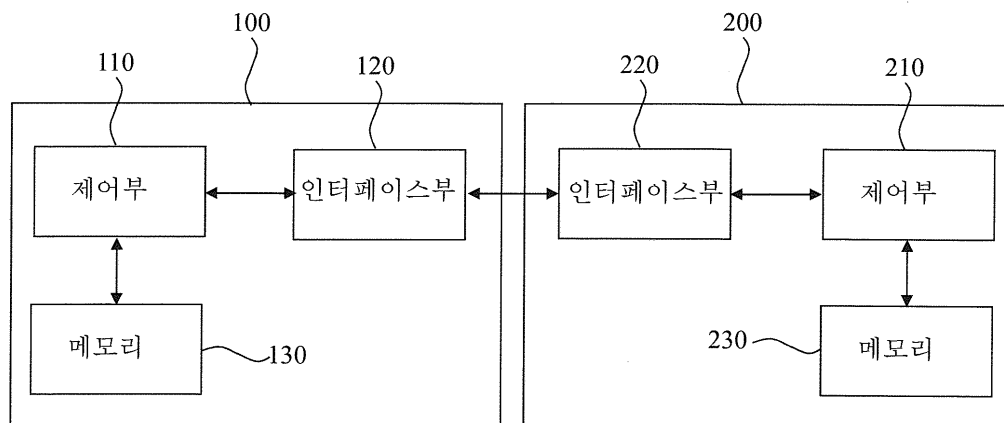
[0149] 100: 제1 서버 시스템 200: 제2 서버 시스템
110, 210: 제어부 120, 220: 인터페이스부
130, 230: 메모리

도면

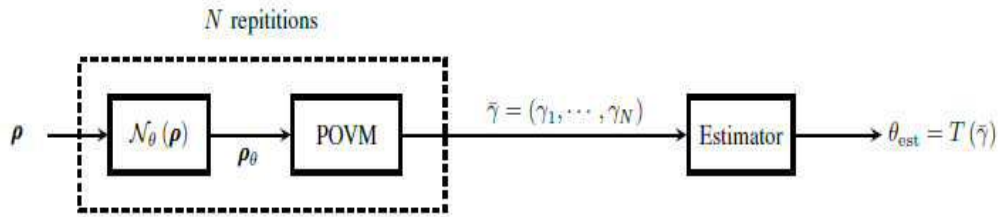
도면1



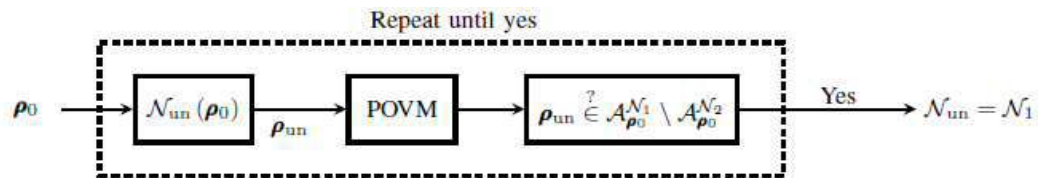
도면2



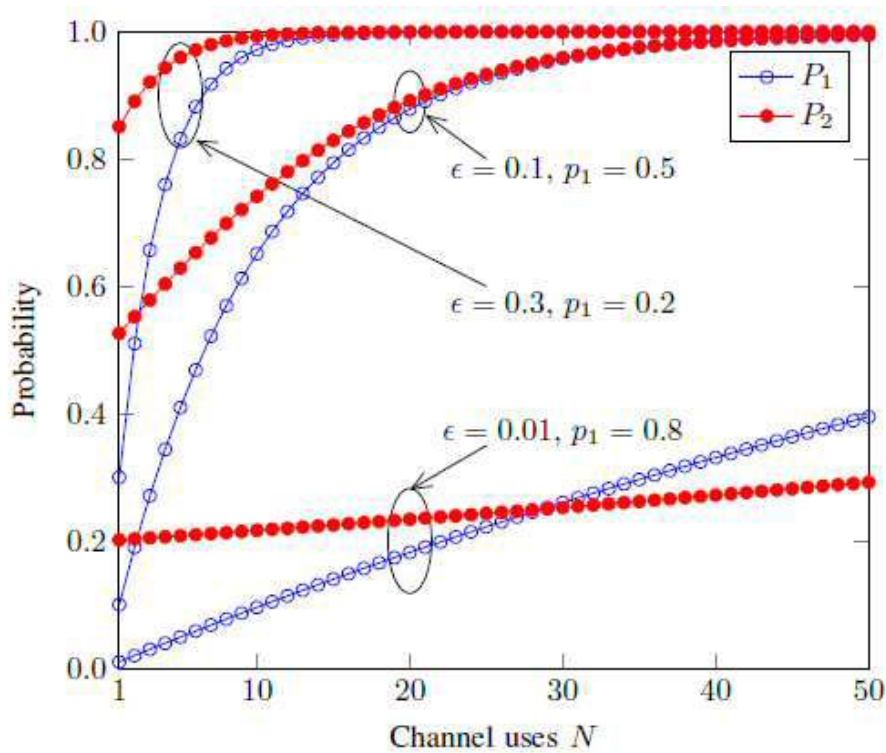
도면3



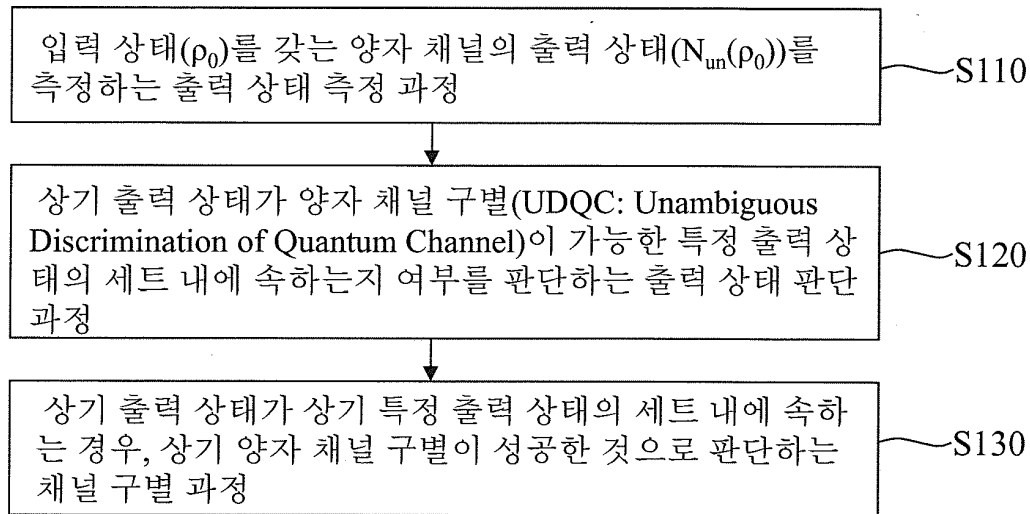
도면4



도면5



도면6



도면7

